DRI CANADA
Train. Prepare. Recover.
Former • Préparer • Rétablir

ISSN 2816-900X (print)
ISSN 2816-9018 (online)

TRUE NORTH RESILIENCE
Résilience du vrai nord

DRI Canada's magazine / Magazine de DRI Canada

Vol 04 No 2 Fall/Automne 2025 (7th Edition)

In this Issue:

- **THE IMPORTANCE OF IMS**

plus:

- **ARTIFICIAL INTELLIGENCE**

and much more…

Dans ce numéro :

- **L'IMPORTANCE DE L'IMS**

plus:

- **INTELLIGENCE ARTIFICIELLE**

et plus encore…

Canadian Publication Agreement Number 44001035

www.dri.ca

Upcoming Symposium
Symposium à venir

DRI Canada Gatineau Symposium - November 20, 2025 Hilton Lac Leamy

The DRI Canada Symposium in Gatineau is a premier bilingual gathering for senior-level professionals specializing in business continuity, disaster recovery, cyber resilience, and risk management. This one-day event, themed "One Country, One Network," will bring together experts and practitioners from across Canada to foster collaboration, share knowledge, and explore innovative approaches to building resilient organizations.

Join DRI Canada in Gatineau for a day of impactful learning, strategic networking, and the opportunity to strengthen Canada's unified business continuity network.

Symposium DRI Canada à Gatineau - 20 novembre 2025 Hilton Lac Leamy

Le symposium DRI Canada à Gatineau est un événement bilingue de premier plan qui rassemble des professionnels de haut niveau spécialisés dans la continuité des activités, la reprise après sinistre, la cyber-résilience et la gestion des risques. Cet événement d'une journée, intitulé « Un pays, un réseau », réunira des experts et des praticiens de partout au Canada afin de favoriser la collaboration, de partager des connaissances et d'explorer des approches novatrices pour bâtir des organisations résilientes.

Joignez-vous à DRI Canada à Gatineau pour une journée d'apprentissage enrichissante, de réseautage stratégique et l'occasion de renforcer le réseau unifié de continuité des activités du Canada.

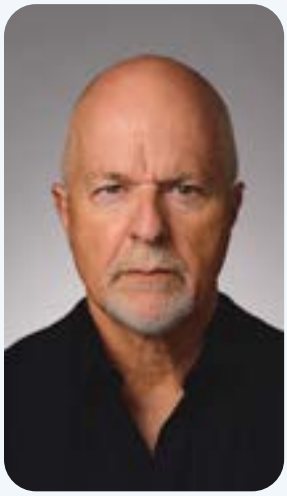
REGISTER ONLINE AT:

INSCRIVEZ-VOUS EN LIGNE :

https://mms.dri.ca/members/evr/reg_event.php?orgcode=DRIC&evid=54190491

Keynote Speaker: Chris Mathers

Mathers is a unique, humorous, and fascinating speaker who touches on issues from security, hiring decisions, and background checks to money laundering, corporate fraud, and the incredible impact artificial intelligence (AI) is having on the prevention and spread of crime.



Conférencier principal : Chris Mathers

M. Mathers est un conférencier unique, plein d'humour et fascinant qui aborde des questions allant de la sécurité, des décisions d'embauche et des vérifications des antécédents au blanchiment d'argent, à la fraude d'entreprise et à l'incroyable impact de l'intelligence artificielle (IA) sur la prévention et la propagation de la criminalité.

Vol 04 No 2 Fall/Automne 2025 (7th Edition)

CONTENTS • LE SOMMAIRE

President's Message 5
Message du président
Nancy Holloway-White

Editors' Desk 7
Bureau des redacteurs
Garth Tucker

FEATURE ARTICLE • ARTICLE VEDETTE

Why Customized IMS Systems are Essential 9
Pourquoi les systèmes IMS personnalisés sont essentiels
Claire Mechan

The Papal Conclave Succession Plan 16
Le plan de succession du conclave papal
Vito Mangialardi MBCI, CBCP, PMP

An Expert's Impression 21
L'impression d'un expert
Aidan Firlotte, Kristin Nelles, Robin Whyte, Nancy Holloway-White, Rick Cooper, Helen Feng, Jonathan Cummings, & Sukhmani Sandhu

Artificial Intelligence in Disaster Recovery Planning 42
L'intelligence artificielle dans la planification de la reprise après sinistre
ChatGPT 5 Thinking (AI)

Artificial Confidence: The Illusion of AI-Led Resilience 56
Confiance Artificielle: l'illusion de la résilience induite par l'IA
Jason Firlotte & Jessa Cinnamon

Dollars And Sense: Boost Your Salary With Certification 63
Le bon sens financier : augmentez votre salaire grâce à une certification
Joel Baglole

Sometimes We Need To Unlearn 68
Parfois, nous devons désapprendre
Andy Prince

A Student's Perspective of AI 70
Le point de vue d'un étudiant sur l'IA
Katelyn Holowachuk

Modernizing Resilience 75
Moderniser la resilience
Nancy Holloway-White, Emad Aziz, & Garth Tucker

Lunch & Learn - Reviews 87
Déjeuner et apprentissage - Examens
Brock Holowachuk

DRIC Student Award and Scolarship 91
Prix et bourses DRIC pour les étudiants

STUDENT ARTICLES • ARTICLES POUR LES ÉTUDIANTS

Adapting to the Smoke 92
S'adapter à la fuméeAndy Prince
Sharon Sa

Closing the Gaps 100
Combler les lacunes
Oscar Vincente, PhD

Call for Articles 106
Appel à articles

2025 Awards of Excellence 107
Prix d'excellence 20252

* Cliquez sur le numéro de page pour naviguer

* Click page number to navigate

Advertisers' Index • Index des annonceurs

Sponsor	*Page*	*Website*
Benoit Racette Services-conseils inc	33	racetteconseils.com
Continuity & Resilience Today (Oct. 21-22)	25	crtdemcon.ca
DRIC - Upcoming Events	54	dri.ca/events.php
DRIC - Gatineau Symposium (Nov 20)	2	https://crtdemcon.ca/crt/
Vanguard EMC Inc.	6	vanguardemergency.com

DRI CANADA
Train. Prepare. Recover.
Former • Préparer • Rétablir

www.dri.ca

TRUE NORTH RESILIENCE
Résilience du vrai nord

DRI Canada's magazine / Magazine de DRI Canada

True North Resilience is published twice per year. Its mission is to facilitate the exchange of information among professionals in the field of disaster recovery, risk management, high availability and resilience; provide them with practical tools and techniques, and serve as a forum for discussion of emerging trends and issues.

La Magazine de Résilience du vrai nord est publié deux fois par an. Sa mission est de faciliter l'échange d'informations entre les professionnels dans le domaine de la reprise après sinistre, de la gestion des risques, de la haute disponibilité et de la résilience ; de leur fournir des outils et des techniques pratiques, et de servir de forum de discussion sur les tendances et les questions émergentes.

Manuscripts, other editorial submissions, and advertising should be submitted via email to:

Les manuscrits, les autres propositions éditoriales et la publicité doivent être envoyés par courrier électronique à l'adresse suivante:

Editor-in-Chief:
Garth Tucker, CBCP, CORP
Email: editors@dri.ca
Toll Free: 1-844-228-8135
Local: 416-646-2750

©2025 Disaster Recovery Institute Canada. All rights reserved. Unless otherwise specified, all letters and articles received are assumed for publication and become the copyright property of True North Resilience if published.

©2025 Disaster Recovery Institute Canada. Tous droits réservés. Sauf indication contraire, toutes les lettres et tous les articles reçus sont supposés être publiés et deviennent la propriété de True North Resilience en cas de publication.

Send mailing list queries, and requests for reprints, bulk copies, or reprint permission by email to: editors@dri.ca, or by surface mail to:
DRIC, 701 Rossland Road East,
Suite 375, Whitby, ON, L1N 8Y9.

Envoyez vos demandes de renseignements sur la liste d'envoi et vos demandes de réimpression, de copies en vrac ou d'autorisation de réimpression par courriel à : editors@dri.ca, ou par courrier ordinaire à :
DRIC, 701 Rossland Road East,
Suite 375, Whitby, ON, L1N 8Y9.

Printed in Canada

Board of Directors
Conseil d'administratio

The Board of Directors sets DRI CANADA's goals, strategic direction and policy, and offers guidance, under the guidelines and ethical direction set by DRI International. The Board is the governing body of DRI CANADA and is responsible for the business direction, policy making, public awareness and fiscal management of the organization.

Nancy Holloway-White, CBCP, CBCA
President

Lisa Maddock, ABCP
Vice-President

Scott Leavitt, CBCP
Treasurer

Brenda Escribano, CBCP
Secretary & Privacy Officer

Steve Palubiski, MBCP
Certification Commission Chair

Jason Firlotte, MBCP, CBRM, MBCI, CSP, CBCV
Education Commission Chair
Director Ontario Region

Troy McQuinn, CEM, ABCP
Director Atlantic Region

Patrick Leduc, CBCP
Director Quebec Region

Jeff Hortobagyi, CBCP
Director Pacific Region

Brock Holowachuk, CBCP
Past President, Director at Large

Andrea Buchholz, CBCLA
Director at Large

Alexander Landry, CBCP
Director at Large

Jeremy Paulis, CBCP
Director at Large

Greg Solecki, CBCP
Director at Large

Perry Ruehlen, CAE
Executive Director

Magazine Steering Committee
Comité directeur du magazine

Executive Director	Perry Ruehlen, CAE
Editor-in-Chief	Garth Tucker, CBCP, CORP
Design Editor	Vaughn Dragland, BASc, ISP, PMP
Associate Editor	Brenda Escribano, CBCP
Associate Editor	Brock Holowachuk, CBCP
Associate Editor	Lisa Maddock, ABCP
Associate Editor	Nancy Holloway-White, CBCP, CBCA

About DRI Canada

DRI Canada is a non-profit organization that provides internationally recognized education and certification to business continuity, disaster recovery and emergency management professionals in Canada.

DRI CANADA mission (or how we are creating a value for our certified professionals):

- Promoting a base of common knowledge for the continuity and resiliency management profession together with DRI;
- Certifying qualified individuals in the disciplines of business continuity, disaster recovery and emergency management;
- Advocating for and increasing the professional value of DRI's credentials and those who hold them.

À propos de DRI Canada

DRI Canada est un organisme sans but lucratif qui offre une formation et une certification reconnues internationalement aux professionnels de la continuité des affaires, de la reprise après sinistre et de la gestion des urgences au Canada. Mission de DRI CANADA (ou comment nous créons une valeur pour nos professionnels certifiés) :

- Promouvoir une base de connaissances communes pour la profession de gestion de la continuité et de la résilience en collaboration avec DRI;
- Certifier des personnes qualifiées dans les disciplines de la continuité des affaires, de la reprise après sinistre et de la gestion des urgences;
- Promouvoir et accroître la valeur professionnelle des titres de compétences de DRI et de ceux qui les détiennent.

© DRI Canada, and the DRI Canada logo are trademarks or registered trademarks of the Disaster Recovery Institute of Canada, in Canada and other countries.

Eclipse
Graphic Design
Eclipse Technologies Inc.
416-219-8790
e-clipse.ca

CANMARK COMMUNICATIONS
Printing, Binding, Lettershop
Canmark Communicatrions
416.553.8228
canmarkcommunications.com

ISSN 2816-9018 (on-line)

President's Message
Message du président

By/Par Nancy Holloway-White, CBCP, CBCA, President, DRI Canada

To my fellow BCM professionals,

So far, **2025** has presented BCM professionals in Canada with some solid work variety: geopolitical tensions, supply chain disruptions & outright changes, labour disruptions, natural disasters, floods, wildfires, and other climate-driven events, continuing to learn about artificial intelligence (either intentionally or by osmosis), and for some, understanding the impact of the growing demand for computing power. Customer expectations (rightfully-so) remain high, and the interdependencies are complex.

According to an insurance industry corporate risk survey in 2025; business interruption (includes supply chain issues), tops Canada's list of business risks at 38%, followed closely by natural catastrophes at 37% and cyber incidents at 35%[1]. According to the Canadian Cyber Security Network, cyber threats are a growing concern, with ransomware, AI-powered attacks, and deepfake scams targeting critical systems across healthcare, finance, energy, and technology sectors[2 3]. The Canadian Government's 2025 National Cyber Security Strategy lists whole-of-society engagement as an overarching principal; the report states the need for robust partnerships across provinces, Indigenous communities, industry, and academia to secure Canada's digital infrastructure[4]. You can read the thoughts of professionals from BCM and other industries on this topic in the 'An Expert's Impression' section as the True North Resilience Editor suggested an AI-related question.

Floods and wildfires are certainly top-of-mind for BCM professionals in Canada. According to the OECD, wildfires have increasingly costly infrastructure impacts in densely populated areas like Toronto, Montreal, and Vancouver[5]. "Canada's second-worst wildfire season on record has already burned

À mes collègues professionnels de la gestion de la continuité des activités (GCA),

Jusqu'à présent, l'année 2025 a offert aux professionnels de la GCA au Canada une grande variété de tâches : tensions géopolitiques, perturbations et changements radicaux dans la chaîne d'approvisionnement, perturbations du travail, catastrophes naturelles (inondations, incendies de forêt et autres événements liés au climat), apprentissage continu de l'intelligence artificielle (intentionnellement ou par osmose) et, pour certains, compréhension de l'impact de la demande croissante en puissance de calcul. Les attentes des clients (à juste titre) restent élevées et les interdépendances sont complexes.

Selon une enquête sur les risques d'entreprise menée en 2025 dans le secteur des assurances, les interruptions d'activité (y compris les problèmes liés à la chaîne d'approvisionnement) arrivent en tête de la liste des risques commerciaux au Canada avec 38 %, suivies de près par les catastrophes naturelles avec 37 % et les cyberincidents avec 35 %[1]. Selon le Réseau canadien de cybersécurité, les cybermenaces sont une préoccupation croissante, avec les ransomwares, les attaques basées sur l'IA et les escroqueries par deepfake qui ciblent les systèmes critiques dans les secteurs de la santé, de la finance, de l'énergie et de la technologie[2 3]. La Stratégie nationale de cybersécurité 2025 du gouvernement canadien cite l'engagement de l'ensemble de la société comme principe fondamental ; le rapport souligne la nécessité de partenariats

[1] https://isure.ca/inews/2025-canadian-business-risks/#Allianz_Risk_Barometer_Methodology
[2] https://canadiancybersecuritynetwork.com/hubfs/CS-Report-CCN-2025-All-v10.pdf
[3] Not to mention our maturer population, who, as BCM professionals, we include in planning
[4] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/ntnl-cbr-scrt-strtg-2025-en.pdf

7.8 million hectares", with fires across the Prairies and Atlantic regions[6].

I am encouraged by Canada's Emergency Management Strategy promoting a "whole-of-society" approach involving annual reviews by federal, provincial, and territorial agencies[7]. I challenge further that it is through collaborating, looking beyond the clear-cut and into the nuanced understanding of others; truly listening and working together for change that we can collectively make a more resilient Canada. Qualified Business Continuity Management professionals are a somewhat hidden, yet essential resource in Canada. We need to continue to do our part with our specialized understanding of risk management. Ω

Nancy Holloway-White, CBCP, CBCA (she/her)
President, DRI Canada

solides entre les provinces, les communautés autochtones, l'industrie et le monde universitaire afin de sécuriser l'infrastructure numérique du Canada[4]. Vous pouvez lire les réflexions de professionnels du BCM et d'autres secteurs sur ce sujet dans la section « L'avis d'un expert », où le rédacteur en chef de True North Resilience a posé une question liée à l'IA.

Les inondations et les incendies de forêt sont certainement au premier plan des préoccupations des professionnels de la gestion de la continuité des activités au Canada. Selon l'OCDE, les incendies de forêt ont des répercussions de plus en plus coûteuses sur les infrastructures dans les zones densément peuplées comme Toronto, Montréal et Vancouver[5]. « La deuxième pire saison d'incendies de forêt jamais enregistrée au Canada a déjà brûlé 7,8 millions d'hectares », avec des incendies dans les Prairies et les régions atlantiques[6].

Je trouve encourageante la stratégie canadienne de gestion des urgences, qui promeut une approche « globale » impliquant des examens annuels par les agences fédérales, provinciales et territoriales[7]. Je soutiens en outre que c'est en collaborant, en regardant au-delà des idées reçues et en cherchant à comprendre les nuances chez les autres, en écoutant véritablement et en travaillant ensemble pour le changement, que nous pouvons collectivement rendre le Canada plus résilient. Les professionnels qualifiés en gestion de la continuité des activités sont une ressource quelque peu cachée, mais essentielle au Canada. Nous devons continuer à jouer notre rôle grâce à notre compréhension spécialisée de la gestion des risques. Ω

Nancy Holloway-White, CBCP, CBCA (elle)
Présidente, DRI Canada

[5] https://www.oecd.org/en/publications/2025/05/oecd-economic-surveys-canada-2025_ee18a269/full-report/adapting-to-climate-change-challenges_e62681b8.html

[6] https://www.reuters.com/business/environment/canadas-wildfires-could-continue-into-fall-says-government-2025-08-18/#:~:text=WINNIPEG%2C%20Manitoba%2C%20Aug%2018%20(,federal%20government%20officials%20said%20Monday

[7] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgncy-mngmnt-strtgy/index-en.aspx

Editors' Desk
Bureau des rédacteurs

Many exciting things coming up this fall, by the time you read this, some of them will have taken place and we hope you enjoyed them! This issue is released to coincide with DRI Canada's annual Fall Symposium in Gatineau, PQ (https://dri.ca/details.php) and I strongly suggest registering as it has proven to be an incredibly beneficial experience to all who attended in the past, with Best of Breed sessions covering many aspects of our industry. The Symposium takes place on November 20th and as a bonus, on the day leading up to this, there are two sessions being held on the 19th by Suzanne Bernier (BCP Ethics in Crisis Management: Navigating Integrity Through Chaos and Crisis) and Jonathan Cummings (a high-intensity tabletop exercise simulates a ransomware attack on a critical public sector organization). Not to be missed - in our humble opinions. $59 per session (includes certificate of attendance, 3 continuing education credits and nutritional break) or $129 for both sessions (includes certificate of attendance, 6 continuing education points, lunch and nutritional breaks.)

This issue is predominantly devoted to Artificial Intelligence (AI) as it has exploded into everyone's daily lives in a big way this year and we're all trying to determine how we can be effective with its capabilities. So, we searched out subject matter experts to provide their experiences with its use, a better understanding of its abilities and functionality, as well as how it can be used in Resilience. Our feature, "An Expert's Impression", question this issue is;

De nombreux événements passionnants sont prévus cet automne. Au moment où vous lirez ces lignes, certains d'entre eux auront déjà eu lieu et nous espérons que vous les aurez appréciés ! Ce numéro est publié à l'occasion du symposium annuel d'automne de DRI Canada à Gatineau, au Québec (https://dri.ca/details.php). Je vous recommande vivement de vous y inscrire, car il s'agit d'une expérience extrêmement enrichissante pour tous ceux qui y ont participé par le passé, avec des sessions de haut niveau couvrant de nombreux aspects de notre secteur. Le symposium aura lieu le 20 novembre et, en prime, la veille, le 19, deux sessions seront animées par Suzanne Bernier (Éthique BCP dans la gestion de crise : naviguer dans l'intégrité à travers le chaos et la crise) et Jonathan Cummings (un exercice de simulation à haute intensité simulant une attaque par ransomware contre une organisation critique du secteur public). À ne pas manquer, à notre humble avis. 59 $ par session (comprend un certificat de participation, 3 crédits de formation continue et une pause nutritionnelle) ou 129 $ pour les deux sessions (comprend un certificat de participation, 6 points de formation continue, le déjeuner et les pauses nutritionnelles).

Ce numéro est principalement consacré à l'intelligence artificielle (IA), qui a fait une entrée fracassante dans la vie quotidienne de chacun cette année et dont nous essayons tous de déterminer comment tirer le meilleur parti des capacités. Nous avons donc sollicité des experts en la matière afin qu'ils nous fassent part de leur

"With the rapid advancement and adoption of artificial intelligence across all sectors of business, how do you foresee AI reshaping your industry in the next 3 to 5 years, in terms of innovation, workforce, and competitive advantage?"

A very diverse group of experts graciously agreed to provide their impressions and I think it's an incredible opportunity to expand your thought processes on AI and its impact on not just our industry, but all the possibilities for good and not so good.

The AI articles featured in this issue include:

- Artificial Intelligence in Disaster Recovery Planning, by ChatGPT 5 Thinking (prompted by Miles Jenkins)
- Artificial Confidence: The Illusion of AI-Led Resilience, by Jason Firlotte and Jenna Cinnamon (with help from ChatGPT)

In addition to AI, we have some great articles from Vito Mangialardi providing an entertaining view of succession planning (an often-overlooked function of BC), advice on maintaining mental health by Andy Prince. Dollars and Sense by Joel Baglole in which he interviews two very experienced folks regarding the financial advantages of having an industry designation. A frequent contributor and ally of DRI Canada, Claire Mechan, has provided us with an in-depth discussion on why IMS systems are essential. Finally, last but not least, Nancy Holloway-White, Emad Aziz, and myself have put together an overview on integrating criticality scoring to inform RTOs and make your restoration priorities more accurate.

We like to think that this magazine belongs to DRI's Certified Professionals, and we hope you feel part of the process. Thanks to everyone who makes our magazine function!

- Garth Ω

expérience dans son utilisation, nous aident à mieux comprendre ses capacités et ses fonctionnalités, et nous expliquent comment elle peut être utilisée dans le domaine de la résilience. Notre rubrique « L'avis d'un expert » pose la question suivante :

« Avec les progrès rapides et l'adoption généralisée de l'intelligence artificielle dans tous les secteurs d'activité, comment voyez-vous l'IA transformer votre secteur au cours des 3 à 5 prochaines années, en termes d'innovation, de main-d'œuvre et d'avantage concurrentiel ? »

Un groupe très diversifié d'experts a gracieusement accepté de partager ses impressions, et je pense que c'est une occasion incroyable d'élargir votre réflexion sur l'IA et son impact non seulement sur notre secteur, mais aussi sur toutes les possibilités, bonnes ou moins bonnes.

Les articles sur l'IA présentés dans ce numéro sont les suivants :

- L'intelligence artificielle dans la planification de la reprise après sinistre, par ChatGPT 5 Thinking (à l'initiative de Miles Jenkins)
- Confiance artificielle : l'illusion de la résilience guidée par l'IA, par Jason Firlotte et Jenna Cinnamon (avec l'aide de ChatGPT)

En plus de l'IA, nous avons d'excellents articles de Vito Mangialardi qui offrent une vision divertissante de la planification de la relève (une fonction souvent négligée de la CB), des conseils sur le maintien de la santé mentale par Andy Prince. Dollars and Sense de Joel Baglole, dans lequel il interviewe deux personnes très expérimentées sur les avantages financiers d'avoir une désignation professionnelle. Claire Mechan, collaboratrice régulière et alliée de DRI Canada, nous a fourni une analyse approfondie des raisons pour lesquelles les systèmes IMS sont essentiels. Enfin, Nancy Holloway-White, Emad Aziz et moi-même avons rédigé un aperçu sur l'intégration de la notation de criticité pour informer les RTO et rendre vos priorités de restauration plus précises.

Nous aimons penser que ce magazine appartient aux professionnels certifiés de DRI, et nous espérons que vous vous sentez partie prenante dans ce processus. Merci à tous ceux qui contribuent au bon fonctionnement de notre magazine !

- Garth Ω

FEATURE ARTICLE

Why Customized IMS Systems are Essential

ARTICLE VEDETTE

Pourquoi les systèmes IMS personnalisés sont essentiels

By/Par Claire Mechan

Why Business Continuity and Emergency Management (EMBC) Professionals Should Champion Tailored Incident Management Systems in Corporate Settings

As we see increasing disruptions impacting corporate environments, from cyber incidents to severe weather and civil unrest, EMBC professionals should be promoting that corporations rethink and redesign how they prepare for, respond to, and recover from crises. One of the most strategic actions an organization can take is to develop an internal incident management system (IMS) that is purpose-built for its business operations, culture, and risk profile.

This article will focus on the importance of not only having an IMS but ensuring it is an IMS that will work for your organization. An effective IMS does more than just tick compliance boxes, it enhances resilience, protects continuity, and supports decision-makers when it matters most.

The Origins of ICS: Lessons from the Public Sector

Many organizations start their IMS journey by turning to the Incident Command System (ICS). Widely used today, ICS has its roots in wildland firefighting. It was born in the aftermath of a series of devastating wildfires in Southern California during the 1970s. In response to the coordination breakdowns during those fires, a review determined that a new system was needed, one that could unify command, communication, and control across multiple agencies.

At that time, the Large Fire Organization (LFO), which was originally developed by veterans returning from WWII, served as a foundational model. This evolved into FIRESCOPE (Firefighting Resources of Southern California Organized

Pourquoi les professionnels de la continuité des activités et de la gestion des urgences (EMBC) devraient promouvoir des systèmes de gestion des incidents adaptés aux entreprises

Alors que nous assistons à une multiplication des perturbations affectant les environnements d'entreprise, qu'il s'agisse d'incidents cybernétiques, de conditions météorologiques extrêmes ou de troubles civils, les professionnels de l'EMBC devraient encourager les entreprises à repenser et à redéfinir leur manière de se préparer, de réagir et de se remettre des crises. L'une des mesures les plus stratégiques qu'une organisation puisse prendre consiste à développer un système interne de gestion des incidents (IMS) spécialement conçu pour ses opérations commerciales, sa culture et son profil de risque.
Cet article mettra l'accent sur l'importance non seulement de disposer d'un IMS, mais aussi de s'assurer qu'il est adapté à votre organisation. Un IMS efficace ne se contente pas de cocher des cases de conformité, il renforce la résilience, protège la continuité et soutient les décideurs lorsque cela est le plus important.

Les origines de l'ICS : les enseignements tirés du secteur public

De nombreuses organisations commencent leur transition vers l'IMS en se tournant vers le système de commandement des interventions (ICS). Largement utilisé aujourd'hui, l'ICS trouve ses origines dans la lutte contre les incendies de forêt. Il est né à la suite d'une série d'incendies dévastateurs dans le sud de la Californie dans les années 1970. En réponse aux problèmes de coordination rencontrés lors de ces incendies, une étude a conclu à la nécessité de mettre en place un nouveau système capable d'unifier le commandement, la communication et le contrôle entre plusieurs agences.

for Potential Emergencies), a FEMA-funded initiative involving several agencies. FIRESCOPE initially developed the Field Command Operations System, which later became the ICS we know today.

By the mid-1980s, ICS was in wide use across the United States, and its principles of standardized command, control, and coordination began spreading internationally.

ICS and the Canadian Context

Before ICS became the standard in Canada, many Canadian response agencies followed an Emergency Site Management (ESM) model in the 1980s. ESM divided operations between two main locations: the emergency site and the Emergency Operations Centre (EOC).

Starting in the early 1990s, ICS gained traction in Canada and is now widely adopted across response organizations and governments. Today, most Canadian organizations are encouraged to use ICS for both their Incident Command Posts (ICPs) and EOCs, promoting a consistent and scalable command structure during incidents.

The Rise of NIMS: A National Framework

Following the September 11 attacks in the U.S., the need for a unified, nationwide approach to incident management became clear. This led to the development of the National Incident Management System (NIMS), which extends the ICS model into a broader, more comprehensive framework.

NIMS provides shared language, principles, and operational systems to help all stakeholders—from first responders to executives in EOCs, collaborate effectively. In the United States, adopting NIMS is a requirement for local, state, and tribal jurisdictions that receive federal preparedness funding.

ICS with its extension initiatives is a

À l'époque, la Large Fire Organization (LFO), initialement développée par des vétérans de la Seconde Guerre mondiale, a servi de modèle de base. Ce modèle a évolué pour devenir FIRESCOPE (Firefighting Resources of Southern California Organized for Potential Emergencies), une initiative financée par la FEMA et impliquant plusieurs agences. FIRESCOPE a initialement développé le Field Command Operations System, qui est devenu plus tard l'ICS que nous connaissons aujourd'hui.

Au milieu des années 1980, l'ICS était largement utilisé aux États-Unis et ses principes de commandement, de contrôle et de coordination standardisés ont commencé à se répandre à l'échelle internationale.

L'ICS et le contexte canadien

Avant que l'ICS ne devienne la norme au Canada, de nombreux organismes d'intervention canadiens suivaient un modèle de gestion des sites d'urgence (ESM) dans les années 1980. L'ESM répartissait les opérations entre deux sites principaux : le site d'urgence et le centre des opérations d'urgence (COU).

À partir du début des années 1990, l'ICS a gagné en popularité au Canada et est désormais largement adopté par les organismes d'intervention et les gouvernements. Aujourd'hui, la plupart des organismes canadiens sont encouragés à utiliser l'ICS pour leurs postes de commandement des interventions (PCI) et leurs COU, ce qui favorise une structure de commandement cohérente et évolutive lors des incidents.

L'essor du NIMS : un cadre national

À la suite des attentats du 11 septembre aux États-Unis, la nécessité d'une approche unifiée et nationale de la gestion des incidents est apparue clairement. Cela a conduit à l'élaboration du Système national de gestion des incidents (NIMS), qui étend le modèle ICS à un cadre plus large et plus complet.

Le NIMS fournit un langage, des principes et des systèmes opérationnels communs afin d'aider toutes les parties prenantes, des premiers intervenants aux cadres des centres d'opérations d'urgence, à collaborer efficacement. Aux États-Unis, l'adoption du NIMS est obligatoire pour les juridictions locales,

fantastic system when many organizations are managing an event and have specific tactical roles and responsibilities. It's designed to enable effective, efficient incident management by integrating a combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure. However, many believe it is 'the' incident management system as opposed to 'an' incident management system.

While there are some great bones to work with for ICS, it may need some innovation and agility to be tailored to your organization, especially if it is a corporate environment as opposed to a field focused one. Some steps to developing a customized incident management system for a corporate environment are:

1. Business-Specific Risk Identification and Prioritization

Unlike public institutions, corporate environments are exposed to a diverse set of risks influenced by their industry, customer expectations, reliance on digital systems, and even international operations. EMBC specialists are uniquely positioned to conduct hazard and vulnerability assessments that align with these realities, ensuring their IMS reflects the actual threats to operations, from IT failures and regulatory investigations to reputational crises and supply chain breakdowns.

2. Bridging Business Functions for Effective Response

Emergency response in a corporate context is mostly focused on business continuity and therefor must navigate layers of business functions and decision-making hierarchies. A custom IMS allows for integrated response protocols that fit how the business operates. EMBC professionals can help map functional roles, escalation paths, dependencies, and recovery strategies that reflect organizational workflows, not abstract response models.

étatiques et tribales qui reçoivent des fonds fédéraux pour la préparation aux situations d'urgence.

Avec ses initiatives d'extension, l'ICS est un système fantastique lorsque de nombreuses organisations gèrent un événement et ont des rôles et des responsabilités tactiques spécifiques. Il est conçu pour permettre une gestion efficace et efficiente des incidents en intégrant une combinaison d'installations, d'équipements, de personnel, de procédures et de communications fonctionnant au sein d'une structure organisationnelle commune. Cependant, beaucoup considèrent qu'il s'agit du « seul » système de gestion des incidents, par opposition à « un » système de gestion des incidents.

Bien que l'ICS présente de nombreux avantages, il peut nécessiter une certaine innovation et agilité pour être adapté à votre organisation, en particulier s'il s'agit d'un environnement d'entreprise plutôt que d'un environnement axé sur le terrain. Voici quelques étapes pour développer un système de gestion des incidents personnalisé pour un environnement d'entreprise :

1. Identification et hiérarchisation des risques spécifiques à l'entreprise

Contrairement aux institutions publiques, les entreprises sont exposées à divers risques liés à leur secteur d'activité, aux attentes de leurs clients, à leur dépendance aux systèmes numériques et même à leurs opérations internationales. Les spécialistes d'EMBC sont particulièrement bien placés pour mener des évaluations des risques et des vulnérabilités qui tiennent compte de ces réalités, garantissant ainsi que leur IMS reflète les menaces réelles qui pèsent sur leurs opérations, qu'il s'agisse de pannes informatiques, d'enquêtes réglementaires, de crises de réputation ou de ruptures de la chaîne d'approvisionnement.

2. Relier les fonctions opérationnelles pour une réponse efficace

Dans un contexte d'entreprise, les interventions d'urgence sont principalement axées sur la continuité des activités et doivent donc passer par plusieurs niveaux de fonctions opérationnelles et hiérarchies décisionnelles. Un plan de gestion des incidents d'urgence (IMS) personnalisé permet

3. Supporting Leadership with Actionable Intelligence

In a crisis, corporate leaders require swift access to accurate information to guide critical decisions. A business-aligned IMS, developed with business strategy inputs ensures the right data flows to the right people at the right time. Dashboards that focus on roles, functions, recovery time objectives (RTOs), predefined decision thresholds, and real-time situational awareness tools are vital components that support a corporate emergency coordination centre team and leadership.

4. Scalable Solutions for a Shifting Risk Landscape

Today's incident management systems must align with business strategies and key operational outcomes. A customized, IMS allows for scalability without sacrificing relevance. EMBC professionals should ensure the system remains agile, adaptive, and innovative while incorporating lessons learned from exercises or actual incidents into real-time improvements.

5. Aligned to Corporate Governance

Whether it's ISO 22301, CSA Z1600-17, or sector-specific regulations, EMBC specialists know that documentation, traceability, and defensibility are essential. A well-structured internal IMS supports compliance reporting, internal audits, and board-level oversight making it easier for corporations to demonstrate duty of care and due diligence before, during, and after an incident.

6. Culture Meets Compliance: The Power of Working Together

EMBC strategists understand the importance of exercises, training, and cultural readiness. Tailoring an IMS enables stronger alignment with internal communication, cultural values, and existing business processes. Having this alignment increases senior leadership buy-in, promotes accountability, and enhances the maturity

de mettre en place des protocoles d'intervention intégrés adaptés au fonctionnement de l'entreprise. Les professionnels de l'EMBC peuvent aider à définir les rôles fonctionnels, les procédures d'escalade, les dépendances et les stratégies de reprise qui reflètent les flux de travail de l'organisation, et non des modèles d'intervention abstraits.

3. Soutenir le leadership grâce à des renseignements exploitables

En cas de crise, les dirigeants d'entreprise ont besoin d'accéder rapidement à des informations précises pour prendre des décisions cruciales. Un IMS aligné sur l'activité, développé à partir des données stratégiques de l'entreprise, garantit que les bonnes données parviennent aux bonnes personnes au bon moment. Les tableaux de bord axés sur les rôles, les fonctions, les objectifs de temps de récupération (RTO), les seuils de décision prédéfinis et les outils de connaissance de la situation en temps réel sont des éléments essentiels qui soutiennent l'équipe du centre de coordination d'urgence de l'entreprise et ses dirigeants.

4. Des solutions évolutives pour un environnement de risques en mutation

Les systèmes actuels de gestion des incidents doivent s'aligner sur les stratégies commerciales et les principaux résultats opérationnels. Un système IMS personnalisé permet une évolutivité sans sacrifier la pertinence. Les professionnels de l'EMBC doivent veiller à ce que le système reste agile, adaptatif et innovant, tout en intégrant les enseignements tirés des exercices ou des incidents réels dans des améliorations en temps réel.

5. Conformité à la gouvernance d'entreprise

Qu'il s'agisse de la norme ISO 22301, de la norme CSA Z1600-17 ou de réglementations spécifiques à un secteur, les spécialistes EMBC savent que la documentation, la traçabilité et la défendabilité sont essentielles. Un système de gestion intégré (IMS) interne bien structuré facilite la production de rapports de conformité, les audits internes et la supervision au niveau du conseil d'administration, ce qui permet aux entreprises de démontrer plus facilement leur devoir de diligence avant, pendant et après un incident.

of the organization's emergency management and business continuity culture, something the "one-size fits all" systems struggle to achieve.

In today's world, where we are constantly evolving through transformation initiatives and digital enhancements, emergency management and business continuity professionals play a far more strategic role than simply responding to crises. EMBC specialists are the architects of resilience, bridging the gap between day-to-day operations and high-impact disruptions. Too often, organizations rely on generic, pre-packaged solutions that may look comprehensive on paper but fail to reflect the unique realities of their business. Many organizations recognized this challenge when they activated their business continuity and emergency response plans and teams during COVID. These one-size-fits-all approaches create the illusion of preparedness and collaboration without addressing the specific vulnerabilities and strengths that exist within each organization.

By developing customized incident management systems tailored to an organization's culture, operations, and real-world risks, EMBC professionals move away from reactive responders to proactive strategists, enhancing an organization's resilience. Custom-fit plans and systems ensure that response protocols align with how people work, communicate, and make decisions in practice, not just how they are expected to be based on a single methodology. This level of alignment fosters

6. Quand culture rime avec conformité : le pouvoir du travail collaboratif

Les stratèges EMBC comprennent l'importance des exercices, de la formation et de la préparation culturelle. L'adaptation d'un IMS permet un meilleur alignement avec la communication interne, les valeurs culturelles et les processus opérationnels existants. Cet alignement renforce l'adhésion des cadres supérieurs, favorise la responsabilisation et améliore la maturité de la culture de gestion des urgences et de continuité des activités de l'organisation, ce que les systèmes « universels » ont du mal à réaliser.

Dans le monde actuel, où nous évoluons constamment grâce à des initiatives de transformation et des améliorations numériques, les professionnels de la gestion des urgences et de la continuité des activités jouent un rôle bien plus stratégique que la simple gestion des crises. Les spécialistes EMBC sont les architectes de la résilience, comblant le fossé entre les opérations quotidiennes et les perturbations à fort impact. Trop souvent, les organisations s'appuient sur des solutions génériques et toutes faites qui peuvent sembler complètes sur le papier, mais qui ne reflètent pas les réalités propres à leur activité. De nombreuses organisations ont pris conscience de ce défi lorsqu'elles ont activé leurs plans et équipes de continuité des activités et d'intervention d'urgence pendant la pandémie de COVID. Ces approches uniformisées créent l'illusion d'une préparation et d'une collaboration sans tenir compte des vulnérabilités et des forces spécifiques qui existent au sein de chaque organisation.

En développant des systèmes de gestion des incidents personnalisés, adaptés à la culture, aux opérations et aux risques réels d'une organisation, les professionnels de l'EMBC passent du statut d'intervenants réactifs à celui de stratèges proactifs, renforçant ainsi la résilience des organisations. Des plans et des systèmes sur mesure garantissent que les protocoles d'intervention sont adaptés à la manière dont les personnes travaillent, communiquent et prennent des décisions dans la pratique, et non pas seulement à la manière dont elles sont censées le faire selon une méthodologie unique. Ce niveau d'alignement favorise la collaboration, la confiance, accélère la reprise et réduit le risque de défaillances en cascade en cas de perturbation.

collaboration, confidence, speeds recovery, and reduces the likelihood of cascading failures when disruptions occur.

Ultimately, resilience is not built through templated forms, binders on a shelf, or compliance checklists, it is cultivated through systems and teams that grow from within the organization. When emergency management and business continuity are embedded into everyday decision-making, they strengthen trust, empower leaders and staff, and prepare teams to act with clarity under pressure. This change represents more than readiness; it institutionalizes resilience as a defining characteristic of the organization. Ω

En fin de compte, la résilience ne se construit pas à l'aide de formulaires types, de classeurs rangés sur une étagère ou de listes de contrôle de conformité, mais grâce à des systèmes et des équipes qui se développent au sein même de l'organisation. Lorsque la gestion des urgences et la continuité des activités sont intégrées dans la prise de décision quotidienne, elles renforcent la confiance, responsabilisent les dirigeants et le personnel, et préparent les équipes à agir avec clarté sous pression. Ce changement représente plus qu'une simple préparation ; il institutionnalise la résilience en tant que caractéristique déterminante de l'organisation. Ω

ABOUT THE AUTHOR

Claire Mechan, BA, CBCP, MADEM

Claire is a highly experienced business continuity and emergency management strategist and leader with expertise across various sectors, including education and government. She holds the Certified Business Continuity Professional (CBCP) designation, a Master of Arts in Disaster and Emergency Management (MADEM) from Royal Roads University (2013), and a Bachelor of Arts in Criminology from Vancouver Island University (2006). Claire has been actively involved in emergency management and business continuity since 2012.

Claire is the Owner and Primary Consultant of AILM Resiliency Consulting Agency. She is also the Manager of the Emergency Management and Business Continuity department at the Northern Alberta Institute of Technology (NAIT), where she is also the Director of the Emergency Coordination Centre. Claire has led transformative initiatives at NAIT, including steering NAIT's COVID-19 response and recovery as Director of the Coordinated Response Team. Since 2015, she has also been a dedicated instructor in NAIT's Disaster and Emergency Management academic program.

Claire is deeply committed to empowering women in her field, volunteering with the Mentor for Women in Business Continuity Management program through the DRII Foundation. She also serves on the CSA Group technical committee for emergency and continuity management, where she contributed to the development of the CSA Z1600-17 standard. A member of IAEM, DRI Canada, and BCI, Claire continues to advance resilience and leadership in the business continuity and emergency management professions.

À PROPOS DE L'AUTEUR

Claire Mécan, BA, CBCP, MADEM

Claire est une stratège et une leader très expérimentée en matière de continuité des activités et de gestion des urgences, possédant une expertise dans divers secteurs, notamment l'éducation et le gouvernement. Elle est titulaire du titre de Certified Business Continuity Professional (CBCP), d'une maîtrise ès arts en gestion des catastrophes et des urgences (MADEM) de l'Université Royal Roads (2013) et d'un baccalauréat ès arts en criminologie de l'Université de l'île de Vancouver (2006). Claire s'implique activement dans la gestion des urgences et la continuité des affaires depuis 2012.

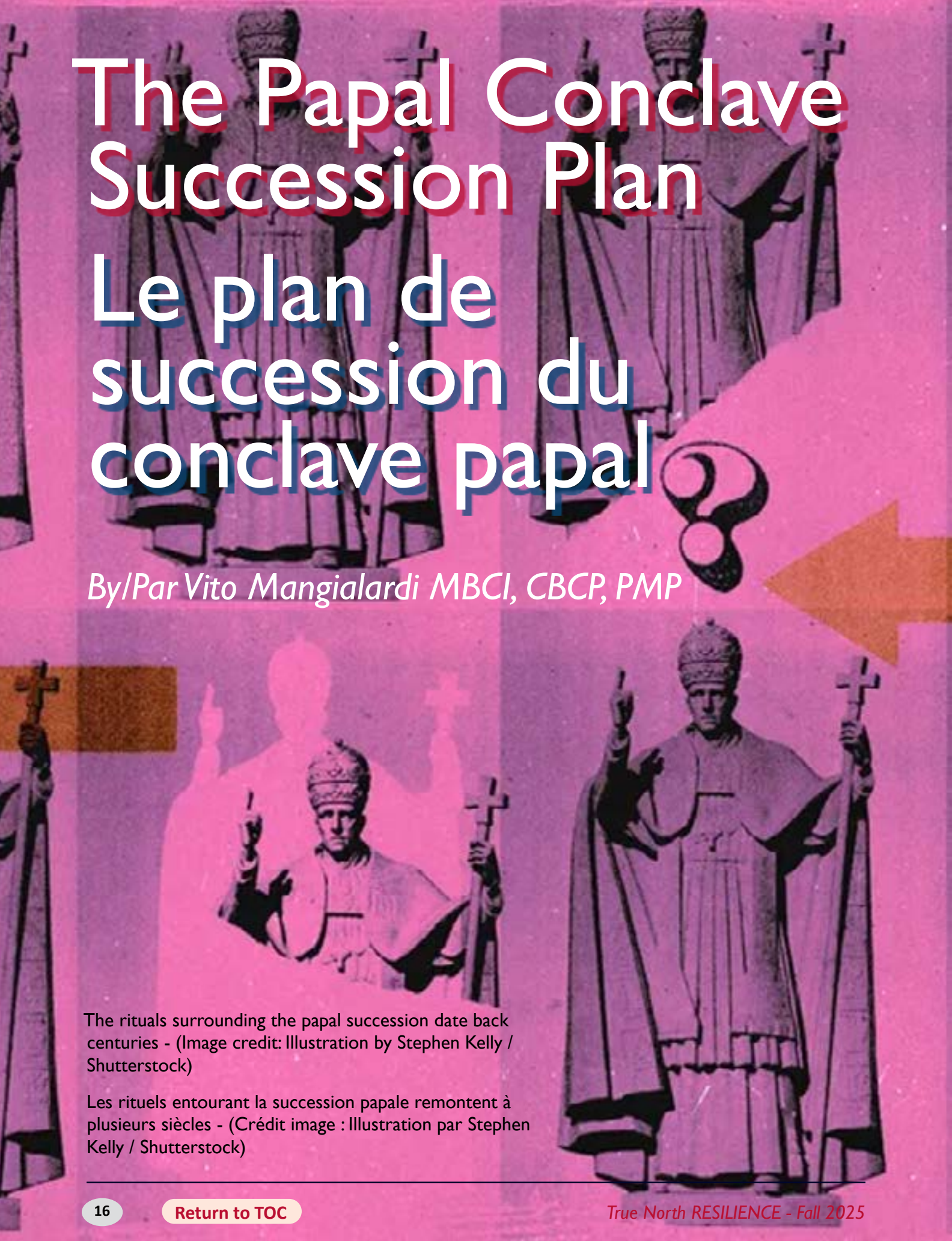
Claire est la propriétaire et consultante principale de l'agence de conseil en résilience AILM. Elle est également gestionnaire du département de gestion des urgences et de continuité des activités du Northern Alberta Institute of Technology (NAIT), où elle est également directrice du Centre de coordination des urgences. Claire a dirigé des initiatives de transformation au NAIT, notamment en dirigeant la réponse et le rétablissement du NAIT face à la COVID-19 en tant que directrice de l'équipe de réponse coordonnée. Depuis 2015, elle est également instructrice dédiée au programme académique de gestion des catastrophes et des urgences du NAIT.

Claire est profondément engagée dans l'autonomisation des femmes dans son domaine, en faisant du bénévolat auprès du programme Mentor for Women in Business Continuity Management par l'intermédiaire de la Fondation DRII. Elle siège également au comité technique du Groupe CSA pour la gestion des urgences et de la continuité, où elle a contribué à l'élaboration de la norme CSA Z1600-17. Membre de l'IAEM, de DRI Canada et de BCI, Claire continue de faire progresser la résilience et le leadership dans les métiers de la continuité des activités et de la gestion des urgences.

The Papal Conclave Succession Plan

Le plan de succession du conclave papal

By/Par Vito Mangialardi MBCI, CBCP, PMP



The rituals surrounding the papal succession date back centuries - (Image credit: Illustration by Stephen Kelly / Shutterstock)

Les rituels entourant la succession papale remontent à plusieurs siècles - (Crédit image : Illustration par Stephen Kelly / Shutterstock)

Succession Planning: Lessons from the Papal Conclave for Business Continuity

Preface:

This article was originally authored by Vito Mangialardi and first published in the **DRIE Toronto Digest magazine in 2013**, during a significant moment in modern Church history—the election of Pope Francis as the 266th pope on March 13, 2013. As the first Latin American and Jesuit pope, his election marked a turning point not only for the Roman Catholic Church but also for how we understand leadership transitions in large, complex organizations.

The piece draws a compelling parallel between the papal conclave, one of the oldest succession planning models in the world, and the critical need for structured succession planning in business continuity management (BCM). Although more than a decade has passed since its original publication, the insights offered here remain highly relevant in today's fast-evolving business environment, where organizations continue to face mounting pressures around talent retention, leadership gaps, and operational resilience.

This information is shared to reinforce the ongoing importance of succession planning as a cornerstone of organizational resilience and continuity. Whether in religious institutions or modern enterprises, the principles of foresight, preparedness, and leadership continuity are timeless.

Introduction

In light of the current papal conclave, it's a timely opportunity to reflect on the importance of **succession planning**, especially for roles critical to organizational continuity. The **conclave**, the centuries-old process by which the Catholic Church selects a new Pope (its de facto CEO), is one of the longest-standing succession models. This ancient process is designed to ensure seamless leadership transition and avoid operational disruption—principles that modern businesses would do well to emulate.

Just as the Church faces risk without a Pope, any business lacking a plan for leadership succession leaves itself vulnerable to instability and potential failure.

Planification de la succession : Les leçons du conclave papal pour la continuité des activités

Préface :

Cet article a été rédigé à l'origine par Vito Mangialardi et publié pour la première fois dans le magazine DRIE Toronto Digest en 2013, à un moment important de l'histoire de l'Église moderne - l'élection du pape François en tant que 266e pape le 13 mars 2013. Premier pape latino-américain et jésuite, son élection a marqué un tournant non seulement pour l'Église catholique romaine, mais aussi pour la façon dont nous comprenons les transitions de leadership dans les grandes organisations complexes.

L'article établit un parallèle convaincant entre le conclave papal, l'un des plus anciens modèles de planification de la succession au monde, et le besoin critique d'une planification structurée de la succession dans le cadre de la gestion de la continuité des activités (BCM). Bien que plus d'une décennie se soit écoulée depuis sa publication initiale, les idées proposées ici restent très pertinentes dans l'environnement commercial actuel en évolution rapide, où les organisations continuent à faire face à des pressions croissantes en matière de rétention des talents, de lacunes en matière de leadership et de résilience opérationnelle.

Ces informations sont partagées afin de renforcer l'importance de la planification de la succession en tant que pierre angulaire de la résilience et de la continuité des organisations. Qu'il s'agisse d'institutions religieuses ou d'entreprises modernes, les principes de prévoyance, de préparation et de continuité du leadership sont intemporels.

Introduction

Le conclave papal actuel est l'occasion de réfléchir à l'importance de la planification de la succession, en particulier pour les fonctions essentielles à la continuité de l'organisation. Le conclave, processus séculaire par lequel l'Église catholique sélectionne un nouveau pape (son PDG de facto), est l'un des modèles de succession les plus anciens. Ce processus ancien est conçu pour assurer une transition transparente de la direction et éviter les ➤

What Is Succession Planning?

According to **Wikipedia**, succession planning is "a process for identifying and developing internal people with the potential to fill key leadership positions." This has direct implications for **business continuity,** as leadership voids can lead to operational, financial, and reputational consequences.

Historically, succession planning has focused on top-tier executives, VPs, and C-level leaders. However, modern experience suggests the need to broaden this focus to include **mid-level and emerging leaders**, who represent the organization's future and help maintain stability during change.

The Role of Business Continuity Management (BCM)

Business Continuity Management is a proactive process that identifies operational risks and implements strategies to mitigate them. One of the most significant—and often overlooked—risks is the **loss of key personnel.**

Effective BCM recognizes that people are among the most critical assets of any organization. Today's businesses face compounding pressures:

- Global operations
- 24/7 service demands
- Technology and automation dependencies
- High customer expectations
- Increased burnout and turnover
- Retirement of experienced professionals

These factors all contribute to a **widening resource and talent gap**, posing serious risks if not properly managed.

Why Succession Planning Matters

Ensuring adequate staffing during disruption is vital to maintaining service delivery and financial performance. When conducting a **Business Impact Analysis** (BIA) or **Risk Assessment**, it's essential to consider not only systems and data, but also the **people** who keep them running.

perturbations opérationnelles – des principes dont les entreprises modernes feraient bien de s'inspirer.

Tout comme l'Église est exposée à des risques en l'absence d'un pape, toute entreprise qui ne dispose pas d'un plan de succession de ses dirigeants se rend vulnérable à l'instabilité et à l'échec potentiel.

Qu'est-ce que la planification de la relève ?

Selon **Wikipédia**, la planification de la relève est "un processus d'identification et de développement des personnes internes susceptibles d'occuper des postes de direction clés". Cela a des conséquences directes sur la continuité de l'activité, car des postes de direction vacants peuvent avoir des conséquences opérationnelles, financières et sur la réputation de l'entreprise.

Historiquement, la planification des successions s'est concentrée sur les cadres supérieurs, les vice-présidents et les dirigeants de haut niveau. Toutefois, l'expérience moderne montre qu'il est nécessaire d'élargir ce champ d'action aux **dirigeants de niveau intermédiaire et émergents**, qui représentent l'avenir de l'organisation et contribuent à maintenir la stabilité pendant les périodes de changement.

Le rôle de la gestion de la continuité des activités (BCM)

La gestion de la continuité des activités est un processus proactif qui identifie les risques opérationnels et met en œuvre des stratégies pour les atténuer. L'un des risques les plus importants – et souvent négligé – est **la perte de personnel clé**.

Une gestion efficace de la continuité des activités reconnaît que les personnes font partie des actifs les plus critiques de toute organisation. Les entreprises d'aujourd'hui sont confrontées à des pressions croissantes :

- Opérations mondiales
- Exigences de service 24 heures sur 24, 7 jours sur 7
- Dépendance à l'égard de la technologie et de l'automatisation
- Attentes élevées des clients
- Augmentation de l'épuisement professionnel et de la rotation du personnel
- Départ à la retraite de professionnels expérimentés

Tous ces facteurs contribuent à **creuser le fossé entre les ressources et les talents**, ce qui pose de sérieux

Key positions and staff with unique skill sets are often irreplaceable in the short term. Without backup plans, these roles can become **single points of failure**. A strong continuity plan should identify both **primary** and **alternate** personnel for each business-critical function.

Four Steps to Integrate Succession Planning into Continuity Strategy

Step 1: Identify Critical Positions

Start by identifying which roles and functions are **mission-critical**—those that must be maintained to meet legal, regulatory, or customer obligations. Use insights from your **BIA** to define the minimum staffing required and assess needs over the short and long term. Note that critical roles can exist at **any level,** not just executive.

Step 2: Define Position Capabilities

For each identified role, create an inventory of **required skills, knowledge, and experience**. This may already be documented in job descriptions. Define performance metrics to help evaluate both current and potential future candidates for succession or backup planning.

Step 3: Develop Succession Strategies

Once roles and capabilities are defined, identify internal or external candidates who match the required profiles. Use tools such as:

- Internal development and training
- Professional networking
- Recruitment platforms and social media
- External search firms

In the papal conclave model, only Cardinals are eligible to be considered, ensuring that all candidates are **pre-vetted** and **qualified**. This focused

risques s'ils ne sont pas correctement gérés.

L'importance de la planification des successions

Garantir une dotation en personnel adéquate en cas d'interruption est essentiel pour maintenir la prestation de services et les performances financières. Lors d'une **analyse d'impact sur l'activité (BIA) ou d'une évaluation des risques**, il est essentiel de prendre en compte non seulement les systèmes et les données, mais aussi les personnes qui les font fonctionner.

Les postes clés et le personnel possédant des compétences uniques sont souvent irremplaçables à court terme. En l'absence de plans de secours, ces fonctions peuvent **devenir des points de défaillance uniques**. Un plan de continuité solide doit identifier le personnel principal et le personnel de remplacement pour chaque fonction critique de l'entreprise.

Quatre étapes pour intégrer la planification des successions dans la stratégie de continuité

Étape 1 : Identifier les postes critiques

Commencez par identifier les rôles et les fonctions critiques, c'est-à-dire ceux qui doivent être maintenus pour respecter les obligations légales, réglementaires ou celles des clients. Utilisez les résultats de votre **BIA** pour définir les effectifs minimums requis et évaluer les besoins à court et à long terme. Notez que les rôles critiques peuvent exister à n'importe quel niveau, et pas seulement au niveau de la direction.

Étape 2 : Définir les capacités du poste

Pour chaque rôle identifié, dressez un inventaire des compétences, des connaissances et de l'expérience requises. Il se peut que ces éléments soient déjà documentés dans les descriptions de poste. Définir des indicateurs de performance pour aider à évaluer les candidats actuels et les futurs candidats potentiels dans le cadre de la planification de la succession ou de la relève.

Étape 3 : Élaborer des stratégies de succession

Une fois les rôles et les capacités définis, identifiez les candidats internes ou externes qui correspondent aux profils requis. Utilisez des outils tels que

- le développement et la formation internes
- le réseautage professionnel
- les plateformes de recrutement et les médias sociaux
- les cabinets de recherche externes.

approach has enabled smooth leadership transitions for centuries.

Step 4: Create a Succession Action Plan

With strategies in place, document a formal **Succession Action Plan**. This may range from a simple plan (for common roles) to a detailed roadmap (for niche skills or senior leadership). Include clear **timelines, responsibilities, and review checkpoints** to keep the plan on track.

Embedding Succession Planning into Business Continuity Plans

As part of your **Business Continuity Plan** (BCP), identify **key roles and their backups**. Just as important is **training and exercising the plan** to:

- Validate its **operational effectiveness**
- Ensure staff are **prepared and confident** in their roles during a disruption

Even planned absences—or non-BCP-related resignations—can introduce risk. Proactively developing succession plans within your continuity framework enhances your organization's ability to withstand staffing-related shocks.

Conclusion: A Safeguard for the Future

Succession planning is more than an HR task, it's a **strategic imperative** and a core element of organizational resilience. Whether dealing with an emergency or a leadership transition, having the right people in place ensures that your business continues to thrive under pressure.

By adopting practices inspired by enduring traditions like the papal conclave, your organization can be better prepared, more agile, and ultimately more **resilient** in the face of change. Ω

Vito Mangialardi *is a Senior Business Continuity Management (BCM) Leader with more than 25 years of achievement delivering Business Continuity, Disaster Recovery Planning, Emergency, and Incident Management Programs in private and public sectors.*

Dans le modèle du conclave papal, seuls les cardinaux peuvent être pris en considération, ce qui garantit que tous les candidats sont présélectionnés et qualifiés. Cette approche ciblée a permis des transitions de leadership en douceur pendant des siècles.

Étape 4 : Créer un plan d'action pour la succession

Une fois les stratégies en place, établissez un plan d'action formel pour la succession. Il peut s'agir d'un plan simple (pour les fonctions courantes) ou d'une feuille de route détaillée (pour les compétences spécialisées ou les cadres supérieurs). Prévoyez des échéances, des responsabilités et des points de contrôle clairs afin de maintenir le plan sur la bonne voie.

Plans de continuité des activités

Dans le cadre de votre plan de continuité des activités (PCA), identifiez les rôles clés et leurs sauvegardes. Il est tout aussi important de former et d'exercer le plan pour :

- valider son efficacité opérationnelle
- S'assurer que le personnel est préparé et confiant dans son rôle en cas d'interruption.

Même les absences planifiées - ou les démissions non liées au BCP - peuvent entraîner des risques. L'élaboration proactive de plans de succession dans votre cadre de continuité renforce la capacité de votre organisation à résister aux chocs liés au personnel.

Conclusion : Un garde-fou pour l'avenir

La planification de la relève est plus qu'une tâche RH, c'est un impératif stratégique et un élément central de la résilience organisationnelle. Qu'il s'agisse d'une situation d'urgence ou d'une transition de direction, le fait de disposer des bonnes personnes permet à votre entreprise de continuer à prospérer sous la pression.

En adoptant des pratiques inspirées de traditions durables telles que le conclave papal, votre organisation peut être mieux préparée, plus agile et, en fin de compte, plus résiliente face au changement. Ω

Vito Mangialardi *est un leader senior de la gestion de la continuité des activités (BCM) avec plus de 25 ans de réalisations dans la prestation de programmes de continuité des activités, de planification de la reprise après sinistre, d'urgence et de gestion des incidents dans les secteurs privé et public.*

An Experts' Impression

L'Impression d'un expert

This feature has quickly become very popular with readers of True North Resilience, and to be honest, one of our favorite parts of putting the magazine together.

- Determining the question to pose
- Finding SMEs to provide their insights and then seeing things through a different lens from Resilience.

Yeah, we're nerds, but we have a lot of fun! 😉

AI has become almost like a third hand for many folks in the last year, many organizations are insisting that their staff adopt an AI tool and use it to enhance, or increase, their work-product. In all reality, it's still in its infancy and needs significant governance to avoid gaping security holes in your organization. Taking a course on AI security and governance seems almost like it should be part of the on-boarding process for organizations so new hires understand your policies and procedures.

If you would like to be added to the pool of Experts for future editions of this feature, please email your credentials (your LinkedIn profile works well) to editors@dri.ca and we'll reach out when we have a question that falls into your wheelhouse, or sooner if it's a question like this issue that is far ranging across industries.

Thanks! **- GAT**

Cette rubrique est rapidement devenue très populaire auprès des lecteurs de True North Resilience, et pour être honnête, c'est l'une de nos parties préférées dans la réalisation du magazine.

- Déterminer la question à poser
- Trouver des experts pour nous faire part de leurs idées, puis voir les choses sous un angle différent de celui de Resilience.

Oui, nous sommes des geeks, mais nous nous amusons beaucoup ! 😉

Au cours de l'année dernière, l'IA est devenue presque comme une troisième main pour beaucoup de gens. De nombreuses organisations insistent pour que leur personnel adopte un outil d'IA et l'utilise pour améliorer ou augmenter leur rendement au travail. En réalité, cette technologie en est encore à ses balbutiements et nécessite une gouvernance importante pour éviter des failles de sécurité béantes dans votre organisation. Suivre une formation sur la sécurité et la gouvernance de l'IA semble presque indispensable dans le processus d'intégration des nouvelles recrues, afin qu'elles comprennent vos politiques et procédures.

Si vous souhaitez rejoindre le groupe d'experts pour les prochaines éditions de cette rubrique, veuillez envoyer vos références (votre profil LinkedIn convient parfaitement) à editors@dri.ca. Nous vous contacterons lorsque nous aurons une question relevant de votre domaine de compétence, ou plus tôt s'il s'agit d'une question comme celle-ci, qui concerne de nombreux secteurs.

Merci ! **- GAT** ➤

This issue's question is:

"WITH THE RAPID ADVANCEMENT AND ADOPTION OF ARTIFICIAL INTELLIGENCE ACROSS ALL SECTORS OF BUSINESS, HOW DO YOU FORESEE AI RESHAPING YOUR INDUSTRY IN THE NEXT 3 TO 5 YEARS, IN TERMS OF INNOVATION, WORKFORCE, AND COMPETITIVE ADVANTAGE?"

ADDITIONAL CONSIDERATIONS:

- **STRATEGIC:** "WHAT ARE THE MOST PROFOUND TRANSFORMATIONS AI IS DRIVING IN YOUR INDUSTRY, AND HOW SHOULD ORGANIZATIONS POSITION THEMSELVES TO THRIVE?"
- **ETHICAL/DISRUPTIVE:** "AI IS DISRUPTING ESTABLISHED NORMS. WHAT ETHICAL, OPERATIONAL, OR SOCIETAL CHALLENGES DO YOU BELIEVE YOUR INDUSTRY MUST URGENTLY ADDRESS AS AI BECOMES PERVASIVE?"
- **LEADERSHIP-FOCUSED:** "AS A LEADER IN YOUR FIELD, WHAT'S THE SINGLE MOST CRITICAL AI-RELATED OPPORTUNITY, OR RISK, YOU THINK YOUR INDUSTRY WILL FACE BY 2030?"

La question abordée dans ce numéro est la suivante :

« AVEC LES PROGRÈS RAPIDES ET L'ADOPTION GÉNÉRALISÉE DE L'INTELLIGENCE ARTIFICIELLE DANS TOUS LES SECTEURS D'ACTIVITÉ, COMMENT ENVISAGEZ-VOUS LA TRANSFORMATION DE VOTRE SECTEUR AU COURS DES 3 À 5 PROCHAINES ANNÉES EN TERMES D'INNOVATION, DE MAIN-D'ŒUVRE ET D'AVANTAGE CONCURRENTIEL ? »

CONSIDÉRATIONS SUPPLÉMENTAIRES :

- **STRATÉGIQUE :** « QUELLES SONT LES TRANSFORMATIONS LES PLUS PROFONDES INDUITES PAR L'IA DANS VOTRE SECTEUR, ET COMMENT LES ORGANISATIONS DOIVENT-ELLES SE POSITIONNER POUR PROSPÉRER ? »
- **ÉTHIQUE/PERTURBATRICE :** « L'IA BOULEVERSE LES NORMES ÉTABLIES. SELON VOUS, QUELS SONT LES DÉFIS ÉTHIQUES, OPÉRATIONNELS OU SOCIÉTAUX AUXQUELS VOTRE SECTEUR DOIT S'ATTAQUER DE TOUTE URGENCE À MESURE QUE L'IA SE GÉNÉRALISE ? »
- **AXÉE SUR LE LEADERSHIP :** « EN TANT QUE LEADER DANS VOTRE DOMAINE, QUELLE EST, SELON VOUS, L'OPPORTUNITÉ OU LE RISQUE LE PLUS IMPORTANT LIÉ À L'IA AUQUEL VOTRE SECTEUR SERA CONFRONTÉ D'ICI 2030 ? »

An Expert's Impression

Aidan Firlotte

AI (artificial intelligence) has been as to computer science as the calculator to the field of mathematics, and the future will indicate this impact; through change in human tasks in work force, change in the kind of taught language, and change information accessible by the masses, the field of computer science has been moved forward by AI.

In an AI powered workplace there will be less need for menial tasks like code commenting and minor debugging leaving high concept run time complexity or high-level problems for human coders, thus we will see more specialist in fields that work directly with AI.

Language will change, AI still does not grasp large problems we will see functions working more independently and less high-level programming languages that are difficult for AI like Assembly, but more efficient low level programming languages such as python or java since AI will introduce these to the public.

The average joe now has access to AI, which will be the best code breaker in the world, and it will touch the security world. Cyber security workers will now have to prepare for higher levels of security; there will be no more low-level hacking blocks in the world of AI: in an AI world cyber security employees will be some of the more valued workers in a company.

The world has changed forever, and our skills must change with these new advancements whether through training for more specialised fields; familiarizing with AI friendly languages and its limitations in languages; and being prepared for high level data breaches and all contingencies.

L'impression d'un expert

Aidan Firlotte

L'intelligence artificielle (IA) a été à l'informatique ce que la calculatrice a été aux mathématiques, et l'avenir montrera l'ampleur de cet impact. Grâce à l'évolution des tâches humaines dans le monde du travail, à l'évolution des langages enseignés et à l'évolution des informations accessibles au grand public, l'informatique a été propulsée vers l'avant par l'IA.

Dans un environnement de travail alimenté par l'IA, les tâches subalternes telles que les commentaires de code et le débogage mineur seront moins nécessaires, laissant aux codeurs humains les problèmes complexes liés à l'exécution ou les problèmes de haut niveau. Nous verrons donc apparaître davantage de spécialistes dans les domaines qui travaillent directement avec l'IA.

Le langage va changer, l'IA ne saisit toujours pas les problèmes complexes. Nous verrons des fonctions fonctionner de manière plus indépendante et moins de langages de programmation de haut niveau difficiles pour l'IA, comme l'Assembly, mais davantage de langages de programmation de bas niveau plus efficaces, tels que Python ou Java, car l'IA les introduira au grand public.

Le citoyen lambda a désormais accès à l'IA, qui sera le meilleur décrypteur de code au monde, et cela aura des répercussions sur le monde de la sécurité. Les professionnels de la cybersécurité devront désormais se préparer à des niveaux de sécurité plus élevés ; il n'y aura plus de blocs de piratage de bas niveau dans le monde de l'IA : dans un monde dominé par l'IA, les employés chargés de la cybersécurité feront partie des travailleurs les plus précieux d'une entreprise.

Le monde a changé pour toujours, et nos compétences doivent évoluer avec ces nouvelles avancées, que ce soit par le biais de formations dans des domaines plus spécialisés, en se familiarisant avec les langages adaptés à l'IA et leurs limites, ou en se préparant à des violations de données de haut niveau et à toutes les éventualités. ➤

Kristin Nelles

As an intermediate teacher, I'm just starting to see AI used in education. For students, its role is minimal and often associated with cheating, as Boards focus on banning access rather than teaching ethical AI use. Meanwhile, educators are encouraged to use AI for lesson planning, worksheets, and report card comments, with promises of saving time and producing quality resources. I expect a push to further cut costs by using AI to replace textbooks and other materials.

However, there are concerns. Over-reliance on AI could erode the quality of lessons and weaken essential teaching skills. AI-generated content is not flawless; for example, a worksheet I created had a multiple-choice question where every answer was correct—confusing for learners. Dependence on AI risks reducing opportunities for educators and students to develop critical thinking and problem-solving skills. Moreover, AI can only replicate existing ideas, which could stifle creativity and innovation in students.

Moving forward, education systems must stop blocking AI and instead focus on teaching responsible use. With thoughtful guidance, AI can enhance teaching, save resources, and support student learning—but it requires proactive education for both teachers and students.

Robin Whyte

AI is reshaping industries in ways that go far beyond efficiency — it's opening new doors for accessibility and inclusion. As an accessibility consultant and a person with a disability, I see AI as both a transformative opportunity and a responsibility.

Kristin Nelles

En tant qu'enseignante de niveau intermédiaire, je commence tout juste à voir l'IA utilisée dans l'éducation. Pour les élèves, son rôle est minime et souvent associé à la tricherie, car les commissions scolaires se concentrent sur l'interdiction de l'accès plutôt que sur l'enseignement d'une utilisation éthique de l'IA. Parallèlement, les enseignants sont encouragés à utiliser l'IA pour la planification des cours, les feuilles de travail et les commentaires sur les bulletins scolaires, avec la promesse de gagner du temps et de produire des ressources de qualité. Je m'attends à ce que l'on cherche à réduire davantage les coûts en utilisant l'IA pour remplacer les manuels scolaires et autres supports pédagogiques.

Cependant, cela soulève certaines inquiétudes. Une dépendance excessive à l'IA pourrait nuire à la qualité des cours et affaiblir les compétences pédagogiques essentielles. Le contenu généré par l'IA n'est pas infaillible ; par exemple, une fiche de travail que j'ai créée comportait une question à choix multiples où toutes les réponses étaient correctes, ce qui a semé la confusion chez les apprenants. La dépendance à l'IA risque de réduire les possibilités pour les enseignants et les élèves de développer leur esprit critique et leurs compétences en matière de résolution de problèmes. De plus, l'IA ne peut que reproduire des idées existantes, ce qui pourrait étouffer la créativité et l'innovation chez les élèves.

À l'avenir, les systèmes éducatifs doivent cesser de bloquer l'IA et se concentrer plutôt sur l'enseignement d'une utilisation responsable. Avec des conseils avisés, l'IA peut améliorer l'enseignement, économiser des ressources et soutenir l'apprentissage des élèves, mais cela nécessite une éducation proactive tant pour les enseignants que pour les élèves.

Robin Whyte

L'IA transforme les industries bien au-delà de l'efficacité : elle ouvre de nouvelles perspectives en matière d'accessibilité et d'inclusion. En tant que consultant en accessibilité et personne handicapée, je considère l'IA à la fois comme une opportunité de transformation et une responsabilité.

Dans le secteur du tourisme et de l'hôtellerie, l'IA permet déjà de mettre en place des plateformes

In the tourism and hospitality sector, AI is already enabling smarter booking platforms, real-time accessibility information, and personalized recommendations for travelers with diverse needs. In broader workplaces, tools like AI-driven captioning, adaptive communication aids, and predictive accessibility checks are helping to remove barriers before they arise.

This shift means organizations must evolve – not just in technology, but in mindset. AI can't be treated as a "one size fits all" solution. To thrive, leaders must prioritize inclusive design, ethical data use, and collaboration with people who have lived experience of disability.

Looking ahead, the most critical challenge is trust: ensuring AI advances don't deepen inequalities but instead make society more accessible, transparent, and equitable. By 2030, the true competitive advantage will lie with organizations that use AI not only to innovate, but to include.

de réservation plus intelligentes, de fournir des informations en temps réel sur l'accessibilité et de proposer des recommandations personnalisées aux voyageurs ayant des besoins divers. Dans les lieux de travail au sens large, des outils tels que le sous-titrage basé sur l'IA, les aides à la communication adaptatives et les contrôles prédictifs d'accessibilité contribuent à éliminer les obstacles avant qu'ils ne surviennent.

Cette évolution implique que les organisations doivent changer, non seulement sur le plan technologique, mais aussi dans leur état d'esprit. L'IA ne peut pas être considérée comme une solution « universelle ». Pour prospérer, les dirigeants doivent donner la priorité à la conception inclusive, à l'utilisation éthique des données et à la collaboration avec des personnes ayant une expérience vécue du handicap.

À l'avenir, le défi le plus important sera celui de la confiance : veiller à ce que les progrès de l'IA ne creusent pas les inégalités, mais rendent au contraire la société plus accessible, plus transparente et plus équitable. D'ici 2030, le véritable avantage concurrentiel reviendra aux organisations qui utilisent l'IA non seulement pour innover, mais aussi pour inclure.

Nancy Holloway-White

The Government of Canada defines Artificial intelligence (AI) as "…where a computer performs a task that typically requires human intelligence, such as reasoning or learning. AI models can solve problems, learn from experience, understand language and interpret visual scenes."[1]

AI has the potential to transform banking, evolving from manual, rules-based systems toward adaptive models. AI promises efficiency and insight at scale, but also introduces new risks around fairness, trust, and compliance.

A real opportunity for AI is to enhance fraud detection and customer experience in Canadian banking. Instead of the traditional means of writing rules to react to known and human-predicted risks, proactive systems can work through volumes of data greater than we could to date to identify hidden patterns and anomalies with the intention of staying ahead (or at least keeping pace) with fraudsters. AI could improve interactions and remove repetitive pain points in the customer service field, and if implemented well, potentially enable more personalized service.

In the strategy space, AI models are subject to the biases and assumptions of the humans who developed them. As the performance and fairness of AI models learns on the accuracy and diversity of its subject data, banks need to take care that data is precise and representative of the targeted population. Financial services institutions will need to align their implementation of AI systems with their existing ethics and bias practices.

AI will change – not replace – the banking workforce. Repetitive coding and administrative tasks could be reduced, resulting in more rewarding work, such as problem-solving, and AI oversight. However, insights from a TD Bank Group survey reveals while many Canadian workers see AI as a helpful tool, they lack the training and support needed

Nancy Nancy Holloway-White

Le gouvernement du Canada définit l'intelligence artificielle (IA) comme « [...] une technologie qui permet à un ordinateur d'effectuer une tâche qui nécessite généralement l'intelligence humaine, comme le raisonnement ou l'apprentissage. Les modèles d'IA peuvent résoudre des problèmes, apprendre de l'expérience, comprendre le langage et interpréter des scènes visuelles. »[1]

L'IA a le potentiel de transformer le secteur bancaire, en faisant évoluer les systèmes manuels basés sur des règles vers des modèles adaptatifs. L'IA promet efficacité et perspicacité à grande échelle, mais elle introduit également de nouveaux risques en matière d'équité, de confiance et de conformité.

L'IA offre une réelle opportunité d'améliorer la détection des fraudes et l'expérience client dans le secteur bancaire canadien. Au lieu des moyens traditionnels consistant à rédiger des règles pour réagir aux risques connus et prévus par l'homme, les systèmes proactifs peuvent traiter des volumes de données plus importants que ce que nous pouvions faire jusqu'à présent afin d'identifier des schémas cachés et des anomalies dans le but de garder une longueur d'avance (ou au moins de suivre le rythme) sur les fraudeurs. L'IA pourrait améliorer les interactions et éliminer les points faibles répétitifs dans le domaine du service à la clientèle et, si elle est bien mise en œuvre, permettre un service plus personnalisé.

Dans le domaine stratégique, les modèles d'IA sont soumis aux préjugés et aux hypothèses des humains qui les ont développés. Comme la performance et l'équité des modèles d'IA dépendent de l'exactitude et de la diversité des données sur lesquelles ils s'appuient, les banques doivent veiller à ce que ces données soient précises et représentatives de la population ciblée. Les institutions financières devront aligner la mise en œuvre de leurs systèmes d'IA sur leurs pratiques existantes en matière d'éthique et de préjugés.

L'IA va changer – et non remplacer – la main-d'œuvre bancaire. Les tâches répétitives de

to use it effectively.[2] Canadian banks need to invest in training and strengthen employees to have the tools and confidence to adapt.

In the next three to five years, success will depend on speed of implementation to be competitive on the world-wide stage, while balancing innovation with responsibility. Canadian regulators have introduced some guidance around AI, but as the industry evolves, a more comprehensive AI regulatory framework which strikes a balance between encouraging innovation and protecting Canadians needs to be introduced. With the right framework in place, banks that embed ethical safeguards and upskill their workforce will lead in saving trust and unlocking AI's full potential.

[1]Artificial intelligence in banking - Canada.ca. https://www.canada.ca/en/financial-consumer-agency/services/banking/artificial-intelligence.html

[2] Majority of Canadian workers are optimistic about AI but aren't ready. https://www.newswire.ca/news-releases/majority-of-canadian-workers-are-optimistic-about-ai-but-aren-t-ready-899524757.html.

AI in banking / L'IA dans le secteur bancaire

codage et d'administration pourraient être réduites, ce qui permettrait de se consacrer à des tâches plus gratifiantes, telles que la résolution de problèmes et la supervision de l'IA. Cependant, les résultats d'une enquête menée par le Groupe Banque TD révèlent que si de nombreux travailleurs canadiens considèrent l'IA comme un outil utile, ils ne disposent pas de la formation et du soutien nécessaires pour l'utiliser efficacement.[2] Les banques canadiennes doivent investir dans la formation et renforcer les compétences de leurs employés afin qu'ils disposent des outils et de la confiance nécessaires pour s'adapter.

Au cours des trois à cinq prochaines années, le succès dépendra de la rapidité de mise en œuvre pour être compétitif sur la scène mondiale, tout en trouvant un équilibre entre innovation et responsabilité. Les régulateurs canadiens ont publié certaines directives concernant l'IA, mais à mesure que le secteur évolue, il est nécessaire de mettre en place un cadre réglementaire plus complet qui trouve un équilibre entre la promotion de l'innovation et la protection des Canadiens. Avec un cadre approprié en place, les banques qui intègrent des garanties éthiques et améliorent les compétences de leur personnel seront les premières à gagner la confiance et à libérer tout le potentiel de l'IA.

[1]L'intelligence artificielle dans le secteur bancaire - Canada.ca. https://www.canada.ca/en/financial-consumer-agency/services/banking/artificial-intelligence.html

[2] La majorité des travailleurs canadiens sont optimistes à l'égard de l'IA, mais ne sont pas prêts. https://www.newswire.ca/news-releases/majority-of-canadian-workers-are-optimistic-about-ai-but-aren-t-ready-899524757.html.

Rick Cooper

AI in the Military: Transforming Operations, Training, and Strategic Superiority

As artificial intelligence (AI) continues to evolve and permeate every sector of business, its impact on military operations is becoming increasingly profound. Over the next three to five years, AI is expected to reshape the defense landscape—streamlining innovation, accelerating workforce development, and redefining strategic advantage. But with these advancements come new risks, particularly in cybersecurity and supply chain integrity, that must be addressed with equal urgency.

The military has always been a crucible for technological innovation. From dispatch riders carrying handwritten orders on horseback to encrypted radio transmissions and now real-time digital reporting, the evolution of communication has been relentless. AI continues this trajectory by bridging the gap between mundane human tasks and advanced technological capabilities. Routine functions like data entry, system monitoring, and logistics coordination are increasingly automated, allowing personnel to focus on mission-critical decisions. This shift not only enhances operational efficiency but also extends the time available for training and tactical development—making soldiers more effective, faster.

One of the most significant challenges in defense is the time it takes to train new recruits. On average, it takes about 2.5 years to transform a civilian into a soldier proficient in basic operational tasks. AI is dramatically shortening this timeline. Intelligent systems can assist with software installation, configuration, and troubleshooting—tasks that once required specialized training. AI-driven virtual assistants and adaptive learning platforms can guide new personnel through complex procedures, enabling them to contribute meaningfully to operations much sooner. This not only boosts efficiency but also helps retain talent by reducing the initial barrier to entry.

Rick Cooper

L'IA dans l'armée : transformation des opérations, de la formation et de la supériorité stratégique

À mesure que l'intelligence artificielle (IA) continue d'évoluer et de s'imposer dans tous les secteurs d'activité, son impact sur les opérations militaires devient de plus en plus profond. Au cours des trois à cinq prochaines années, l'IA devrait remodeler le paysage de la défense, en rationalisant l'innovation, en accélérant le développement de la main-d'œuvre et en redéfinissant l'avantage stratégique. Mais ces progrès s'accompagnent de nouveaux risques, notamment en matière de cybersécurité et d'intégrité de la chaîne d'approvisionnement, qui doivent être traités avec la même urgence.

L'armée a toujours été un creuset d'innovation technologique. Des cavaliers transportant des ordres manuscrits à cheval aux transmissions radio cryptées et maintenant aux rapports numériques en temps réel, l'évolution des communications a été incessante. L'IA poursuit cette trajectoire en comblant le fossé entre les tâches humaines banales et les capacités technologiques avancées. Les fonctions routinières telles que la saisie de données, la surveillance des systèmes et la coordination logistique sont de plus en plus automatisées, ce qui permet au personnel de se concentrer sur les décisions critiques pour la mission. Ce changement améliore non seulement l'efficacité opérationnelle, mais prolonge également le temps disponible pour la formation et le développement tactique, rendant les soldats plus efficaces et plus rapides.

L'un des défis les plus importants dans le domaine de la défense est le temps nécessaire pour former les nouvelles recrues. En moyenne, il faut environ deux ans et demi pour transformer un

As adversaries also adopt AI technologies, the battlefield is becoming increasingly digitized and symmetrical. The key to maintaining a strategic edge lies in speed, foresight, and adaptability. While AI cannot yet physically capture terrain, it can simulate scenarios, optimize logistics, and support operational planning through advanced wargaming. These capabilities allow commanders to anticipate enemy moves, allocate resources more effectively, and make data-informed decisions faster than ever before. In a world where milliseconds matter, being the first to act—guided by AI insights—can be the difference between victory and defeat.

Despite its promise, AI integration into military systems carries significant risks—chief among them, cybersecurity and supply chain vulnerabilities. Modern military hardware relies on a vast array of electrical components sourced globally. Ensuring that microchips, interfaces, and embedded systems are free from compromise is a daunting challenge. A single vulnerability in the supply chain could lead to system failures, data breaches, or sabotage.

Moreover, AI systems themselves are susceptible to exploitation. Adversaries may attempt to manipulate training data, launch adversarial attacks, or embed malicious code

AI in the Military / L'IA dans l'armée

civil en soldat compétent dans les tâches opérationnelles de base. L'IA réduit considérablement ce délai. Les systèmes intelligents peuvent aider à l'installation, à la configuration et au dépannage des logiciels, tâches qui nécessitaient auparavant une formation spécialisée. Les assistants virtuels basés sur l'IA et les plateformes d'apprentissage adaptatif peuvent guider les nouveaux employés à travers des procédures complexes, leur permettant ainsi de contribuer de manière significative aux opérations beaucoup plus rapidement. Cela permet non seulement d'améliorer l'efficacité, mais aussi de fidéliser les talents en réduisant les obstacles initiaux à l'entrée.

Les adversaires adoptant eux aussi les technologies d'IA, le champ de bataille devient de plus en plus numérisé et symétrique. La clé pour conserver un avantage stratégique réside dans la rapidité, la prévoyance et la capacité d'adaptation. Si l'IA ne peut pas encore conquérir physiquement du terrain, elle peut simuler des scénarios, optimiser la logistique et faciliter la planification opérationnelle grâce à des jeux de guerre avancés. Ces capacités permettent aux commandants d'anticiper les mouvements de l'ennemi, d'allouer plus efficacement les ressources et de prendre des décisions éclairées par les données plus rapidement que jamais. Dans un monde où chaque milliseconde compte, être le premier à agir, guidé par les informations fournies par l'IA, peut faire la différence entre la victoire et la défaite.

Malgré ses promesses, l'intégration de l'IA dans les systèmes militaires comporte des risques importants, notamment en matière de cybersécurité et de vulnérabilité de la chaîne d'approvisionnement. Le matériel militaire moderne repose sur une vaste gamme de composants électriques provenant du monde entier. Garantir que les micropuces, les interfaces et les systèmes embarqués ne soient pas compromis représente un défi de taille.

into seemingly benign inputs. These tactics could cause AI systems to misinterpret threats, misallocate resources, or disrupt command-and-control functions. Additionally, the vast datasets that fuel AI—often containing sensitive operational information—must be rigorously protected. If compromised, they could be reverse-engineered to predict strategies or expose vulnerabilities.

Finally, overreliance on AI introduces systemic risk. If systems are compromised or malfunction, human operators must be prepared to take over seamlessly. Building resilient architectures with human-in-the-loop safeguards and fallback protocols is essential to mitigate this risk.

In conclusion, AI is not just a tool—it's a transformative force. By enhancing innovation, accelerating workforce development, and sharpening strategic planning, it is redefining what it means to be mission-ready. But to fully harness its potential, the military must remain vigilant against emerging threats and invest in robust security measures. The future of warfare will be shaped not just by who has the most powerful weapons, but by who can wield intelligence—artificial and human—with the greatest precision.

Helen Feng

The Human-AI Partnership: Reshaping Resilience

Artificial Intelligence (AI) presents a tremendous opportunity to address two immediate and persistent challenges in the resilience space: talent shortages and the need for effective operational efficiency. In small organizations especially, where capacity is limited and the scope of work is vast, AI can act as a force multiplier to automate routine tasks, accelerating data analysis, and enhancing decision-making. From meeting documentation to risk reporting, AI tools are helping professionals reclaim time and redirect their focus toward strategic work. But the real value lies not just in automation—it's in how AI augments human capability. It's not replacing us though! It's reshaping how we work, learn, and lead.

Une seule vulnérabilité dans la chaîne d'approvisionnement pourrait entraîner des pannes du système, des violations de données ou des sabotages. De plus, les systèmes d'IA eux-mêmes sont susceptibles d'être exploités. Des adversaires peuvent tenter de manipuler les données d'entraînement, lancer des attaques adversaires ou intégrer du code malveillant dans des entrées apparemment inoffensives. Ces tactiques pourraient amener les systèmes d'IA à mal interpréter les menaces, à mal répartir les ressources ou à perturber les fonctions de commandement et de contrôle. En outre, les vastes ensembles de données qui alimentent l'IA, contenant souvent des informations opérationnelles sensibles, doivent être rigoureusement protégés. S'ils sont compromis, ils pourraient faire l'objet d'une ingénierie inverse afin de prédire des stratégies ou d'exposer des vulnérabilités.

Enfin, une dépendance excessive à l'IA introduit un risque systémique. Si les systèmes sont compromis ou tombent en panne, les opérateurs humains doivent être prêts à prendre le relais de manière transparente. Il est essentiel de mettre en place des architectures résilientes avec des mesures de protection impliquant l'intervention humaine et des protocoles de secours afin d'atténuer ce risque.

En conclusion, l'IA n'est pas seulement un outil, c'est une force de transformation. En stimulant l'innovation, en accélérant le développement de la main-d'œuvre et en affinant la planification stratégique, elle redéfinit ce que signifie être prêt pour la mission. Mais pour exploiter pleinement son potentiel, l'armée doit rester vigilante face aux menaces émergentes et investir dans des mesures de sécurité robustes. L'avenir de la guerre ne sera pas seulement déterminé par ceux qui possèdent les armes les plus puissantes, mais aussi par ceux qui sauront utiliser l'intelligence, artificielle et humaine, avec la plus grande précision.

At Canadian Medical Assistance Teams (CMAT), where resources are lean and every volunteer wears multiple hats, AI has become indispensable. We use Read, an AI-powered meeting assistant, to generate transcripts, summarize key points, and highlight action items in real time. What used to take hours of manual effort is now completed within minutes. Our board secretary still creates a separate version of the minutes for formal approval, but they can now rely on organized, searchable, and pre-themed transcripts and recordings to guide their work. This isn't just about saving time—it's about enhancing the quality, clarity, and accessibility of information to support better decision-making and engagement.

At Central 1 Credit Union, where I lead the operational resilience function, I use tools like M365 Copilot to tailor communications and documentation for the right audience such as for technical teams, business units, or executive leadership. One of the ongoing challenges is analyzing large volumes of data from Business Impact Analysis or Operational Risk Events, especially when much of it has historically been collected manually. That's beginning to shift as we onboard a new Governance, Risk, and Compliance (GRC) platform to centralize and streamline data for enterprise risk functions.

Human-AI Partnership
Partenariat entre l'homme et l'intelligence artificielle

Helen Feng

Le partenariat entre l'humain et l'IA : redéfinir la résilience

L'intelligence artificielle (IA) offre une formidable opportunité de relever deux défis immédiats et persistants dans le domaine de la résilience : la pénurie de talents et la nécessité d'une efficacité opérationnelle efficace. Dans les petites organisations en particulier, où les capacités sont limitées et l'étendue du travail vaste, l'IA peut agir comme un multiplicateur de force pour automatiser les tâches routinières, accélérer l'analyse des données et améliorer la prise de décision. De la documentation des réunions aux rapports sur les risques, les outils d'IA aident les professionnels à gagner du temps et à se concentrer davantage sur leur travail stratégique. Mais la véritable valeur ne réside pas seulement dans l'automatisation, mais aussi dans la manière dont l'IA augmente les capacités humaines. Elle ne nous remplace pas pour autant ! Elle remodèle notre façon de travailler, d'apprendre et de diriger.

Au sein des Équipes canadiennes d'aide médicale (ECAM), où les ressources sont limitées et où chaque bénévole porte plusieurs casquettes, l'IA est devenue indispensable. Nous utilisons Read, un assistant de réunion alimenté par l'IA, pour générer des transcriptions, résumer les points clés et mettre en évidence les mesures à prendre en temps réel. Ce qui prenait auparavant des heures de travail manuel est désormais réalisé en quelques minutes. Notre secrétaire du conseil d'administration continue de créer une version séparée du procès-verbal pour approbation officielle, mais il peut désormais s'appuyer sur des transcriptions et des enregistrements organisés, consultables et pré-thématisés pour guider son travail. Il ne s'agit pas seulement de gagner du temps, mais aussi d'améliorer la qualité, la clarté et l'accessibilité des informations afin de favoriser une meilleure prise de décision et un meilleur engagement. ➤

Each business line owns its risks, but the second line of defense provides neutral oversight, which requires identifying root causes, understanding mitigation strategies, and spotting emerging trends. AI helps sift through initial data groupings and surface themes, allowing me to focus on the deeper analysis and strategic conversations. When disruptions occur, accurate tracking is essential—but true understanding comes from context, relationships, and critical thinking, which AI supports but cannot replace. AI can surface patterns and flag anomalies, but it cannot replicate the insights gained from conversations with frontline teams. It's a tool for initial insight, not final judgment. And in a sector where language matters—where technical risk assessments must be translated for executive audiences—AI helps reframe content in ways that are both accurate and digestible.

AI is not just changing how we work—it's changing who we need to be as professionals. In resilience and risk roles, communication is key. Whether you're speaking with IT teams, business units, or board members, the ability to adapt your tone and language is essential. AI helps me practice that adaptability. I can use it to rephrase technical content, simulate different communication styles, and even prepare for difficult conversations. This has real implications for career development. AI is becoming a learning partner—helping us build credibility faster, understand unfamiliar domains, and refine our leadership voice. It's not just about technical skills anymore; it's about emotional intelligence, strategic thinking, and the ability to synthesize complex information. As AI becomes more embedded in our workflows, leaders will need to cultivate a new kind of fluency—not just in using the tools, but in guiding their ethical and effective use. The skillset of tomorrow's resilience professional will be part analyst, part communicator, and part steward of integrity.

The sheer volume of data AI can process introduces incredible opportunities for insight, prediction, and automation. But it also raises questions about integrity, transparency, and trust. There's a danger in over dependence

Chez Central 1 Credit Union, où je dirige la fonction de résilience opérationnelle, j'utilise des outils tels que M365 Copilot pour adapter les communications et la documentation au public concerné, qu'il s'agisse des équipes techniques, des unités commerciales ou de la direction. L'un des défis permanents consiste à analyser de grands volumes de données issues de l'analyse d'impact sur l'activité ou des événements liés aux risques opérationnels, d'autant plus que la plupart de ces données ont été collectées manuellement jusqu'à présent. Cette situation commence à changer depuis que nous avons mis en place une nouvelle plateforme de gouvernance, de gestion des risques et de conformité (GRC) afin de centraliser et de rationaliser les données relatives aux fonctions de gestion des risques de l'entreprise.

Chaque secteur d'activité assume ses propres risques, mais la deuxième ligne de défense assure une surveillance neutre, ce qui nécessite d'identifier les causes profondes, de comprendre les stratégies d'atténuation et de repérer les tendances émergentes. L'IA aide à passer au crible les premiers regroupements de données et à faire ressortir les thèmes, ce qui me permet de me concentrer sur l'analyse approfondie et les conversations stratégiques. En cas de perturbations, un suivi précis est essentiel, mais la véritable compréhension vient du contexte, des relations et de la pensée critique, que l'IA soutient mais ne peut remplacer. L'IA peut mettre en évidence des tendances et signaler des anomalies, mais elle ne peut pas reproduire les informations obtenues lors des conversations avec les équipes de première ligne. Il s'agit d'un outil permettant d'obtenir des informations initiales, et non de porter un jugement définitif. Et dans un secteur où le langage est important, où les évaluations des risques techniques doivent être traduites pour les cadres dirigeants, l'IA aide à reformuler le contenu de manière à la fois précise et compréhensible.

on AI, especially when decisions affect people, operations, and reputations. There's a real temptation to lean heavily on AI for speed and efficiency, especially when time is limited and the volume of data is high. But efficiency should never come at the expense of understanding the human context such as the concerns, conflicts, and complexities of the end users experience. AI can help organize and analyze information, but it cannot fully grasp the emotional undercurrents or operational realities that shape risk. Even when I do present AI-supported analysis, it's never a final answer. It is simply a starting point for dialogue! I invite and have my door open for stakeholders to challenge, refine, and reframe the insights. I see AI as a facilitator, not a decision-maker. It helps me work faster, yes, but more importantly, it helps me work smarter and more collaboratively, ensuring that the people impacted by decisions are part of the conversation.

The challenge ahead is to embed AI thoughtfully, ensuring that human oversight remains central

L'IA ne change pas seulement notre façon de travailler, elle change aussi ce que nous devons être en tant que professionnels. Dans les rôles liés à la résilience et aux risques, la communication est essentielle. Que vous vous adressiez à des équipes informatiques, à des unités commerciales ou à des membres du conseil d'administration, il est essentiel de savoir adapter votre ton et votre langage. L'IA m'aide à mettre en pratique cette capacité d'adaptation. Je peux l'utiliser pour reformuler des contenus techniques, simuler différents styles de communication et même me préparer à des conversations difficiles. Cela a des implications réelles pour le développement de carrière. L'IA devient un partenaire d'apprentissage qui nous aide à renforcer plus rapidement notre crédibilité, à comprendre des domaines qui nous sont peu familiers et à affiner notre leadership. Il ne s'agit plus seulement de compétences techniques, mais aussi d'intelligence émotionnelle, de réflexion stratégique et de capacité à synthétiser des informations

and that ethical guardrails are in place. My prediction? AI will continue to reshape our industry, but the organizations that thrive will be those that blend technology with human judgment, using AI not as a crutch, but as a catalyst for deeper understanding and better outcomes. Even this article is a product of that partnership. The ideas are mine but shaped, refined, and structured with the help of AI. It's a testament to what's possible when we embrace innovation without losing sight of our values.

Ultimately, AI is a powerful enabler, but true value in resilience comes from human connection, critical engagement, and thoughtful leadership. In a crisis, AI isn't running our command centre. It can support the work, but it cannot replace the judgment, empathy, and collaboration required to navigate uncertainty. A simple risk taxonomy that could be generated by AI isn't enough. To make a meaningful impact, resilience professionals must go beyond listing risks and presenting AI-generated insights. We need to engage the business and end-users, challenge assumptions, and bring forward perspectives that reflect the lived realities of those affected.

I have heard, "They're not my risks, they're your risks." That shift in ownership is where real resilience begins. I use AI to bolster my rationale, structure my analysis, and accelerate my work—but the heart of my role lies in building relationships, asking the right questions, and creating space for dialogue. AI can guide the conversation, but it's up to us to ensure it's the right conversation. This year, I attended a webinar on how emerging AI technologies are making business continuity programs more dynamic and efficient. It's exciting to be in an age where these tools can help us map business processes, understand critical vulnerabilities, manage regulatory requirements, and stay ahead of potential disruptions. But even with these advancements, the real opportunity lies in how we, as professionals, choose to use them—not just to work faster, but to work smarter, more inclusively, and with greater integrity.

complexes. À mesure que l'IA s'intègre dans nos processus de travail, les dirigeants devront cultiver une nouvelle forme d'aisance, non seulement dans l'utilisation des outils, mais aussi dans la promotion d'une utilisation éthique et efficace de ceux-ci. Les compétences requises pour les professionnels de la résilience de demain seront à la fois celles d'un analyste, d'un communicateur et d'un garant de l'intégrité. Le volume considérable de données que l'IA peut traiter offre des possibilités incroyables en matière d'analyse, de prévision et d'automatisation. Mais cela soulève également des questions d'intégrité, de transparence et de confiance. Il est dangereux de trop dépendre de l'IA, en particulier lorsque les décisions ont une incidence sur les personnes, les opérations et la réputation. Il est très tentant de s'appuyer fortement sur l'IA pour gagner en rapidité et en efficacité, en particulier lorsque le temps est limité et que le volume de données est élevé. Mais l'efficacité ne doit jamais se faire au détriment de la compréhension du contexte humain, tel que les préoccupations, les conflits et les complexités de l'expérience des utilisateurs finaux. L'IA peut aider à organiser et à analyser les informations, mais elle ne peut pas saisir pleinement les courants émotionnels sous-jacents ou les réalités opérationnelles qui façonnent le risque. Même lorsque je présente une analyse soutenue par l'IA, il ne s'agit jamais d'une réponse définitive. C'est simplement un point de départ pour le dialogue ! J'invite les parties prenantes à remettre en question, affiner et recadrer les idées, et je leur ouvre ma porte. Je considère l'IA comme un facilitateur, et non comme un décideur. Elle m'aide à travailler plus rapidement, certes, mais surtout, elle m'aide à travailler de manière plus intelligente et plus collaborative, en veillant à ce que les personnes concernées par les décisions participent à la conversation.

Le défi à relever consiste à intégrer l'IA de manière réfléchie, en veillant à ce que le contrôle humain reste central et que des garde-fous éthiques soient mis en place. Ma

Jonathan Cummings

AI in Cyber Security: Friend or Foe?

As someone who's been in technology and cyber security for a while, I'm both excited and apprehensive about AI's trajectory. It's not just a tool, it's a force that's redefining our field in ways that are thrilling, unsettling, and full of unknowns. We can look at this through the lenses of innovation, workforce, and competitive advantage, while grappling with the dual reality of AI as both a defender's ally and an attacker's weapon, plus the risks of weaving it so deeply into our systems!

On innovation, AI is already pushing boundaries, and in the next three to five years, I think it'll transform how we prevent and recover from cyber incidents. On the defense side, we're seeing AI systems that don't just detect threats but predict them, analyzing vast datasets to spot anomalies. Agentic AI supercharges Security Operations Centres, autonomously hunting threats with razor-sharp precision, slashing response times.

But what's keeping me up at night: attackers are leveraging AI just as fast. Imagine AI-crafted phishing emails that perfectly mimic a CEO's tone, or malware that evolves mid-attack to dodge detection. In a few years, we could face AI-driven botnets that learn from our defenses in real-time. This raises a haunting question: How do you contain and recover from an attack, when the attack itself is intelligent and faster than anything seen before? Right now, we don't know.

The workforce angle is equally complex. AI could free us from repetitive tasks, think log monitoring or basic threat hunting, letting analysts focus on strategic challenges, like designing resilient architectures. I can see a future where we're not just responders but AI orchestrators, training models to tailor defenses to our specific environments. Yet, there's a catch: this shift could gut entry-level roles. If AI handles the basics, how do new professionals learn and get to the stage of being able to oversee AI, when they will need to learn technology, cyber security and AI? monitoring or basic threat hunting, letting analysts focus on strategic challenges, like prédiction ? L'IA continuera à remodeler notre secteur, mais les organisations qui prospéreront seront celles qui associeront la technologie au jugement humain, en utilisant l'IA non pas comme une béquille, mais comme un catalyseur pour une compréhension plus approfondie et de meilleurs résultats. Même cet article est le fruit de ce partenariat. Les idées sont les miennes, mais elles ont été façonnées, affinées et structurées à l'aide de l'IA. Cela témoigne de ce qu'il est possible de réaliser lorsque nous adoptons l'innovation sans perdre de vue nos valeurs.

En fin de compte, l'IA est un puissant catalyseur, mais la véritable valeur de la résilience provient des relations humaines, de l'engagement critique et d'un leadership réfléchi. En cas de crise, l'IA ne dirige pas notre centre de commande. Elle peut soutenir le travail, mais elle ne peut remplacer le jugement, l'empathie et la collaboration nécessaires pour naviguer dans l'incertitude. Une simple taxonomie des risques générée par l'IA ne suffit pas. Pour avoir un impact significatif, les professionnels de la résilience doivent aller au-delà de la simple énumération des risques et de la présentation des informations générées par l'IA. Nous devons impliquer l'entreprise et les utilisateurs finaux, remettre en question les hypothèses et proposer des perspectives qui reflètent les réalités vécues par les personnes concernées. J'ai entendu dire : « Ce ne sont pas mes risques, ce sont vos risques. » C'est dans ce transfert de responsabilité que réside la véritable résilience. J'utilise l'IA pour étayer mon raisonnement, structurer mon analyse et accélérer mon travail, mais l'essentiel de mon rôle consiste à établir des relations, à poser les bonnes questions et à créer un espace de dialogue. L'IA peut guider la conversation, mais c'est à nous de veiller à ce qu'elle soit pertinente. Cette année, j'ai participé à un webinaire sur la manière dont les technologies émergentes d'IA rendent les programmes de continuité des activités plus dynamiques et plus efficaces. Il est passionnant de vivre à une époque où ces outils peuvent

designing resilient architectures. I can see a future where we're not just responders but AI orchestrators, training models to tailor defenses to our specific environments. Yet, there's a catch: this shift could gut entry-level roles. If AI handles the basics, how do new professionals learn and get to the stage of being able to oversee AI, when they will need to learn technology, cyber security and AI?

Artificial intelligence is weaving itself into every tool we use at a breathtaking pace, its tentacles spreading across systems, processes, and technologies in nearly every sector and business. From firewalls that adapt in real-time to recovery platforms that predict optimal failover paths, AI boosts efficiency, slashing response times and automating complex tasks. Yet, this deep integration introduces serious supply chain risks, as third-party AI models, often opaque, become potential weak links, vulnerable to tampering or data poisoning. When incidents strike, troubleshooting becomes a nightmare; how do you pinpoint a flaw in a black-box algorithm or remediate a process where AI's decisions are inscrutable?

Ultimately, AI's impact on cyber security isn't a tidy narrative—it's a paradox. In three to five years, it could make us faster, smarter, and more resilient, but it's also arming attackers and complicating our systems in ways we're only starting to grasp. The real challenge is whether we can harness AI's power without losing the human judgment that anchors our field.

Sukhmani Sandhu

Artificial Intelligence: A Force Multiplier for Resilience and Business Continuity

In today's rapidly evolving landscape—marked by climate-induced disasters, cyber threats, and geopolitical instability—artificial intelligence (AI) is transforming the traditional domains of resilience, business continuity (BC), and disaster recovery (DR). AI is redefining the boundaries of preparedness by enabling real-time analysis of vast and diverse data sources, allowing for earlier detection of potential threats.

nous aider à cartographier les processus commerciaux, à comprendre les vulnérabilités critiques, à gérer les exigences réglementaires et à anticiper les perturbations potentielles. Mais même avec ces progrès, la véritable opportunité réside dans la manière dont nous, en tant que professionnels, choisissons de les utiliser, non seulement pour travailler plus rapidement, mais aussi pour travailler de manière plus intelligente, plus inclusive et avec une plus grande intégrité.

Jonathan Cummings

L'IA dans la cybersécurité : Ami ou ennemi ?

Travaillant depuis un certain temps dans le domaine de la technologie et de la cybersécurité, je suis à la fois enthousiaste et inquiet de la trajectoire de l'IA. Ce n'est pas seulement un outil, c'est une force qui redéfinit notre domaine d'une manière à la fois passionnante, troublante et pleine d'inconnues. Nous pouvons l'envisager sous l'angle de l'innovation, de la main-d'œuvre et de l'avantage concurrentiel, tout en étant confrontés à la double réalité de l'IA, à la fois alliée du défenseur et arme de l'attaquant, ainsi qu'aux risques de l'intégrer aussi profondément dans nos systèmes !

En ce qui concerne l'innovation, l'IA repousse déjà les limites et, dans les trois à cinq prochaines années, je pense qu'elle transformera la manière dont nous prévenons les cyberincidents et dont nous nous en remettons. Du côté de la défense, nous voyons des systèmes d'IA qui ne se contentent pas de détecter les menaces, mais qui les prédisent, en analysant de vastes ensembles de données pour repérer les anomalies. L'IA agentique renforce les centres d'opérations de sécurité, chassant de manière autonome les menaces avec une précision extrême, réduisant ainsi les temps de réponse.

Mais ce qui m'empêche de dormir, c'est que les attaquants exploitent l'IA tout

AI is not just improving how quickly we recover from disruptions—it's reshaping resilience into a smarter, more adaptive approach. This is especially critical in high-stakes, public- facing environments. With over seven years of experience leading complex technology projects across transit, supply chain, and public service sectors, I've seen firsthand how AI revolutionizes planning, response, and recovery. It empowers organizations to not only react to disruptions more effectively, but to anticipate—and in some cases prevent—them entirely.

AI-driven automation reduces downtime while ensuring consistent and accurate response protocols. By accelerating incident response and recovery without requiring human intervention, AI identifies disruptions early—whether it's an operational failure, cyberattack, or extreme weather event. Leveraging both historical and real-time data, AI uncovers patterns and flags anomalies, offering critical foresight to decision-makers. As such, AI acts as a powerful force multiplier, helping organizations evolve from reactive recovery to proactive resilience.

Importantly, AI is not about replacing professionals or eliminating jobs. Instead, it's about enhancing risk detection, automating decision-making, and streamlining responses. For organizations managing complex operations—such as vast fleets or geographically distributed assets—AI-powered adaptive planning ensures site-specific responses and optimized resource allocation.

As cyber threats grow more sophisticated, AI plays a crucial role in cybersecurity. It monitors systems for unusual behavior, conducts forensic analysis, and rapidly contains breaches by understanding attack vectors. AI can automatically trigger response protocols, initiate system failovers, or reroute critical operations—minimizing aussi rapidement. Imaginez des courriels de phishing conçus par l'IA qui imitent parfaitement le ton d'un PDG, ou des logiciels malveillants qui évoluent en cours d'attaque pour éviter d'être détectés. Dans quelques années, nous pourrions être confrontés à des réseaux de zombies pilotés par l'IA qui tirent des enseignements de nos défenses en temps réel. Cela soulève une question lancinante : Comment contenir une attaque et s'en remettre lorsque l'attaque elle-même est intelligente et plus rapide que tout ce qui a été vu auparavant ? Pour l'instant, nous n'en savons rien.

La question de la main-d'œuvre est tout aussi complexe. L'IA pourrait nous libérer des tâches répétitives.

Sukhmani Sandhu

L'intelligence artificielle : Un multiplicateur de force pour la résilience et la continuité des activités

Dans le contexte actuel d'évolution rapide, marqué par les catastrophes climatiques, les cybermenaces et l'instabilité géopolitique, l'intelligence artificielle (IA) transforme les domaines traditionnels de la résilience, de la continuité des activités et de la reprise après sinistre. L'IA redéfinit les limites de la préparation en permettant l'analyse en temps réel de sources de données vastes et diverses, ce qui permet de détecter plus rapidement les menaces potentielles.

L'IA ne se contente pas d'améliorer la rapidité avec laquelle nous nous remettons des perturbations, elle transforme la résilience en une approche plus intelligente et plus adaptative. Cela est particulièrement important dans les environnements publics à fort enjeu. Avec plus de sept ans d'expérience à la tête de projets technologiques complexes dans les secteurs des transports, de la chaîne d'approvisionnement et des services publics, j'ai vu de mes propres yeux comment l'IA révolutionne la planification, la réponse et le rétablissement. Elle permet aux

downtime and reducing the margin for error in time-sensitive situations. For organizations spread across Canada's vast geography, AI-enhanced situational awareness enables more coordinated responses from regional teams.

Unlike traditional continuity plans that quickly become outdated, AI systems evolve continuously. They learn from past incidents and adapt in real time, creating a dynamic feedback loop. This ensures that business continuity and disaster recovery plans remain living documents—agile and responsive to changing threats, infrastructures, and business models.

During crises, AI supports real-time decision-making by aggregating operational, environmental, and market data. Its role in cybersecurity is especially pronounced in projects where Single Sign-On (SSO) and Multi-Factor Authentication (MFA) were implemented, integrated AI monitored anomalous login behaviors, adding a critical layer of threat intelligence.

Given the unique challenges faced by Canada's public and private sectors—aging infrastructure, increasing climate risks, and escalating cybersecurity threats—AI-enhanced BC/DR is no longer optional; it's a strategic imperative. However, effective AI deployment must be grounded in strong governance frameworks to ensure ethical use, transparency, and

organisations non seulement de réagir plus efficacement aux perturbations, mais aussi de les anticiper et, dans certains cas, de les prévenir complètement.

L'automatisation pilotée par l'IA réduit les temps d'arrêt tout en garantissant des protocoles de réponse cohérents et précis. En accélérant la réponse aux incidents et la récupération sans nécessiter d'intervention humaine, l'IA identifie rapidement les perturbations, qu'il s'agisse d'une défaillance opérationnelle, d'une cyberattaque ou d'un événement météorologique extrême. En s'appuyant sur des données historiques et en temps réel, l'IA découvre des schémas et signale des anomalies, offrant ainsi aux décideurs une vision prospective essentielle. En tant que telle, l'IA agit comme un puissant multiplicateur de force, aidant les organisations à passer d'une reprise réactive à une résilience proactive.

Il est important de noter que l'IA ne vise pas à remplacer les professionnels ou à supprimer des emplois. Il s'agit plutôt d'améliorer la détection des risques, d'automatiser la prise de décision et de rationaliser les réponses. Pour les organisations qui gèrent des opérations complexes, telles que de vastes flottes ou des actifs répartis géographiquement, la planification adaptative alimentée par l'IA garantit des réponses spécifiques au site et une allocation optimisée des ressources.

Les cybermenaces devenant de plus en plus sophistiquées, l'IA joue un rôle crucial dans la cybersécurité. Elle surveille les systèmes à la recherche de comportements inhabituels, effectue des analyses médico-légales et identifie rapidement les brèches en comprenant les vecteurs d'attaque. L'IA peut automatiquement déclencher des protocoles de réponse, initier des basculements de systèmes ou réacheminer des opérations critiques – minimisant ainsi les temps d'arrêt et réduisant la marge d'erreur dans les situations où le temps est compté. Pour les organisations réparties sur le vaste territoire canadien, la connaissance de la situation améliorée par l'IA permet aux équipes régionales de mieux coordonner leurs interventions.

Contrairement aux plans de continuité traditionnels qui deviennent rapidement obsolètes, les systèmes d'IA évoluent continuellement. Ils tirent des leçons des incidents passés et s'adaptent en temps réel, créant ainsi une boucle de rétroaction dynamique. Cela garantit que les plans de continuité des activités et de reprise après sinistre restent des documents vivants, agiles et réactifs face à l'évolution des menaces, des infrastructures et des modèles d'entreprise.

explainability. Cross-functional collaboration between IT, operations, and leadership is essential, along with building internal capacity to manage and maintain AI systems.

AI must be layered thoughtfully—augmenting rather than replacing human expertise. Its true power lies in enhancing our ability to anticipate, respond, and recover—not only faster and smarter but also more sustainably.

Of course, adopting AI comes with challenges: poor-quality data can lead to misguided predictions; organizations may lack the necessary skills; upfront investments can be significant. Ethical considerations, transparency, and aligning AI with existing BC/DR frameworks—without creating silos—must also be addressed. Yet, when implemented well, AI doesn't just help organizations "bounce back" from disruptions—it enables them to "bounce forward," building smarter, more resilient systems.

By integrating AI into organizational ecosystems, companies can shift from reactive to proactive postures—positioning themselves to not only survive disruptions, but to thrive in their aftermath. As many AI professionals say: the next crisis may be unpredictable—but with AI, your response doesn't have to be.. Ω

En cas de crise, l'IA facilite la prise de décision en temps réel en regroupant les données opérationnelles, environnementales et commerciales. Son rôle dans la cybersécurité est particulièrement prononcé dans les projets où l'authentification unique (SSO) et l'authentification multifactorielle (MFA) ont été mises en œuvre, l'IA intégrée a surveillé les comportements de connexion anormaux, ajoutant une couche critique de renseignements sur les menaces.

Compte tenu des défis uniques auxquels sont confrontés les secteurs public et privé du Canada - le vieillissement des infrastructures, l'augmentation des risques climatiques et l'escalade des menaces de cybersécurité - l'amélioration de la BC/DR par l'IA n'est plus facultative ; c'est un impératif stratégique. Cependant, le déploiement efficace de l'IA doit s'appuyer sur des cadres de gouvernance solides afin de garantir une utilisation éthique, la transparence et la possibilité d'expliquer. La collaboration interfonctionnelle entre l'informatique, les opérations et la direction est essentielle, de même que le renforcement des capacités internes de gestion et de maintenance des systèmes d'IA.

L'IA doit être mise en place de manière réfléchie, en complétant plutôt qu'en remplaçant l'expertise humaine. Son véritable pouvoir réside dans l'amélioration de notre capacité à anticiper, à répondre et à récupérer, non seulement plus rapidement et plus intelligemment, mais aussi de manière plus durable.

Bien sûr, l'adoption de l'IA s'accompagne de défis : des données de mauvaise qualité peuvent conduire à des prédictions erronées ; les organisations peuvent ne pas disposer des compétences nécessaires ; les investissements initiaux peuvent être importants. Les considérations éthiques, la transparence et l'alignement de l'IA sur les cadres existants de prévention des catastrophes et de continuité des activités – sans créer de silos – doivent également être abordés. Pourtant, lorsqu'elle est bien mise en œuvre, l'IA n'aide pas seulement les organisations à "rebondir" après des perturbations, elle leur permet de "rebondir", en construisant des systèmes plus intelligents et plus résilients.

En intégrant l'IA dans les écosystèmes organisationnels, les entreprises peuvent passer d'une position réactive à une position proactive, ce qui leur permet non seulement de survivre aux perturbations, mais aussi de prospérer après celles-ci. Comme le disent de nombreux professionnels de l'IA : la prochaine crise peut être imprévisible, mais grâce à l'IA, votre réponse n'a pas à l'être. Ω

ABOUT THE EXPERTS

Aidan Firlotte is a 3rd Year Computer Science Major at St. Francis Xavier University, NS, where his studies include software engineering and computer programming, database, computer security, and emerging areas of computer science such artificial intelligence.

Kristin Nelles attended the University of Ottawa in 1993 and completed 2 years towards a Bachelor of Science before leaving to work in the restaurant business. In 2003, she returned to university to complete both her Bachelor of Environmental Studies and Bachelor of Education. She graduated in 2006 and started teaching with the Trillium Lakelands District School Board in the City of Kawartha Lakes, ON.

With 19 years of experience teaching Grades 7 and 8, Kristin has dedicated her career to helping students build confidence and skills, specifically in Mathematics and Language. As the field of education continues to evolve, she has embraced the impact that artificial intelligence and new technologies have had on the classroom.

Robin Whyte is the Vancouver Island Community Advisor for Technology for Living, an accessibility consultant, and the creator of Girl About Town: Accessible Victoria. She co-founded Mosaic Access Consulting and authored the tourism accessibility guide for 4VI, bringing her passion for universal design and inclusion to her work in tourism, community, and beyond.

Nancy Holloway-White, CBCP, CBCA (she/her), is currently serving as the President DRI Canada and has been volunteering for DRI Canada in various capacities for over a decade. Nancy works in financial services risk management, specializing in internal controls, process and governance, with a concentration in business continuity.

Major Rick Cooper is a Canadian Solider specializing in Digital Communication and Electronics Engineering with over 2 decades of Military experience.

À PROPOS DES EXPERTS

Aidan Firlotte est étudiant en troisième année d'informatique à l'université St. Francis Xavier, en Nouvelle-Écosse, où il suit des cours d'ingénierie logicielle et de programmation informatique, de bases de données, de sécurité informatique et de domaines émergents de l'informatique tels que l'intelligence artificielle.

Kristin Nelles a fréquenté l'Université d'Ottawa en 1993 et a suivi deux ans d'études en vue d'obtenir un baccalauréat ès sciences avant de quitter l'université pour travailler dans le secteur de la restauration. En 2003, elle est retournée à l'université pour obtenir un baccalauréat en études environnementales et un baccalauréat en éducation. Elle a obtenu son diplôme en 2006 et a commencé à enseigner au sein du conseil scolaire du district de Trillium Lakelands, dans la ville de Kawartha Lakes, en Ontario.

Forte de 19 ans d'expérience dans l'enseignement aux élèves de 7e et 8e année, Kristin a consacré sa carrière à aider les élèves à acquérir de la confiance et des compétences, en particulier en mathématiques et en langues. Alors que le domaine de l'éducation continue d'évoluer, elle a su tirer parti de l'impact de l'intelligence artificielle et des nouvelles technologies sur l'enseignement en classe.

Robin Whyte est conseillère communautaire pour Technology for Living sur l'île de Vancouver, consultante en accessibilité et créatrice de Girl About Town: Accessible Victoria. Elle a cofondé Mosaic Access Consulting et rédigé le guide d'accessibilité touristique pour 4VI, mettant ainsi sa passion pour la conception universelle et l'inclusion au service de son travail dans le domaine du tourisme, de la communauté et au-delà.

Nancy Holloway-White, CBCP, CBCA (elle/elle), est actuellement présidente d'IRN Canada et fait du bénévolat pour DRI Canada à divers titres depuis plus d'une décennie. Nancy travaille dans la gestion des risques des services financiers, se spécialisant dans les contrôles internes, les processus et la gouvernance, avec une concentration dans la continuité des activités.

Le major Rick Cooper est un soldat canadien spécialisé dans les communications numériques et l'ingénierie électronique, avec plus de 20 ans d'expérience militaire.

ABOUT THE EXPERTS

Helen Feng *is a cross-sector resilience leader with a proven track record in both healthcare and financial services. Currently serving as Manager, Business Continuity and Operational Resilience at Central 1, Helen leads integrated strategies that enhance organizational preparedness and safeguard critical operations. Her approach is rooted in the end-user experience and a passion for cross-functional collaboration, enabling her to design practical and sustainable programs that align with business goals, regulatory expectations, and real-world scenarios.*

Helen brings a unique blend of strategic insight, operational experience, and creative thinking to every challenge - driven by a commitment to resilience, collaboration, and continuous improvement.

Jonathan Cummings *is a Chief Information Security Officer, with a background in HealthTech, Financial Services and cyber threat intelligence. He also advises governments, businesses and charities on cyber security, AI-driven innovation, global cyber laws and risk.*

Sukhmani Sandhu *is an experienced IT Project Manager with over seven years of experience leading complex, high-impact technology initiatives across the public transit, supply chain, and infrastructure sectors. Her focus is on aligning digital solutions with operational strategy—especially in complex, regulated sectors where precision, resilience, and innovation intersect.*

Currently at BC Transit, Sukhmani spearheads smart fleet integration projects, with a portfolio that includes battery electric bus (BEB) electrification, disaster recovery modernization, and the automation of fleet and infrastructure management systems. Sukhmani thrive at the intersection of technology, data, and sustainability, and have a growing interest in the responsible integration of AI/ML in operational workflows and decision support systems.

Sukhmani holds a Project Management Professional (PMP) certification, along with advanced credentials from Harvard Business School and Royal Roads University. She also brings a unique interdisciplinary background in biochemistry and business from the University of Victoria.

À PROPOS DES EXPERTS

Helen Feng *est une leader intersectorielle en matière de résilience qui a fait ses preuves dans les domaines de la santé et des services financiers. Actuellement responsable de la continuité des activités et de la résilience opérationnelle chez Central 1, Helen dirige des stratégies intégrées qui améliorent la préparation organisationnelle et protègent les opérations critiques. Son approche est fondée sur l'expérience de l'utilisateur final et sa passion pour la collaboration interfonctionnelle, ce qui lui permet de concevoir des programmes pratiques et durables qui correspondent aux objectifs commerciaux, aux attentes réglementaires et aux scénarios réels.*

Helen apporte à chaque défi un mélange unique de perspicacité stratégique, d'expérience opérationnelle et de pensée créative, motivée par un engagement en faveur de la résilience, de la collaboration et de l'amélioration continue.

Jonathan Cummings *est directeur de la sécurité informatique. Il possède une expérience dans les domaines des technologies de la santé, des services financiers et du renseignement sur les cybermenaces. Il conseille également les gouvernements, les entreprises et les organisations caritatives en matière de cybersécurité, d'innovation basée sur l'IA, de législation mondiale sur le cyberespace et de risques.*

Sukhmani Sandhu *est une chef de projet informatique expérimentée qui compte plus de sept ans d'expérience dans la direction d'initiatives technologiques complexes et à fort impact dans les secteurs des transports publics, de la chaîne d'approvisionnement et des infrastructures. Elle s'attache principalement à aligner les solutions numériques sur la stratégie opérationnelle, en particulier dans les secteurs complexes et réglementés où se croisent précision, résilience et innovation.*

Actuellement chez BC Transit, Sukhmani dirige des projets d'intégration de flottes intelligentes, avec un portefeuille qui comprend l'électrification des bus à batterie (BEB), la modernisation de la reprise après sinistre et l'automatisation des systèmes de gestion des flottes et des infrastructures. Sukhmani s'épanouit à la croisée de la technologie, des données et de la durabilité, et s'intéresse de plus en plus à l'intégration responsable de l'IA/ML dans les flux de travail opérationnels et les systèmes d'aide à la décision.

Sukhmani est titulaire d'une certification PMP (Project Management Professional) et de diplômes supérieurs de la Harvard Business School et de la Royal Roads University. Elle apporte également une expérience interdisciplinaire unique en biochimie et en commerce acquise à l'université de Victoria.

Artificial Intelligence in Disaster Recovery Planning

Written entirely by: ChatGPT 5
(Prompted by: Miles Jenkins)

L'intelligence artificielle dans la planification de la reprise après sinistre

Écrit entièrement par : ChatGPT 5
(Sur instruction de: Miles Jenkins)

Prologue:

It is the general policy of this magazine to discourage the use of AI when writing articles for TNR. We feel that our **content should be created by humans**. In fact, it is shamefully dishonest for someone to claim authorship of a piece that was actually written in whole or in part by an AI app (like ChatGBT) without disclosing that fact. Nevertheless, artificial intelligence is becoming more and more ubiquitous in today's world. The following article is a special case: It is about AI, written by AI, which should serve to demonstrate the amazing capabilities of this new tool, and its use in disaster recovery planning.

The Impact of Artificial Intelligence on Business Resilience and Disaster Recovery (BR/DR)

Executive summary

Artificial intelligence (AI) is reshaping core practices across business resilience and disaster recovery (BR/DR). Three capabilities are especially consequential for organizations of all sizes: (i) risk prediction, where machine-learning models improve hazard, cyber, and system-failure forecasts; (ii) automated incident response, where AI-enabled detection, triage, and orchestration shorten mean time to detect/respond (MTTD/MTTR); and (iii) AI-driven simulations, where digital twins and agent-based models stress-test interdependent systems and response plans. In Canada, these developments intersect with an evolving risk landscape—escalating climate-related

Prologue :

La politique générale de ce magazine est de décourager l'utilisation de l'IA pour la rédaction d'articles destinés à TNR. Nous estimons que notre **contenu doit être créé par des humains**. En effet, il est honteusement malhonnête de revendiquer la paternité d'un article qui a été rédigé en tout ou en partie par une application d'IA (comme ChatGBT) sans le mentionner. Néanmoins, l'intelligence artificielle est de plus en plus omniprésente dans le monde actuel. L'article suivant est un cas particulier : il traite de l'IA, est rédigé par une IA et vise à démontrer les capacités étonnantes de ce nouvel outil, ainsi que son utilisation dans la planification de la reprise après sinistre.

L'impact de l'intelligence artificielle sur la résilience des entreprises et la reprise après sinistre (BR/DR)

Résumé

L'intelligence artificielle (IA) est en train de remodeler les pratiques fondamentales en matière de résilience des entreprises et de reprise après sinistre. Trois capacités sont particulièrement importantes pour les organisations de toutes tailles : (i) la prédiction des risques, où les modèles d'apprentissage automatique améliorent les prévisions en matière de dangers, de cybercriminalité et de défaillance des systèmes ; (ii) la réponse automatisée aux incidents, où la détection, le triage et l'orchestration basés

losses, sophisticated cyber threats, and aging critical infrastructure—along with domestic standards and guidance (CSA Z1600, OSFI Guideline B-13, the Canadian Centre for Cyber Security's Top 10 IT Security Actions and Ransomware Playbook, Public Safety Canada's National Risk Profile, and Natural Resources Canada's Earthquake Early Warning rollout). Together, they provide a practical foundation for responsible adoption.

Key takeaways for BR/DR professionals:

- **Risk prediction:** AI already augments wildfire ignition likelihood, smoke dispersion, and flood-susceptibility forecasts; in parallel, cyber threat intelligence is increasingly AI-enabled on both sides of the offence–defence divide. Integrating these signals with business impact analyses can materially enhance readiness and prioritization.

- **Automated incident response (AIR):** AI embedded in EDR/XDR/SIEM/SOAR stacks curates alerts, correlates indicators, proposes playbook steps, and can trigger controlled actions (isolation, containment, rollback). Updated guidance (e.g., NIST SP 800-61 Rev. 3) emphasizes lifecycle integration with risk management. Canadian sectoral guidance (e.g., OSFI B-13) codifies expectations for regulated entities.

- **AI-driven simulations:** Digital twins and agent-based models allow "what-if" rehearsal of cascading events (wildfires, floods, cyber-physical outages), validating plans under dynamic conditions and informing investment trade-offs. Adoption is advancing in utilities and public safety.

The report that follows provides a concise evidence-based synthesis and a practical adoption roadmap for organizations operating in Canada and beyond.

---

1) Context: A risk environment trending upward in frequency, severity, and interdependence

Canada has experienced repeated years with **>$3 billion** in insured losses from severe weather, reflecting higher wildfire, flood, and convective storm impacts; 2023 alone exceeded $3.1 billion. Public Safety Canada's first **National Risk Profile (NRP)** (2023) prioritizes **floods, wildland fires,**

sur l'IA réduisent le temps moyen de détection/réponse (MTTD/MTTR) ; et (iii) les simulations basées sur l'IA, où les jumeaux numériques et les modèles basés sur des agents testent les systèmes interdépendants et les plans d'intervention. Au Canada, ces développements se recoupent avec un paysage de risques en évolution - augmentation des pertes liées au climat, cybermenaces sophistiquées et infrastructures essentielles vieillissantes - ainsi qu'avec des normes et des orientations nationales (CSA Z1600, ligne directrice B-13 du BSIF, Top 10 IT Security Actions and Ransomware Playbook du Centre canadien de cybersécurité, profil de risque national de Sécurité publique Canada et déploiement du système d'alerte précoce en cas de tremblement de terre de Ressources naturelles Canada). Ensemble, ils constituent une base pratique pour une adoption responsable.

Principaux enseignements pour les professionnels du BR/DR :

- **Prévision des risques :** L'IA améliore déjà la probabilité de déclenchement des incendies de forêt, la dispersion des fumées et les prévisions de vulnérabilité aux inondations ; parallèlement, les renseignements sur les cybermenaces sont de plus en plus alimentés par l'IA des deux côtés de la ligne de partage entre l'offensive et la défensive. L'intégration de ces signaux aux analyses d'impact sur l'activité peut améliorer sensiblement l'état de préparation et l'établissement des priorités.

- **Réponse automatisée aux incidents (AIR) :** L'IA intégrée dans les piles EDR/XDR/SIEM/SOAR recueille les alertes, met en corrélation les indicateurs, propose des étapes de jeu et peut déclencher des actions contrôlées (isolement, confinement, retour en arrière). Les orientations actualisées (par exemple, NIST SP 800-61 Rev. 3) mettent l'accent sur l'intégration du cycle de vie dans la gestion des risques. Les orientations sectorielles canadiennes (par exemple, OSFI B-13) codifient les attentes des entités réglementées.

- **Simulations pilotées par l'IA :** Les jumeaux numériques et les modèles basés sur des agents permettent de répéter des événements en cascade (feux de forêt, inondations, pannes cyber-physiques), de valider des plans dans des conditions dynamiques

and earthquakes, underscoring the need for nationwide capability uplift.

On the cyber front, the Canadian Centre for Cyber Security (CCCS) assesses that state and criminal actors remain the primary risk to organizations, and its 2025 update on threats to democratic processes explicitly highlights **AI-enabled operations** (e.g., scalable spear-phishing, deepfakes, and automated content operations).

These trends increase the value of **anticipation, acceleration, and adaptation**—all domains where AI can be applied to strengthen BR/DR programs.

2) AI for risk prediction

2.1 Natural hazards

Wildfire. Federal and provincial agencies operate mature modeling and monitoring systems—e.g., Natural Resources Canada's **Canadian Wildland Fire Information System (CWFIS)** and Environment and Climate Change Canada's **FireWork** smoke forecast—but machine learning is now being layered atop these assets. Examples include provincial tools predicting next-day ignition probability and research at national scale on wildfire occurrence and smoke impacts. AI models improve lead time and spatial specificity for resource pre-positioning, air-quality advisories, and continuity triggers (e.g., remote work, filtration upgrades).

Flood. Canada's **Flood Hazard Identification and Mapping Program (FHIMP)** (2023–2028) funds modern flood maps and data products; in parallel, Canadian researchers have demonstrated ML models for river discharge and flood susceptibility. Organizations can integrate these probabilistic forecasts with asset and supply-chain exposure to automate

et d'éclairer les choix d'investissement. L'adoption progresse dans les services publics et la sécurité publique.

Le rapport qui suit fournit une synthèse concise fondée sur des données probantes et une feuille de route pratique pour l'adoption par les organisations opérant au Canada et au-delà.

1) Le contexte : Un environnement de risques dont la fréquence, la gravité et l'interdépendance tendent à augmenter.

Le Canada a connu à plusieurs reprises des années où les pertes assurées dues aux phénomènes météorologiques violents ont été supérieures à 3 milliards de dollars, en raison de l'impact plus important des incendies de forêt, des inondations et des tempêtes convectives ; l'année 2023 a dépassé à elle seule les 3,1 milliards de dollars. Le premier **profil national des risques (PNR)** de Sécurité publique Canada (2023) donne la priorité aux inondations, aux incendies de forêt et aux tremblements de terre, soulignant la nécessité de renforcer les capacités à l'échelle nationale.

Sur le front cybernétique, le Centre canadien de cybersécurité (CCCS) estime que les acteurs étatiques et criminels restent le principal risque pour les organisations, et sa mise à jour de 2025 sur les menaces pesant sur les processus démocratiques met explicitement l'accent sur **les opérations fondées sur l'IA** (par exemple, le spear-phishing évolutif, les deepfakes et les opérations de contenu automatisées).

Ces tendances augmentent la valeur de l'anticipation, de l'accélération et de l'adaptation - autant de domaines où l'IA peut être appliquée pour renforcer les programmes de RE/RD.

2) L'IA pour la prévision des risques

2.1 Risques naturels

Incendies de forêt. Les agences fédérales et provinciales exploitent des systèmes de modélisation et de surveillance éprouvés, par exemple l**e Système canadien d'information sur les feux de végétation (SCIFV)** de Ressources naturelles Canada et les prévisions de fumée **FireWork** d'Environnement et Changement climatique Canada, mais l'apprentissage automatique se superpose désormais à ces actifs. Les exemples incluent des outils provinciaux prédisant la probabilité d'allumage le lendemain et la recherche à l'échelle nationale sur l'occurrence des incendies de forêt et les impacts de la fumée. Les modèles d'IA améliorent les délais et la spécificité spatiale pour le prépositionnement des ressources, les avis sur la qualité de l'air et les déclencheurs de continuité (par exemple, le travail à distance, les mises à niveau de la filtration).

readiness thresholds (e.g., staging generators, hardening data-centre intakes, switching to alternate transport corridors).

Earthquakes. Natural Resources Canada launched **Earthquake Early Warning (EEW)** operations in British Columbia in 2024 and is extending coverage to Ontario and Quebec. EEW delivers seconds to tens of seconds of notice—enough to automate protective actions (open fire-station bay doors, slow trains, pause surgeries), and to trigger enterprise protective playbooks. While EEW is not an AI system per se, organizations can connect EEW triggers to AI-assisted decision logic to optimize actuation (e.g., selecting which industrial process lines to pause based on real-time risk/recovery models).

2.2 Cyber risk and threat intelligence

CCCS's **National Cyber Threat Assessments** describe a landscape of ransomware, supply-chain compromises, and exploitation of cloud and remote access pathways, with adversaries increasingly leveraging AI to scale reconnaissance and social engineering. Risk prediction here involves (a) fusing external indicators (threat intel, dark-web telemetry, vulnerability feeds) with (b) internal telemetry (asset inventories, patch posture, identity graphs) to produce **risk-of-compromise** scores that schedule hardening and tabletop exercises.

2.3 System failures and reliability

Predictive maintenance and **AIOps** methods help anticipate equipment and service degradation across IT and OT. Canadian utilities are piloting AI to forecast vegetation-related outages and to improve load forecasting—measures that directly reduce service interruptions and restoration times. In BR/DR terms,

Inondations. Le programme **canadien d'identification et de cartographie des risques d'inondation (FHIMP)** (2023-2028) finance des cartes et des produits de données modernes sur les inondations ; parallèlement, des chercheurs canadiens ont mis au point des modèles ML pour le débit des rivières et la susceptibilité aux inondations. Les organisations peuvent intégrer ces prévisions probabilistes à l'exposition des actifs et de la chaîne d'approvisionnement afin d'automatiser les seuils de préparation (par exemple, mise en attente des générateurs, renforcement des prises d'eau des centres de données, passage à d'autres couloirs de transport).

Tremblements de terre. Ressources naturelles Canada a lancé des opérations **d'alerte précoce aux tremblements de terre (EEW)** en Colombie-Britannique en 2024 et étend la couverture à l'Ontario et au Québec. Le système EEW fournit un préavis de quelques secondes à quelques dizaines de secondes, suffisant pour automatiser les mesures de protection (ouvrir les portes des casernes de pompiers, ralentir les trains, interrompre les opérations chirurgicales) et pour déclencher les plans de protection de l'entreprise. Bien que le système EEW ne soit pas un système d'intelligence artificielle en soi, les entreprises peuvent relier les déclencheurs EEW à une logique décisionnelle assistée par l'intelligence artificielle afin d'optimiser les actions (par exemple, en sélectionnant les lignes de processus industriel à mettre en pause sur la base de modèles de risque et de récupération en temps réel).

2.2 Risques cybernétiques et renseignements sur les menaces

Les évaluations nationales de la CCCS sur les cybermenaces décrivent un paysage de ransomware, de compromissions de la chaîne d'approvisionnement et d'exploitation des voies d'accès en nuage et à distance, les adversaires utilisant de plus en plus l'IA pour intensifier la reconnaissance et l'ingénierie sociale. La prédiction des risques implique ici (a) la fusion d'indicateurs externes (renseignements sur les menaces, télémétrie du dark-web, flux de vulnérabilités) avec (b) la télémétrie interne (inventaires des actifs, position des correctifs, graphes d'identité) pour produire des scores de risque de compromission qui planifient le renforcement et les exercices de simulation.

2.3 Défaillances et fiabilité du système

Les méthodes de maintenance prédictive et d'**AIOps** permettent d'anticiper la dégradation des équipements et des services dans les domaines de l'informatique et des technologies de l'information. Les services publics canadiens pilotent l'IA pour prévoir les pannes liées à la végétation et pour améliorer les prévisions de charge - des mesures qui réduisent directement les interruptions de service

these models inform **RTO/RPO-aware** failover plans and maintenance windows to minimize business impact.

Implication for practice. Bring AI-based hazard, cyber, and reliability forecasts into the **Risk Register** and **Business Impact Analysis** (BIA): map model outputs to concrete triggers (e.g., "Ignition likelihood > X in service area → enable remote-work posture; Flood return-period forecast at site Y → pre-position pumps; Surge in identity-based intrusion attempts → step-up MFA challenges and SOC staffing").

3) AI-assisted, automated incident response

AI is now embedded across the incident lifecycle:

- **Detection and triage**. Supervised and unsupervised ML on EDR/XDR data clusters related alerts, identifies anomalous sequences, and suppresses noise; LLM-based explainers draft analyst context and propose next steps.
- **Containment and orchestration.** SOAR platforms use rules plus ML to automate isolation (e.g., kill switch, network quarantine), block indicators, and orchestrate credential resets—subject to human approval for high-risk actions.
- **Recovery and lessons-learned.** AI helps reconstruct timelines, correlate logs, and evaluate playbook effectiveness for continuous improvement.

Recent guidance (NIST **SP 800-61 Rev. 3**) integrates incident response with the CSF 2.0 risk-management functions—preparation, detection, analysis, containment, eradication, recovery, and post-incident activities—providing a structure into which AI automation can be safely embedded. For Canadian federally regulated financial institutions,

et les délais de rétablissement. En termes de BR/DR, ces modèles informent les **RTO/RPO** des plans de basculement et des fenêtres de maintenance afin de minimiser l'impact sur l'activité.

Implication pour la pratique. Intégrer les prévisions en matière d'aléas, de cybernétique et de fiabilité fondées sur l'IA dans le registre des risques et l'analyse d'impact sur l'activité (BIA) : associer les résultats du modèle à des déclencheurs concrets (par exemple, "probabilité d'inflammation > X dans la zone de service → mise en place d'une posture de travail à distance ; prévision de la période de retour des inondations sur le site Y →prépositionnement des pompes ; augmentation des tentatives d'intrusion fondées sur l'identité → intensification des défis de l'AMF et de la dotation en personnel du SOC").

3) Réponse automatisée aux incidents assistée par l'IA

L'IA est désormais intégrée dans le cycle de vie des incidents :

- **Détection et triage.** La ML supervisée et non supervisée sur les données EDR/XDR regroupe les alertes connexes, identifie les séquences anormales et supprime le bruit ; les explicateurs basés sur la LLM rédigent le contexte de l'analyste et proposent les étapes suivantes.
- **Confinement et orchestration**. Les plateformes SOAR utilisent des règles et la ML pour automatiser l'isolement (par exemple, kill switch, quarantaine réseau), bloquer les indicateurs et orchestrer les réinitialisations d'identifiants - sous réserve de l'approbation humaine pour les actions à haut risque.
- **Récupération et enseignements tirés**. L'IA aide à reconstruire les chronologies, à corréler les journaux et à évaluer l'efficacité des playbooks pour une amélioration continue.

Des orientations récentes (NIST **SP 800-61 Rev. 3**) intègrent la réponse aux incidents aux fonctions de gestion des risques du CSF 2.0 (préparation, détection, analyse, confinement, éradication, récupération et activités post-incident), fournissant ainsi une structure dans laquelle l'automatisation de l'IA peut être intégrée en toute sécurité. Pour les institutions financières canadiennes sous réglementation fédérale, la ligne directrice **B-13 du BSIF** définit les attentes en matière de gestion des risques technologiques et cybernétiques, en mettant l'accent sur la gouvernance, les risques liés aux tiers et la résilience. Associez-les aux **10 principales mesures de sécurité** des TI et au guide sur les rançongiciels de la CCCS pour aligner l'automatisation sur les bonnes pratiques nationales.

Attention. Les évaluations de la CCCS font également état de l'utilisation de l'IA par les adversaires ; l'automatisation qui ne peut

OSFI Guideline B-13 establishes expectations for technology and cyber risk management, emphasizing governance, third-party risk, and resilience. Pair these with CCCS's **Top 10 IT Security Actions and Ransomware Playbook** to align automation with national good practice.

Caution. CCCS assessments also note adversaries' use of AI; automation that cannot withstand prompt-injection, data poisoning, or adversarial inputs may amplify harm. Guardrails (policy enforcement, strong identity, change-control, and **human-in-the-loop** approvals) are essential.

4) AI-driven simulations and digital twins

AI-enabled **digital twins** of facilities, networks, and communities can simulate cascading impacts (e.g., wildfire encroachment, smoke infiltration, utility outages; or ransomware-driven IT/OT segmentation). Utilities report adoption for scenario testing and grid reliability; public-safety research in Canada highlights their relevance for flood management and inter-agency coordination. For BR/DR, this capability allows validation of **continuity strategies** (alternate sites, alternate suppliers, manual workarounds) under realistic, time-evolving stressors.

Agent-based and traffic simulations, often coupled with machine learning, support **evacuation planning** (e.g., hospital or campus egress, transport choke-points), enabling organizations to test communications and logistics plans pre-incident.

5) Canadian standards, policy, and reference frameworks

- **Emergency & continuity management. CSA Z1600:17 (R2022**) is Canada's emergency and continuity management program

résister à l'injection rapide, à l'empoisonnement des données ou aux intrants des adversaires peut amplifier les dommages. Les garde-fous (application des politiques, identité forte, contrôle des changements et approbations **humaines en boucle**) sont essentiels.

4) Simulations pilotées par l'IA et jumeaux numériques

Les jumeaux numériques d'installations, de réseaux et de communautés basés sur l'IA peuvent simuler des impacts en cascade (par exemple, l'empiètement d'un feu de forêt, l'infiltration de fumée, les pannes de services publics ou la segmentation IT/OT causée par un ransomware). Les services publics font état d'une adoption pour les tests de scénarios et la fiabilité du réseau ; la recherche en matière de sécurité publique au Canada souligne leur pertinence pour la gestion des inondations et la coordination inter-agences. En ce qui concerne la RB/RD, cette capacité permet de valider **les stratégies de continuité** (sites alternatifs, fournisseurs alternatifs, solutions de contournement manuelles) dans le cadre de facteurs de stress réalistes et évoluant dans le temps.

Les simulations de trafic et les simulations basées sur des agents, souvent associées à l'apprentissage automatique, soutiennent la planification de l'évacuation (par exemple, l'évacuation d'un hôpital ou d'un campus, les points d'étranglement des transports), permettant aux organisations de tester les plans de communication et de logistique avant l'incident.

5) Normes, politiques et cadres de référence canadiens

- **Gestion des urgences et de la continuité. La norme CSA Z1600:17 (R2022)** est la norme canadienne relative aux programmes de gestion des urgences et de la continuité ; une nouvelle édition est en cours d'élaboration afin d'intégrer explicitement la résilience climatique. Il est conseillé de s'aligner sur la norme ISO 22301 à des fins de comparabilité internationale.

- **Orientations sectorielles. La norme B-13** du BSIF définit les attentes en matière de technologie et de risque cybernétique pour les institutions financières sous réglementation fédérale, notamment en ce qui concerne la gouvernance et la résilience ; ses principes sont largement applicables à d'autres secteurs.

- **Pratique de la cybersécurité. Les 10 principales mesures de sécurité** informatique et le guide des rançongiciels (Ransomware Playbook) de la CCCS fournissent des contrôles applicables et des listes de contrôle qui peuvent être complétés — mais non remplacés—par l'IA.

standard; a new edition is being developed to explicitly incorporate climate resiliency. Alignment with **ISO 22301** remains advisable for international comparability.

- **Sectoral guidance. OSFI B-13** sets technology/cyber risk expectations for federally regulated financial institutions, including governance and resilience; its principles are broadly applicable to other sectors.
- **Cybersecurity practice. CCCS's Top 10 IT Security Actions and Ransomware Playbook** provide implementable controls and response checklists that can be augmented—but not replaced—by AI.
- **Risk landscape evidence.** Public Safety Canada's **National Risk Profile (2023)** establishes national priorities (flood, fire, earthquakes); NRCan's **EEW** program is moving to national coverage. **FHIMP** funds modern, accessible flood mapping—data AI systems can ingest.
- **AI governance and privacy**. In the federal domain, the **Directive on Automated Decision-Making (DADM)** and its **Algorithmic Impact Assessment (AIA)** tool provide a structured approach to AI risk, complemented by the 2025 **AI Strategy for the Federal Public Service** and the **OPC's** principles for responsible, privacy-protective generative AI. (Note: Canada has not enacted a comprehensive federal AI law as of mid-2025.) Organizations can adapt these instruments for private-sector AI risk governance.

6) Risks, limits, and responsible use

Model validity & drift. Hazard and operational data are non-stationary; models degrade as climate and threat actors change. Establish **model cards**, periodic back-testing, and drift alarms.

- **Données sur le paysage des risques. Le profil de risque national (2023)** de Sécurité publique Canada établit les priorités nationales (inondations, incendies, tremblements de terre) ; le programme **EEW** de RNCan passe à une couverture nationale. Le programme **FHIMP** finance une cartographie moderne et accessible des inondations - des données que les systèmes d'IA peuvent ingérer.
- **Gouvernance de l'IA et protection de la vie privée.** Dans le domaine fédéral, la **Directive sur la prise de décision automatisée (DADM)** et son outil d'évaluation de l'impact des algorithmes **(EAI)** fournissent une approche structurée des risques liés à l'IA, complétée par **la Stratégie 2025 sur l'IA pour la fonction publique fédérale** et les principes du CPVP pour une IA générative responsable et protectrice de la vie privée. (Les organisations peuvent adapter ces instruments à la gouvernance des risques liés à l'IA dans le secteur privé.

6) Risques, limites et utilisation responsable

Validité et dérive des modèles. Les dangers et les données opérationnelles ne sont pas stationnaires ; les modèles se dégradent à mesure que le climat et les acteurs de la menace changent. Établir des cartes de modèles, des tests rétroactifs périodiques et des alarmes de dérive.

Sécurité de l'IA elle-même. Les défenseurs doivent partir du principe que les adversaires cibleront les données d'entraînement, les messages-guides et les chaînes d'approvisionnement des modèles. Les rapports de la CCCS sur les menaces qui pèsent sur les opérations basées sur l'IA soulignent la nécessité de mettre en place des modèles en équipe restreinte et d'isoler les automatismes à haut risque derrière des approbations.

Confidentialité et gouvernance des données. Les modèles d'IA nécessitent souvent des données sensibles. Les organisations opérant au Canada doivent s'aligner sur les orientations du CPVP et anticiper l'évolution de la réglementation ; appliquer la minimisation des données, la limitation des finalités et la transparence, en particulier pour les cas d'utilisation liés à la surveillance et à la sécurité de la main-d'œuvre.

Jugement humain. Les études sur l'IA dans l'aide à la décision en cas de catastrophe soulignent que l'IA ne doit pas remplacer le jugement d'un expert dans des contextes à fort enjeu ; elle doit être conçue pour augmenter la prise de décision et non pour l'autonomiser.

Security of AI itself. Defenders must assume adversaries will target training data, prompts, and model supply chains. CCCS's threat reporting on AI-enabled operations underscores the need for **red-teaming** models and isolating high-risk automations behind approvals.

Privacy and data governance. AI models often require sensitive data. Organizations operating in Canada should align with **OPC** guidance and anticipate evolving regulation; apply data minimization, purpose limitation, and transparency, especially for monitoring and workforce-safety use cases.

Human judgment. Studies of AI in disaster decision-support emphasize that AI should not replace expert judgment in high-stakes contexts; design for decision **augmentation**, not autonomy.

7) Implementation roadmap (12–24 months)

Phase 1: Establish governance and foundations (0–3 months).

- Create an **AI-for-Resilience Charter** that maps to CSA Z1600, ISO 22301, OSFI B-13 (if applicable), CCCS guidance, and your privacy obligations.
- Stand up **data pipelines** to ingest authoritative Canadian signals: CWFIS/FireWork, FHIMP, EEW alerts, municipal hazard layers; ingest CCCS advisories and vulnerabilities for cyber risk scoring.
- Define **automation guardrails**: change control, human-in-the-loop approvals, rollout rings, and rollback criteria tied to NIST SP 800-61 phases.

Phase 2: Pilot use cases with measurable outcomes (3–9 months).

- **Risk-to-trigger integration**. Connect wildfire/flood risk forecasts

7) Feuille de route pour la mise en œuvre (12-24 mois)

Phase 1 : Établir la gouvernance et les fondations (0-3 mois).

- Créez une **charte de l'IA pour la résilience** qui correspond aux normes CSA Z1600, ISO 22301, OSFI B-13 (le cas échéant), aux orientations de la CCCS et à vos obligations en matière de protection de la vie privée.
- Mettre en place **des pipelines** de données pour ingérer des signaux canadiens faisant autorité : CWFIS/FireWork, FHIMP, alertes EEW, couches de danger municipales ; ingérer les avis du CCCS et les vulnérabilités pour l'évaluation du risque cybernétique.
- **Définir les garde-fous de l'automatisation :** contrôle des changements, approbations humaines dans la boucle, anneaux de déploiement et critères de retour en arrière liés aux phases de la norme NIST SP 800-61.

Phase 2 : cas d'utilisation pilotes avec des résultats mesurables (3-9 mois).

- **Intégration du risque au déclenchement.** Connecter les prévisions de risques d'incendies et d'inondations aux changements de posture des installations et du personnel (filtres, télétravail, réacheminement logistique).
- **Automatisation du SOC.** Déployer des playbooks SOAR qui utilisent l'IA pour l'enrichissement et le guidage des opérateurs, mais qui nécessitent une approbation pour des actions telles que la désactivation de comptes ou la micro-segmentation. Associer avec le playbook ransomware de la CCCS.
- **AIOps pour la fiabilité.** Essayer la maintenance prédictive sur les actifs critiques (HVAC, UPS, équipement de distribution) et pour les anomalies de performance des applications ; lorsque cela est possible, adopter les pratiques éprouvées des services publics canadiens (prédiction des pannes liées à la végétation, amélioration de la modélisation de la charge).

Phase 3 : passer aux simulations et à l'échelle de l'entreprise (9 à 18 mois).

- Construire des simulations numériques jumelées (installation/campus, processus critiques) qui injectent des scénarios de danger, de cybernétique et de chaîne d'approvisionnement ; vérifier les stratégies de continuité en situation de stress.
- Intégrer des exercices sur table avec télémétrie simulée et actions suggérées par le modèle ; évaluer la confiance des opérateurs et la qualité des décisions.

Phase 4 : Amélioration continue (en cours).

- Institutionnaliser la gestion des risques liés aux modèles

to facility and workforce posture changes (filters, telework, logistics rerouting).

- **SOC automation**. Deploy SOAR playbooks that use AI for enrichment and operator guidance—but require approval for actions like account disablement or micro-segmentation. Pair with CCCS's ransomware playbook.
- **AIOps for reliability.** Trial predictive maintenance on critical assets (HVAC, UPS, distribution gear) and for application performance anomalies; where feasible, adopt proven Canadian utility practices (vegetation-related outage prediction, improved load modeling).

Phase 3: Expand to simulations and enterprise scale (9–18 months).

- Build digital-twin simulations (facility/campus, critical processes) that inject hazard, cyber, and supply-chain scenarios; verify continuity strategies under stress.
- Integrate **tabletop exercises** with simulated telemetry and model-suggested actions; evaluate operator trust and decision quality.

Phase 4: Continuous improvement (ongoing).

- Institutionalize **model risk management** (validation, drift checks, incident logging specific to AI faults).
- Track **resilience KPIs**: MTTD/MTTR, false-positive rate, % of incidents with automated containment, % of sites with forecast-linked readiness triggers, exercise performance deltas, and loss-avoidance estimates benchmarked to hazard seasons.

8) Practical architecture patterns

- **Data & features**. Curate authoritative feeds (CWFIS hotspots and indices, FireWork PM2.5 forecasts, FHIMP layers, EEW alerts; security intel; asset/identity inventories). Harmonize via a **feature store** with lineage and quality checks.
- **Model services**. Separate **predictive services** (e.g., flood susceptibility, ignition likelihood, anomaly detection) from **decision services** (playbooks). Implement **policy-as-code** to gate automated actions by risk tier.
- **Control plan.** Use SOAR to orchestrate

(validation, contrôles de dérive, enregistrement des incidents spécifiques aux défaillances de l'IA).

- **Suivre les indicateurs clés de résilience :** MTTD/MTTR, taux de faux positifs, % d'incidents avec confinement automatisé, % de sites avec des déclencheurs de préparation liés aux prévisions, deltas de performance des exercices et estimations d'évitement des pertes par rapport aux saisons de danger.

8) Modèles d'architecture pratiques

- **Données et caractéristiques.** Constituer des flux faisant autorité (points chauds et indices CWFIS, prévisions FireWork PM2.5, couches FHIMP, alertes EEW ; renseignements de sécurité ; inventaires de biens et d'identités). Harmonisation par le biais d'un magasin de fonctionnalités avec des contrôles de lignage et de qualité.
- **Services de modélisation.** Séparer les services prédictifs (par exemple, susceptibilité aux inondations, probabilité d'inflammation, détection des anomalies) des services de décision (playbooks). Mettre en œuvre une politique en tant que code pour contrôler les actions automatisées par niveau de risque.
- **Plan de contrôle.** Utiliser SOAR pour orchestrer les actions entre IT/OT, identité et installations (par exemple, les modes du système de badge, les points de consigne du BMS) avec des approbations explicites pour les changements à fort impact. S'aligner sur la norme NIST SP 800-61 pour les étapes de réponse.
- **Assurance.** Enregistrer toutes les décisions assistées par l'IA, conserver des ensembles de données pour les rejouer et mener des examens après action qui calibrent à la fois les modèles et les playbooks. Lorsque des données personnelles sont impliquées, documenter les évaluations des risques et les mesures d'atténuation de type AIA.

9) Notes sectorielles pour les organisations canadiennes

- **Secteur public / municipalités.**

actions across IT/OT, identity, and facilities (e.g., badge-system modes, BMS set-points) with explicit approvals on high-impact changes. Align with NIST SP 800-61 for response stages.

- **Assurance**. Log all AI-assisted decisions, maintain datasets for replay, and conduct **after-action reviews** that calibrate both models and playbooks. Where personal data is involved, document AIA-style risk assessments and mitigations.

9) Sector notes for Canadian organizations

- **Public sector / municipalities**. Leverage the Government of Canada's 2025 **AI Strategy** and **Generative AI Guide** for governance scaffolding; combine with FHIMP and NRP products for hazard-aware service delivery.
- **Financial services**. Map AIR practices to **OSFI B-13**, stress-test third-party and concentration risks (including cloud and AI service providers), and ensure tabletop exercises reflect AI-enabled fraud and social-engineering campaigns.
- **Energy & utilities**. Expand pilots in predictive maintenance and grid simulations; Canadian case work (e.g., Hydro-Québec vegetation and inspection analytics) suggests concrete reliability gains relevant to continuity targets.

Conclusion

AI is not a panacea; it is a force multiplier when anchored in sound governance, calibrated to trustworthy Canadian data sources, and embedded in disciplined BR/DR processes. For risk prediction, automated incident response, and simulation, the path to value is pragmatic: start with well-scoped use cases, wire model outputs to **explicit triggers**, preserve human authority for high-impact actions, and continuously validate outcomes. Anchoring adoption in Canadian standards and guidance—CSA Z1600, OSFI B-13, CCCS best practices, NRP and FHIMP data, NRCan's EEW—will accelerate benefits while keeping defenses robust against adversaries who are themselves increasingly AI-enabled. Ω

Tirer parti de la stratégie d'IA 2025 du gouvernement du Canada et du Guide d'IA générative pour l'échafaudage de la gouvernance ; combiner avec les produits FHIMP et NRP pour la prestation de services tenant compte des aléas.

- **Services financiers**. Faire correspondre les pratiques de RIA à la norme **B-13 du BSIF**, effectuer des tests de stress sur les risques liés aux tiers et à la concentration (y compris les fournisseurs de services d'informatique en nuage et d'IA), et veiller à ce que les exercices de simulation tiennent compte des campagnes de fraude et d'ingénierie sociale fondées sur l'IA.
- **Énergie et services publics**. Élargir les projets pilotes de maintenance prédictive et les simulations de réseau ; les études de cas canadiennes (par exemple, l'analyse de la végétation et de l'inspection d'Hydro-Québec) suggèrent des gains de fiabilité concrets pertinents pour les objectifs de continuité.

Conclusion

L'IA n'est pas une panacée ; c'est un multiplicateur de force lorsqu'elle est ancrée dans une gouvernance saine, calibrée sur des sources de données canadiennes dignes de confiance et intégrée dans des processus disciplinés de RE/RD. Pour la prédiction des risques, la réponse automatisée aux incidents et la simulation, le chemin vers la valeur est pragmatique : commencer par des cas d'utilisation bien définis, relier les sorties du modèle à des déclencheurs explicites, préserver l'autorité humaine pour les actions à fort impact et valider continuellement les résultats. L'ancrage de l'adoption dans les normes et les directives canadiennes - CSA Z1600, OSFI B-13, pratiques exemplaires de la CCCS, données du PNR et du FHIMP, TEE de RNCan - accélérera les avantages tout en maintenant des défenses solides contre les adversaires qui sont eux-mêmes de plus en plus dotés de capacités d'IA. Ω

ABOUT THE AUTHOR

ChatGPT-5

*ChatGPT-5 features a unified system with built-in reasoning, automatically switching between standard and "**Thinking**" modes for complex tasks, resulting in more accurate and efficient responses. GPT-5 Thinking provides deeper, step-by-step analysis, especially beneficial for coding, scientific questions, and financial analysis, significantly improving performance over older models. This advanced reasoning capability allows GPT-5 to handle complex work more effectively, reducing errors and providing more intelligent solutions for users' needs.*

À PROPOS DE L'AUTEUR

ChatGPT-5

ChatGPT-5 dispose d'un système unifié avec raisonnement intégré, passant automatiquement du mode standard au mode « Thinking » pour les tâches complexes, ce qui permet d'obtenir des réponses plus précises et plus efficaces. GPT-5 Thinking fournit une analyse plus approfondie, étape par étape, particulièrement utile pour le codage, les questions scientifiques et l'analyse financière, améliorant considérablement les performances par rapport aux anciens modèles. Cette capacité de raisonnement avancée permet à GPT-5 de traiter plus efficacement les tâches complexes, en réduisant les erreurs et en fournissant des solutions plus intelligentes pour répondre aux besoins des utilisateurs.

Referenced literature (selected) / Bibliographie référencée (sélection)

1. Insurance Bureau of Canada (IBC). "Severe Weather in 2023 Caused Over $3.1 Billion in Insured Damage." 8 Jan 2024. (IBC)
2. Public Safety Canada. National Risk Profile – First Public Report. 2023. (Public Safety Canada)
3. Natural Resources Canada / Canadian Forest Service. Canadian Wildland Fire Information System (CWFIS). Ongoing. (cwfis.cfs.nrcan.gc.ca)
4. Environment and Climate Change Canada. FireWork Air Quality Model Forecast Maps. Ongoing service. (Environment Canada Weather)
5. Natural Resources Canada. Earthquake Early Warning (EEW) System. Operational in B.C. since 2024; expansion to ON/QC underway. (earthquakescanada.nrcan.gc.ca)
6. Natural Resources Canada & Government of B.C. News release on EEW launch in western Canada. 30 Aug 2024. (Canada.ca)
7. Natural Resources Canada. Flood Hazard Identification and Mapping Program (FHIMP). Program materials and guide. 2023–2028. (Natural Resources Canada, Government of Canada Publications)
8. Concordia University. "AI to Predict River Discharge and Flood Risk (Ottawa River)." 18 Nov 2024. (Concordia University)
9. CCCS (Canadian Centre for Cyber Security). National Cyber Threat Assessment 2023–2024; Cyber threats to Canada's democratic process – 2025 update. (Open Canada, Canadian Centre for Cyber Security)
10. CCCS. Top 10 IT Security Actions; Ransomware Playbook (ITSM.00.099). (Canadian Centre for Cyber Security)
11. OSFI. Guideline B-13: Technology and Cyber Risk Management. 2022. (OSFI)
12. CSA Group. CSA Z1600:17 (R2022) – Emergency and continuity management program; Standards Council of Canada notice on new edition and climate resiliency. (CSA Group, scc-ccn.ca)

13. NIST. SP 800-61 Rev. 3 – Incident Response Recommendations and Considerations for Cybersecurity Risk Management. 2025. (NIST Publications)
14. Treasury Board of Canada Secretariat. Directive on Automated Decision-Making and Algorithmic Impact Assessment; AI Strategy for the Federal Public Service 2025–2027; Guide on the Use of Generative AI. (Government of Canada Publications, Canada.ca)

Epilogue:

The forgoing article "*Artificial Intelligence in Disaster Recovery Planning*" was **written entirely by Artificial Intelligence** (ChatGPT) just as an experiment to show how far the tool has come in a short time, and an exercise in effective prompting. This report is just a demo, and while it may contain useful information, it is in no way presented as a professionally endorsed paper. As some might say, it would have a ZeroGPT Score of 100% AI generated!

To create this report, Mr. Jenkins prompted OpenAI's ChatGPT 5 Thinking model as follows:

"Generate a research report on how business resilience and disaster recovery planning will be impacted by AI. The target audience is professionals working in the business resilience and disaster recovery field. The report should include consideration of natural disasters, cyberattacks, and system failures. Use Canadian references when and where possible. The impact of AI should be considered for all organizations in general. Consider AI for risk prediction, automated incident response, and AI-driven simulations. A report of approximately 1800 to 2000 words (no more than 2000 words) would be ideal. Provide a list of referenced literature at the end."

It took 3 minutes and 3 seconds to generate the report.

NB. ChatGPT also generated its own author photo (the robot).

Épilogue :

L'article précédent, intitulé « L'intelligence artificielle dans la planification de la reprise après sinistre », a été entièrement rédigé par l'intelligence artificielle (ChatGPT) à titre expérimental, afin de montrer les progrès réalisés par cet outil en peu de temps et d'illustrer l'efficacité des invites. Ce rapport n'est qu'une démonstration et, bien qu'il puisse contenir des informations utiles, il ne s'agit en aucun cas d'un document approuvé par des professionnels. Comme certains pourraient le dire, il aurait un score ZeroGPT de 100 % généré par l'IA !

Pour créer ce rapport, M. Jenkins a demandé au modèle ChatGPT 5 Thinking d'OpenAI de générer le contenu suivant :

« Générez un rapport de recherche sur l'impact de l'IA sur la résilience des entreprises et la planification de la reprise après sinistre. Le public cible est constitué de professionnels travaillant dans le domaine de la résilience des entreprises et de la reprise après sinistre. Le rapport doit inclure une réflexion sur les catastrophes naturelles, les cyberattaques et les pannes de système. Utilisez des références canadiennes dans la mesure du possible. L'impact de l'IA doit être pris en compte pour toutes les organisations en général. Tenez compte de l'IA pour la prévision des risques, la réponse automatisée aux incidents et les simulations basées sur l'IA. Un rapport d'environ 1 800 à 2 000 mots (pas plus de 2 000 mots) serait idéal. Fournissez une liste des références bibliographiques à la fin. »

La génération du rapport a pris 3 minutes et 3 secondes.

NB. ChatGPT a également généré sa propre photo d'auteur (le robot).

ABOUT THE PROMPTER

***Miles Jenkins** is retired after a 37-year career in IT, from roles in operations, programming, and network management, through technical sales and consulting. He keeps himself technically challenged by trying to stay abreast of developments in Artificial Intelligence.*

À PROPOS DU PROMPTEUR

***Miles Jenkins** a pris sa retraite après une carrière de 37 ans dans le domaine des technologies de l'information, où il a occupé divers postes dans les domaines de l'exploitation, de la programmation et de la gestion de réseaux, ainsi que dans la vente technique et le conseil. Il continue à se tenir à jour sur le plan technique en s'efforçant de suivre les développements dans le domaine de l'intelligence artificielle.*

Upcoming Events

DRI Canada is dedicated to providing continued professional development for its certified professionals through a variety of opportunities - whether it be one day, one hour or one lunch.

Symposia Series

DRIC symposiums are one-day events specifically designed for senior-level business continuity, disaster recovery, cyber resilience and risk management professionals. They aim to provide a dynamic and interactive platform for leaders to explore innovative strategies, share best practices, and discuss the latest trends in business continuity management.

Upcoming Date
November 20, 2025 - Hotel Lac-Leamy, Gatineau, Quebec

Professional Development Guest Speaker Lunch Series

Welcome to our Guest Speaker Lunch Series designed exclusively for DRIC certified professionals. This engaging event series brings industry leaders and subject-matter experts to the table, providing invaluable insights, strategies, and tools tailored to the unique challenges of our field.

Upcoming Date
November 25, 2025 - Victoria, British Columbia

Professional Development Webinar Series

Elevate your expertise with the Professional Development Webinar Series. This online series is designed to empower DRIC professionals with the latest insights, tools, and strategies in disaster recovery, business continuity, and risk management.

Upcoming Date
December 4, 2025

Log in and register for events at:
https://www.dri.ca/events.php

Événements à venir

DRI Canada se consacre à offrir un développement professionnel continu à ses professionnels certifiés à travers une variété d'opportunités - que ce soit une journée, une heure ou un déjeuner.

Série de colloques

Les symposiums DRIC sont des événements d'une journée spécialement conçus pour les professionnels de haut niveau en matière de continuité des activités, de reprise après sinistre, de cyber-résilience et de gestion des risques. Ils visent à fournir une plate-forme dynamique et interactive permettant aux dirigeants d'explorer des stratégies innovantes, de partager les meilleures pratiques et de discuter des dernières tendances en matière de gestion de la continuité des activités.

Date à venir

Le 20 novembre 2025 - Hotel Lac-Leamy, Gatineau, Quebec

Série de déjeuners de conférenciers invités en matière de développement professionnel

Bienvenue à notre série de déjeuners de conférenciers invités conçue exclusivement pour les professionnels certifiés DRIC. Cette série d'événements engageants rassemble des leaders de l'industrie et des experts en la matière, fournissant des informations, des stratégies et des outils inestimables adaptés aux défis uniques de notre domaine.

Date à venir

Le 25 novembre 2025 - Victoria, Colombie-Britannique

Série de webinaires sur le développement professionnel

Élevez votre expertise avec la série de webinaires de développement professionnel. Cette série en ligne est conçue pour donner aux professionnels de DRIC les dernières informations, outils et stratégies en matière de reprise après sinistre, de continuité des activités et de gestion des risques.

Date à venir

Le 4 décembre 2025

Connectez-vous et inscrivez-vous aux événements sur :
https://www.dri.ca/events.php

Artificial Confidence: The Illusion of AI-Led Resilience

Confiance Artificielle: l'illusion de la résilience induite par l'IA

By/Par Jason Firlotte, Jessa Cinnamon, with/avec ChatGPT

The Hidden Dangers of Relying Solely on Artificial Intelligence for Business Continuity and Disaster Recovery Planning

Introduction

In the past five years, artificial intelligence (AI) adoption in business continuity planning (BCP) and disaster recovery planning (DRP) has surged dramatically. A 2024 Gartner survey revealed that 68% of organizations now use AI-driven tools to assist their continuity strategies, up from 30% in 2019 (***Gartner, 2024***). These technologies promise faster risk assessment, automated crisis simulations, and improved decision-making.

However, this rapid adoption masks a critical misunderstanding: AI is not truly "intelligent." Most AI tools today are forms of machine learning—systems trained to recognize patterns in historical data. They do not comprehend context, interpret nuance, or reason through unforeseen scenarios. Furthermore, individuals who are not business continuity professionals lack the technical expertise or incident management experience to critically evaluate AI-generated plans.

Les dangers cachés liés au recours exclusif à l'intelligence artificielle pour la continuité des activités et la planification de la reprise après sinistre

Introduction

Au cours des cinq dernières années, l'adoption de l'intelligence artificielle (IA) dans la planification de la continuité des activités (BCP) et la planification de la reprise après sinistre (DRP) a fait un bond spectaculaire. Une enquête (Gartner de 2024) a révélé que 68 % des organisations utilisent désormais des outils pilotés par l'IA pour aider leurs stratégies de continuité, contre 30 % en 2019 (Gartner, 2024). Ces technologies promettent une évaluation plus rapide des risques, des simulations de crise automatisées et une amélioration de la prise de décision.

Toutefois, cette adoption rapide masque un malentendu majeur : L'IA n'est pas vraiment "intelligente". La plupart des outils d'IA actuels sont des formes d'apprentissage automatique – des systèmes formés pour reconnaître des modèles dans des données historiques. Ils ne comprennent pas le contexte, n'interprètent pas les nuances et ne raisonnent pas en fonction de scénarios imprévus. De plus, les personnes qui ne sont pas

This disconnect fosters a false sense of security—an "artificial confidence"—where organizations place undue trust in AI outputs without sufficient human oversight. This article explores the pitfalls of overreliance on AI in BCP and DRP, illustrated by recent real-world examples.

To write this article, Chat-GPT has been used as our co-author for this article. Chat-GPT was asked to write an article about the artificial confidence that comes with AI and provide examples of when AI failed, we have supplemented its observations with our own.

What is Intelligence?

The Webster dictionary defines Intelligence as: the ability to learn or understand or to deal with new or trying situations; the ability to apply knowledge to manipulate one's environment or to think abstractly as measured by objective criteria (such as tests); mental acuteness.

Comparing AI and humans, in the context of intelligence, it is clear that our ability to adapt to situations, including empathy, and not just repeating tasks is a distinct advantage. Artificial intelligence, while good at analyzing events and recognizing patterns, does not have consciousness, and cannot truly understand concepts, and is only as good as the information it has been provided. If there is any inaccurate, or missing information, AI cannot reason the way humans can, by pulling on their own experiences to bridge the gap between the past and unprecedented events.

However, there is more to business continuity and disaster recovery, which will be explored in this article. We will be discussing areas where artificial intelligence failed, and how experts could've performed differently.

When working in a field where unpredictable and unprecedented events can occur, it's crucial to have experts navigating disasters to leverage their experiences and adapt their knowledge to best fit the situations. AI is trained based on historical pattens and events which limits its ability to handle novel, complex

des professionnels de la continuité d'activité n'ont pas l'expertise technique ou l'expérience de la gestion des incidents pour évaluer de manière critique les plans générés par l'IA.

Ce décalage favorise un faux sentiment de sécurité - une "confiance artificielle" - dans lequel les organisations accordent une confiance excessive aux résultats de l'IA sans une supervision humaine suffisante. Cet article explore les pièges d'une confiance excessive dans l'IA en matière de PCA et de PRD, illustrés par des exemples récents du monde réel.

Pour rédiger cet article, nous avons fait appel à Chat-GPT en tant que co-auteur. Il a été demandé à Chat-GPT d'écrire un article sur la confiance artificielle qui accompagne l'IA et de fournir des exemples d'échecs de l'IA, nous avons complété ses observations par les nôtres.

Qu'est-ce que l'intelligence ?

Le dictionnaire Webster définit l'intelligence comme : la capacité d'apprendre ou de comprendre ou de faire face à des situations nouvelles ou éprouvantes ; la capacité d'appliquer des connaissances pour manipuler son environnement ou de penser de manière abstraite, mesurée par des critères objectifs (tels que des tests) ; l'acuité mentale.

Si l'on compare l'IA et l'homme dans le contexte de l'intelligence, il est clair que notre capacité à nous adapter aux situations, y compris à l'empathie, et à ne pas nous contenter de répéter des tâches, constitue un avantage certain. L'intelligence artificielle, bien qu'elle soit capable d'analyser des événements et de reconnaître des modèles, n'a pas de conscience et ne peut pas vraiment comprendre les concepts. En cas d'informations inexactes ou manquantes, l'intelligence artificielle ne peut pas raisonner comme le font les humains, en s'appuyant sur leurs propres expériences pour combler le fossé entre le passé et les événements sans précédent.

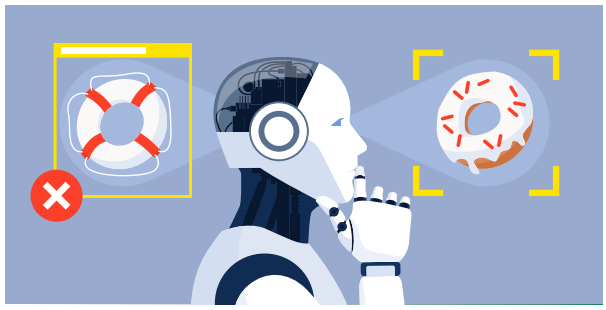
Cependant, la continuité des activités et la reprise après sinistre ne s'arrêtent pas là, et c'est ce que nous allons explorer dans cet article. Nous examinerons les domaines dans lesquels l'intelligence artificielle a échoué et comment les experts auraient pu agir différemment.

Lorsque l'on travaille dans un domaine où des événements imprévisibles et sans précédent peuvent se produire, il est crucial d'avoir des experts qui naviguent

global crises. When companies and experts become too reliant on AI, unpredictable or new crises can be problematic. AI is incapable of having 'gut feelings' that many experts can gain from experience.

AI relies on predictive modeling – but what happens when a disaster is unpredictable? A Continuity professional, trained in the field, and with sufficient experience, not just in BCP an DR, but other life skills, maybe even other unrelated job experience, will draw on that entire body of knowledge to help form their response. That type of adaptive non-linear thinking is currently beyond AI tools.

The Limits of Context: AI Cannot See the Full Picture



AI excels at analyzing structured data but struggles with evolving contexts and human complexities. Effective crisis management requires flexibility and intuition that machines lack. For example, in 2021 there was the crisis of the Ever-Given Suez Canal Blockage, where for six days the canal was blocked which disrupted global supply chains.

AI-powered logistics platforms failed to adapt their risk models or reroute shipments efficiently. Since this situation was unpredictable, there was no data to train AI with for a situation like this, and AI struggled to handle what to do (Coles, 2021).

IBM reported that 42% of supply chain managers found AI systems inadequate for geopolitical and environmental disruptions like the blockage (***IBM Institute for Business Value, 2022***). Human expertise was essential to mitigate cascading effects and communicate with stakeholders.

dans les catastrophes afin de tirer parti de leur expérience et d'adapter leurs connaissances pour qu'elles correspondent le mieux possible à la situation. Lorsque les entreprises et les experts deviennent trop dépendants de l'IA, les crises imprévisibles ou nouvelles peuvent poser problème. L'IA est incapable d'avoir les "intuitions" que de nombreux experts acquièrent avec l'expérience.

L'IA repose sur la modélisation prédictive - mais que se passe-t-il lorsqu'une catastrophe est imprévisible ? Un professionnel de la continuité, formé sur le terrain et disposant d'une expérience suffisante, non seulement en matière de PCA et de DR, mais aussi d'autres compétences pratiques, voire d'une expérience professionnelle sans rapport avec le sujet, s'appuiera sur l'ensemble de ces connaissances pour élaborer sa réponse. Ce type de réflexion adaptative et non linéaire est actuellement hors de portée des outils d'intelligence artificielle.

Les limites du contexte : L'IA ne peut pas avoir une vue d'ensemble

L'IA excelle dans l'analyse de données structurées, mais elle a du mal à s'adapter aux contextes changeants et aux complexités humaines. Une gestion de crise efficace exige une flexibilité et une intuition dont les machines sont dépourvues. Par exemple, en 2021, il y a eu la crise du blocage du canal de Suez, qui a duré six jours et a perturbé les chaînes d'approvisionnement mondiales.

Les plateformes logistiques alimentées par l'IA n'ont pas réussi à adapter leurs modèles de risque ou à réacheminer les expéditions de manière efficace. Cette situation étant imprévisible, il n'y avait pas de données permettant d'entraîner l'IA à une telle situation, et l'IA a eu du mal à savoir quoi faire (Coles, 2021).

IBM a indiqué que 42 % des responsables de la chaîne d'approvisionnement trouvaient les systèmes d'IA inadaptés aux perturbations géopolitiques et environnementales telles que le blocage (IBM Institute for Business Value, 2022). L'expertise humaine était essentielle pour atténuer les effets en cascade et communiquer avec les parties prenantes.

Un exemple similaire des limites de l'IA a été observé lors de l'effondrement de la Silicon

A similar instance of AI's limitations was seen in the 2023 Silicon Valley Bank collapse. AI-based risk systems missed early warning signs because such market conditions lacked precedent. Over 55% of financial institutions' AI models failed to flag SVB's collapse as high-risk (***Financial Times, 2023***). AI cannot reliably predict unprecedented events without human scenario planning and judgment

In both instances, human analysis drawing conclusions outside of the AI generated reports were missing. While the shipping blockage eventually leveraged human expertise to mitigate the cascading effects noted, it was only after days of reliance on flawed models, SVB wasn't as lucky, and its collapse created an unprecedented financial risk in the US.

Legal and Ethical Blind Spots: AI Cannot Navigate Grey Areas

Companies relying on artificial intelligence for disaster recovery may face challenges, as AI cannot adequately interpret the complex legal and ethical aspects of BCP and DR.

In 2021 Robinhood Financial had outages during volatile markets. Robinhood outages caused severe customer losses and legal scrutiny as customers were unable to access their accounts and make trades. AI-driven automated responses delayed critical regulatory communications, exposing the company to lawsuits (***Reuters, 2021***). Legal teams had to intervene extensively post-incident.

If companies implement AI and become too reliant on it, this opens the company up to lawsuits should any issues arise. For Robinhood, they had become too dependent on using AI for chatbots to handle customer complaints and issues. When there was a disaster, the AI chatbots were unable to address people's concerns and handle the complex crisis. AI cannot substitute for human empathy and leadership in managing public perception and trust.

Valley Bank en 2023. Les systèmes de gestion des risques basés sur l'IA n'ont pas détecté les signes avant-coureurs parce que de telles conditions de marché n'avaient pas de précédent. Plus de 55 % des modèles d'IA des institutions financières n'ont pas signalé l'effondrement de la SVB comme présentant un risque élevé (Financial Times, 2023). L'IA ne peut pas prédire de manière fiable des événements sans précédent sans la planification de scénarios et le jugement de l'homme

Dans les deux cas, l'analyse humaine tirant des conclusions en dehors des rapports générés par l'IA faisait défaut. Alors que le blocage du transport maritime a finalement fait appel à l'expertise humaine pour atténuer les effets en cascade constatés, ce n'est qu'après des jours de dépendance à l'égard de modèles défectueux que la SVB n'a pas eu la même chance et que son effondrement a créé un risque financier sans précédent aux États-Unis.

Les angles morts juridiques et éthiques : L'IA ne peut pas naviguer dans les zones grises

Les entreprises qui s'appuient sur l'intelligence artificielle pour la reprise après sinistre peuvent être confrontées à des difficultés, car l'intelligence artificielle ne peut pas interpréter correctement les aspects juridiques et éthiques complexes du PCA et de la reprise après sinistre.

En 2021, Robinhood Financial a connu des pannes pendant la période de volatilité des marchés. Les pannes de Robinhood ont entraîné de graves pertes pour les clients et des poursuites judiciaires, car les clients n'ont pas pu accéder à leurs comptes et effectuer des transactions. Les réponses automatisées pilotées par l'IA ont retardé les communications réglementaires essentielles, exposant l'entreprise à des poursuites judiciaires (Reuters, 2021). Les équipes juridiques ont dû intervenir massivement après l'incident.

Si les entreprises mettent en œuvre l'IA et en deviennent trop dépendantes, elles s'exposent à des poursuites en cas de problème. Dans le cas de Robinhood, l'entreprise était devenue trop dépendante de l'utilisation de l'IA pour les chatbots afin de gérer les plaintes et les problèmes des clients. En cas de catastrophe, les chatbots d'IA n'ont pas été en mesure de répondre aux préoccupations des gens et de gérer la crise complexe. L'IA ne peut pas se substituer à l'empathie et au leadership humains pour gérer la perception et la confiance du public.

Organizational Amnesia: Overreliance on AI Erodes Human Expertise

Another concern of the heavy reliance on AI is the possibility of it degrading critical human skills necessary for disaster recovery.

In 2023, Cloudflare's DNS outage disrupted global internet access. Internal teams struggled to intervene manually due to dependence on AI-driven monitoring systems, delaying recovery (***TechCrunch, 2023***). Therefore, maintaining human skills through training and practice is vital alongside AI tools.

If companies are going to be implementing AI in the workplace, they need to ensure that workers understand how to use, interpret and evaluate the responses of AI. Companies should be incorporating the use of AI in their training, as well as still focusing on how to complete jobs without the use of AI. In a career where disasters are dealt with, it is an oversight to depend on one technology so much that your organization is hindered if it becomes inaccessible. To power outages, downed servers or broken code, AI has many vulnerabilities that could interfere with operations.

Just when using Chat-GPT to help write this article, it took over 10 attempts with different prompts and adjustments to ensure we were getting an accurate, relevant and insightful response. And when doing more research into the examples that Chat-GPT provided, it was found that the references it provided could not be verified without a subscription, as the prompt did not specify what type of resources it should use. If workers do not know how to very precisely and accurately use the AI programs they're using, they could get inaccurate or incomplete information.

Smaller companies with less resources may be tempted to turn to accessible AI such as Chat-GPT, and without experts overseeing the BCP and DR solutions, there is no way for the company to ensure accuracy. These companies are also more susceptible to disasters ruining their companies and forcing

Amnésie organisationnelle : La dépendance excessive à l'égard de l'IA érode l'expertise humaine

Une autre préoccupation liée à la forte dépendance à l'égard de l'IA est la possibilité qu'elle dégrade les compétences humaines essentielles à la reprise après sinistre.

En 2023, la panne de DNS de Cloudflare a perturbé l'accès mondial à l'internet. Les équipes internes ont eu du mal à intervenir manuellement en raison de leur dépendance à l'égard des systèmes de surveillance pilotés par l'IA, ce qui a retardé la reprise (TechCrunch, 2023). Par conséquent, le maintien des compétences humaines par le biais de la formation et de la pratique est essentiel parallèlement aux outils d'IA.

Si les entreprises mettent en œuvre l'IA sur le lieu de travail, elles doivent s'assurer que les travailleurs comprennent comment utiliser, interpréter et évaluer les réponses de l'IA. Les entreprises devraient intégrer l'utilisation de l'IA dans leur formation, tout en continuant à se concentrer sur la manière d'accomplir les tâches sans l'aide de l'IA. Dans une carrière où l'on doit faire face à des catastrophes, c'est une erreur de dépendre d'une technologie au point d'entraver l'organisation si elle devient inaccessible. Qu'il s'agisse de pannes de courant, de serveurs hors service ou de codes défectueux, l'IA présente de nombreuses vulnérabilités susceptibles de perturber les opérations.

Lorsque nous avons utilisé Chat-GPT pour nous aider à rédiger cet article, il nous a fallu plus de 10 tentatives avec différentes invites et ajustements pour nous assurer que nous obtenions une réponse précise, pertinente et perspicace. Et lorsque nous avons fait des recherches plus approfondies sur les exemples fournis par Chat-GPT, nous avons découvert que les références fournies ne pouvaient pas être vérifiées sans abonnement, car l'invite ne spécifiait pas le type de ressources à utiliser. Si les travailleurs ne savent pas comment utiliser avec précision et exactitude les programmes d'intelligence artificielle qu'ils utilisent, ils risquent d'obtenir des informations inexactes ou incomplètes.

them to close. And while being able to use AI to create a plan can be a great tool, if the company has a false sense of security that the AI plan is complete and accurate, they may not take the appropriate measures to ensure their company really can recover, such as contracting out an expert. The expert can then review their plans, consider scenarios they did not, and provide more robust solutions.

Conclusion: Toward a Hybrid Approach to Resilience

Despite this article examining the pitfalls of artificial intelligence, the takeaway is not that it shouldn't be used. Combined with an expert, AI can become an extremely powerful tool that could change the game for disaster recovery and business continuity. AI exceeds expectations when it comes to analyzing massive amounts of real-time data and could potentially notice red flags before people could and allow companies to be more proactive in its solutions. It's what an expert can do with that information that will truly allow the company to thrive.

AI offers powerful capabilities to augment business continuity and disaster recovery—but "artificial confidence" in AI-only resilience is perilous. Effective BCP and DRP require a hybrid approach that combines AI's strengths with human judgment, creativity, ethical reasoning, and leadership.

Organizations must invest equally in sophisticated AI tools and skilled professionals empowered to interpret, challenge, and adapt AI outputs. True resilience is not automated—it is human-centered and machine-assisted. Ω

Les petites entreprises disposant de moins de ressources peuvent être tentées de se tourner vers une IA accessible telle que Chat-GPT, et sans experts pour superviser les solutions BCP et DR, il n'y a aucun moyen pour l'entreprise de s'assurer de la précision. Ces entreprises sont également plus susceptibles d'être ruinées par des catastrophes qui les obligeraient à fermer leurs portes. Bien que l'utilisation de l'IA pour créer un plan puisse être un outil formidable, si l'entreprise a un faux sentiment de sécurité en pensant que le plan de l'IA est complet et précis, elle risque de ne pas prendre les mesures appropriées pour s'assurer que son entreprise peut réellement se rétablir, par exemple en faisant appel à un expert. L'expert peut alors revoir ses plans, envisager des scénarios qu'elle n'a pas envisagés et proposer des solutions plus solides.

Conclusion : Vers une approche hybride de la résilience

Bien que cet article examine les pièges de l'intelligence artificielle, il ne faut pas en conclure qu'il ne faut pas l'utiliser. Associée à un expert, l'IA peut devenir un outil extrêmement puissant qui pourrait changer la donne en matière de reprise après sinistre et de continuité des activités. L'IA dépasse les attentes lorsqu'il s'agit d'analyser des quantités massives de données en temps réel et pourrait potentiellement détecter les signaux d'alarme avant les gens et permettre aux entreprises d'être plus proactives dans leurs solutions. C'est ce qu'un expert peut faire avec ces informations qui permettra à l'entreprise de prospérer.

L'IA offre de puissantes capacités pour améliorer la continuité des activités et la reprise après sinistre, mais la "confiance artificielle" dans la résilience de l'IA seule est périlleuse. Un PCA et un PRS efficaces nécessitent une approche hybride qui combine les forces de l'IA avec le jugement humain, la créativité, le raisonnement éthique et le leadership.

Les organisations doivent investir à parts égales dans des outils d'IA sophistiqués et dans des professionnels qualifiés capables d'interpréter, de remettre en question et d'adapter les résultats de l'IA. La véritable résilience n'est pas automatisée — elle est centrée sur l'humain et assistée par la machine. Ω

ABOUT THE AUTHORS

Jason Firlotte MBCP, CBRM, MBCI, CSP, CBCV

Jason is President of Sentinel BCM (SentinelBCM). Mr. Firlotte has been providing industry leading, high quality consulting and professional services in the critical areas of Business Continuity , Information Technology Continuity and Disaster Recovery planning since 1997. Mr Firlotte is a graduate of Algonquin College's Security Management Program(Honours) in 1996, and Information System Development (Honours), Willis College, 2001. In 2020, he achieved his certification as a Master Business Continuity Professional from DRI, and was inducted into the Order of the Sword and Shield. Mr. Firlotte is currently a Director at Large for DRI Canada.

Jessa Cinnamon

Jessa Cinnamon started her university career at St. Francis Xavier university where she obtained her Diploma in Engineering. Jessa continued her studies at Dalhousie University where she has recently graduated with her Degree with Sexton Distinction in Electrical Engineering with the option in computer engineering and a certificate in Biomedical Engineering. Jessa is also a member of the Golden Key International Honours Society.

ChatGPT

ChatGPT is an AI language model extraordinaire, trained on vast troves of text to help humans craft everything from witty articles to complex code (and sometimes even bedtime stories). Never needing coffee breaks or vacation days, ChatGPT tirelessly assists with brainstorming, drafting, editing, and occasionally throwing in a pun or two just to keep things lively.

Specializing in turning vague ideas into polished prose, ChatGPT excels at juggling facts, facts, and more facts — all while maintaining a charming neutrality about whether cats or dogs truly reign supreme.

À PROPOS DES AUTEURS

Jason Firlotte MBCP, CBRM, MBCI, CSP, CBCV

Jason est président de Sentinel BCM (SentinelBCM). M. Firlotte fournit des services de consultation et des services professionnels de haute qualité de pointe dans les domaines critiques de la continuité des activités, de la continuité des technologies de l'information et de la planification de la reprise après sinistre depuis 1997. M. Firlotte est diplômé du programme de gestion de la sécurité (avec distinction) du Collège Algonquin en 1996 et du développement de systèmes d'information (avec distinction) du Collège Willis, 2001. En 2020, il a obtenu sa certification en tant que maître professionnel de la continuité des affaires de DRI et a été intronisé dans l'Ordre de l'Épée et du Bouclier. M. Firlotte est actuellement administrateur général de DRI Canada.

Jessa Cinnamon

Jessa Cinnamon a commencé ses études universitaires à l'université St. Francis Xavier, où elle a obtenu son diplôme d'ingénieur. Elle a poursuivi ses études à l'université Dalhousie, où elle a récemment obtenu son diplôme avec mention Sexton en génie électrique, avec une option en génie informatique et un certificat en génie biomédical. Jessa est également membre de la Golden Key International Honours Society.

ChatGPT

ChatGPT est un modèle linguistique IA extraordinaire, entraîné sur de vastes quantités de textes afin d'aider les humains à rédiger tout type de contenu, des articles pleins d'esprit aux codifications complexes (et parfois même des histoires pour s'endormir). Ne nécessitant ni pause café ni jours de congé, ChatGPT apporte son aide sans relâche pour le brainstorming, la rédaction, l'édition et, parfois, ajoute une ou deux blagues pour égayer l'atmosphère.

Spécialisé dans la transformation d'idées vagues en prose raffinée, ChatGPT excelle dans la jonglerie des faits, des faits et encore des faits, tout en conservant une charmante neutralité quant à savoir si les chats ou les chiens règnent véritablement en maîtres.

References / Références

Gartner. (2024). AI Adoption in Business Continuity: State of the Market. Gartner Research.

Terri Coles. (2021). Data Center Knowlege. Machine Learning Automation Couldn't Keep the Suez Canal Unstuck. https://www.datacenterknowledge.com/automation/machine-learning-automation-couldn-t-keep-the-suez-canal-unstuck

IBM Institute for Business Value. (2022). Supply Chain Resilience Report. https://www.ibm.com/reports/supply-chain-2022

Financial Times. (2023). AI Models Missed SVB Collapse. https://www.ft.com/svb-collapse-ai

Reuters. (2021). Robinhood Trading Outage Sparks Legal Action. https://www.reuters.com/robinhood-outage-lawsuit

TechCrunch. (2023). Cloudflare DNS Outage Analysis. https://techcrunch.com/cloudflare-dns-2023

Ivalua. (2025). AI-Ready Supply Chains Prove More Resilient Amid Rising Global Risk. https://www.ivalua.com/press-releases/ai-ready-supply-chains-prove-more-resilient-amid-rising-global-risk/

Dollars And Sense: Boost Your Salary With Certification

By/Par Joel Baglole

They say that education is its own reward. But for certified professionals, there is also a financial incentive to attaining higher levels of certification.

The 2025 "Global Compensation Report" from Resilience360 Advisory shows that certified professionals in Canada are well paid, and that there is a direct correlation between salaries and the level of certification that a person holds.

Currently, the average annual salary of a certified professional in Canada is $127,462. That is more than double the $56,400 average yearly income of a Canadian worker, according to data from Statistics Canada. However, the salary range for a certified professional varies depending on their level of certification.

Le bon sens financier : augmentez votre salaire grâce à une certification

On dit que l'éducation est sa propre récompense. Mais pour les professionnels certifiés, il existe également une incitation financière à atteindre des niveaux de certification plus élevés.

Le "Global Compensation Report" 2025 de Resilience360 Advisory montre que les professionnels certifiés au Canada sont bien payés et qu'il existe une corrélation directe entre les salaires et le niveau de certification détenu par une personne.

Actuellement, le salaire annuel moyen d'un professionnel certifié au Canada est de 127 462 $. C'est plus du double du revenu annuel moyen d'un travailleur canadien, qui est de 56 400 $, selon les données de Statistique Canada. Toutefois, l'échelle salariale d'un professionnel agréé varie en fonction de son niveau de certification.

Across the country, compensation for certified professionals ranges from $96,152 to as high as $142,269 depending on one's location and whether they have obtained the Associate Business Continuity Professional (ABCP), Certified Business Continuity Professional (CBCP), or Master Business Continuity Professional (MBCP) designations.

"What's clear is that people with no certification have lower salaries than people with certification," says **Cheyene Marling,** Managing Director of Resilience360 Advisory, who has produced the annual Compensation Report for 23 consecutive years. "Companies value continuous education and going through the certification ranks has monetary benefits."

The latest data shows a clear correlation between advances in certification and a rise in annual salary. In fact, certified professionals with the highest level of certification have salaries that are, on average, 18% higher than people with only one level of certification.

Cheyene Marling

People with no designation behind their name have the lowest salaries in the industry.

"Education is very marketable to a hiring manager or committee," says Marling. "And the Master level certification shows

Dans l'ensemble du pays, la rémunération des professionnels certifiés varie de 96 152 dollars à 142 269 dollars, en fonction du lieu de travail et de l'obtention des titres Associate Business Continuity Professional (ABCP), Certified Business Continuity Professional (CBCP) ou Master Business Continuity Professional (MBCP).

"Ce qui est clair, c'est que les personnes sans certification ont des salaires inférieurs à ceux des personnes certifiées", déclare **Cheyene Marling**, directrice générale de Resilience360 Advisory, qui a produit le rapport annuel sur les rémunérations pendant 23 années consécutives. "Les entreprises accordent de l'importance à la formation continue et le fait de gravir les échelons de la certification présente des avantages pécuniaires.

Les dernières données montrent une corrélation évidente entre les progrès en matière de certification et l'augmentation du salaire annuel. En fait, les professionnels certifiés ayant le niveau de certification le plus élevé ont des salaires qui sont, en moyenne, 18 % plus élevés que ceux qui n'ont qu'un seul niveau de certification. Les personnes qui n'ont pas de titre derrière leur nom ont les salaires les plus bas de l'industrie.

"L'éducation est un argument de vente très convaincant pour un responsable ou un comité d'embauche", explique M. Marling. "Et la certification de niveau Master montre qu'un professionnel a investi dans sa formation.

Dan Duffy est du même avis. Il est président (retraité) du Mid-Range Computer Group,

that a professional has made an investment in their education."

Dan Duffy agrees. He's (retired) President of Mid-Range Computer Group, a successful information technology (IT) company outside Toronto. A certified professional himself, Duffy says he always considered certification levels when making hiring decisions.

"For business recovery, and disaster recovery in particular, certifications earned bring a sense of credibility that the employee has studied what can happen, and, more importantly, how to handle it if and when it does," says Duffy in an interview with TNR magazine. "As an employer, the ability to say to a customer that we have employees who have certification is, once again, credibility."

Both Marling and Duffy say they understand that the certification process can seem daunting and that many people are on the fence when it comes to deciding whether to progress through the higher levels of certification. However, both agree that the salary benefits that can be achieved make moving up the certification ladder worth it.

"Younger workers need to be told that their career paths will be wider and more varied the more they learn, and they always learn a great deal when they get certified," says Duffy.

une entreprise de technologie de l'information (TI) prospère de la région de Toronto. Professionnel certifié lui-même, Duffy dit qu'il a toujours tenu compte des niveaux de certification lorsqu'il a pris des décisions d'embauche.

Dan Duffy

"Pour la reprise d'activité, et la reprise après sinistre en particulier, les certifications obtenues apportent un sentiment de crédibilité, car l'employé a étudié ce qui peut arriver et, plus important encore, comment y faire face si et quand cela se produit", déclare Duffy dans un entretien avec le magazine TNR. "En tant qu'employeur, la capacité de dire à un client que nous avons des employés certifiés est, une fois de plus, un gage de crédibilité.

Marling et Duffy disent comprendre que le processus de certification peut sembler décourageant et que de nombreuses personnes hésitent à franchir les niveaux supérieurs de certification. Cependant, tous deux s'accordent à

Marling notes that there has never been a better time for professionals to start their certification journey as recognition of business continuity and resilience certifications is at an all-time high after the Covid-19 pandemic.

"Recognition and knowledge of business continuity professionals is developing and improving, especially post-Covid," she says, adding that more universities around the world are offering business continuity programs as demand for certified professionals steadily rises.

"It wasn't that long ago, when only North Texas University had a business continuity program," she says. "Not anymore. Over the last 15 years, more universities have come out with business continuity programs, in the U.S. and elsewhere."

In terms of elevating one's renumeration, Marling notes that higher levels of certification demonstrate leadership skills to employers, and that can vault certified professionals into the ranks of senior management at a company where salaries can top $200,000 per year.

dire que les avantages salariaux qui peuvent être obtenus valent la peine de gravir les échelons de la certification.

"Il faut dire aux jeunes travailleurs que leur carrière sera plus large et plus variée à mesure qu'ils apprennent, et ils apprennent toujours beaucoup lorsqu'ils obtiennent une certification", déclare M. Duffy.

Marling note qu'il n'y a jamais eu de meilleur moment pour les professionnels de commencer leur parcours de certification, car la reconnaissance des certifications en matière de continuité et de résilience des entreprises a atteint un niveau record après la pandémie de grippe aviaire de 19 ans.

"La reconnaissance et les connaissances des professionnels de la continuité d'activité se développent et s'améliorent, en particulier après la pandémie de Covid", dit-elle, ajoutant que de plus en plus d'universités dans le monde proposent des programmes de continuité d'activité en raison de la demande croissante de professionnels certifiés.

"Il n'y a pas si longtemps, seule l'université du Texas du Nord proposait un programme de continuité des activités. "Ce n'est plus le cas aujourd'hui. Au cours des 15 dernières années, de plus en plus d'universités ont mis en place des programmes de continuité des activités, aux États-Unis et ailleurs.

En ce qui concerne l'augmentation de la rémunération, Mme Marling note que les niveaux de certification les plus élevés démontrent aux employeurs des compétences de leadership, ce qui peut propulser les professionnels certifiés au rang de cadres supérieurs dans une entreprise où les salaires peuvent dépasser les 200 000 dollars par an.

En fait, les professionnels certifiés ayant le titre de MBCP peuvent gagner plus de 235 000 dollars par an au Canada en tant que cadres supérieurs. Les personnes qui ont le titre "MBCP" après leur nom gagnent des salaires plus élevés que n'importe quelle autre certification ou désignation professionnelle.

In fact, certified professionals with the MBCP designation can earn more than $235,000 annually in Canada as a senior executive. People who have "MBCP" after their name earn higher salaries than just about any other certification or professional designation.

"As business continuity is seen as more of a career, the expectation is that certified professionals bring leadership skills to the table," she says. "It's so important to develop leadership skills. That could be everything from public speaking and presentation experience, to getting published and managing a team," adds Marling.

Duffy says he sees first-hand the ways in which people with advanced levels of certification rise through the ranks, not only at his IT company, but across the corporate world. "Certifications are great for employees, great for companies, and great for businesses. The more they are combined with practical experience, the better," he says.

Yet despite the obvious financial rewards in reaching the highest level of certification, the 2025 Global Compensation Report shows that only 10% of certified professionals hold DRI Internationals' top MBCP certification.

"Business continuity and resilience are very much in demand," says Marling. "And the bottom line is that people with no certification have lower salaries than people with certification." Ω

"La continuité des affaires étant considérée comme une carrière à part entière, on attend des professionnels certifiés qu'ils apportent leurs compétences en matière de leadership", explique-t-elle. "Il est très important de développer des compétences en leadership. Cela peut aller de la prise de parole en public et de l'expérience en matière de présentation à la publication et à la gestion d'une équipe", ajoute Mme Marling.

M. Duffy explique qu'il a pu constater de visu que les personnes ayant obtenu des certifications de haut niveau gravissaient les échelons, non seulement dans sa société informatique, mais aussi dans le monde de l'entreprise. "Les certifications sont excellentes pour les employés, pour les sociétés et pour les entreprises. Plus elles sont combinées à une expérience pratique, mieux c'est", ajoute-t-il.

Pourtant, malgré les avantages financiers évidents liés à l'obtention du plus haut niveau de certification, le rapport mondial sur les rémunérations 2025 montre que seuls 10 % des professionnels certifiés détiennent la certification MBCP de DRI Internationals, qui est la plus élevée.

"La continuité et la résilience des entreprises sont très demandées", affirme M. Marling. "Et le résultat est que les personnes sans certification ont des salaires inférieurs à ceux des personnes certifiées." Ω

ABOUT THE AUTHOR

Joel Baglole

Joel is the Manager of Communications at DRI Canada. Prior to working in corporate communications, he was a journalist. From 1999 to 2004, he was a staff reporter at The Wall Street Journal where he covered economics, financial markets, investment banks, and deals such as mergers and acquisitions. He began his career at The Toronto Star newspaper and has also worked for The Washington Post. He lives outside Ottawa.

À PROPOS DE L'AUTEUR

Joel Baglole

Joel est le directeur des communications de DRI Canada. Avant de travailler dans la communication d'entreprise, il était journaliste. De 1999 à 2004, il a été journaliste au Wall Street Journal, où il a couvert l'économie, les marchés financiers, les banques d'investissement et les transactions telles que les fusions et acquisitions. Il a commencé sa carrière au journal The Toronto Star et a également travaillé pour le Washington Post. Il vit à l'extérieur d'Ottawa.

Sometimes We Need To Unlearn

Parfois, nous devons désapprendre

By/Par Andy Prince

I'm a huge believer that our learning journey never ends. There is ALWAYS something new to learn, something wonderful to stumble upon, something amazing to discover – and oftentimes learning occurs in ways we never expected or anticipated.

But…

Sometimes we need to unlearn things. Societal expectations that make us feel inadequate and excluded. Behaviors and attitudes that make us feel ashamed and unworthy. Feedback and language that makes us feel like we bring no value.

I stumbled upon this post somewhere online (I'm sure I was falling down some Internet rabbit hole at night) and it really struck me. I had to read it multiple times because there is depth and complexity to it that belies the simplicity of the message. The title is simply 10 Things We Need To Unlearn.

I suspect that we've all heard some of these things at some point in our lives – whether with family and friends or at work. On feeling deeply, you're told you're too sensitive. On success equaling hustle at all costs.

I remember a Cadillac commercial (https://www.youtube.com/watch?v=xNzXze5Yza8) that celebrated this thinking and reinforced an unhealthy stereotype about work in the United States. At the time, I remember feeling repulsed by it. For the record, I still

Je crois fermement que notre voyage d'apprentissage ne s'arrête jamais. Il y a TOUJOURS quelque chose de nouveau à apprendre, quelque chose de merveilleux à découvrir par hasard, quelque chose d'étonnant à écouvrir - et souvent, l'apprentissage se produit d'une manière que nous n'avons jamais attendue ou anticipée.

Mais...

Parfois, nous devons désapprendre certaines choses. Les attentes de la société qui nous font nous sentir inadéquats et exclus. Les comportements et les attitudes qui nous font nous sentir honteux et indignes. Les commentaires et le langage qui nous donnent l'impression que nous n'avons aucune valeur.

Je suis tombée par hasard sur cet article quelque part en ligne (je suis sûre que je suis tombée dans un trou de lapin Internet la nuit) et il m'a vraiment frappée. J'ai dû le lire plusieurs fois parce qu'il contient une profondeur et une complexité qui démentent la simplicité du message. Le titre est simplement "10 choses que nous devons désapprendre".

Je pense que nous avons tous entendu certaines de ces choses à un moment ou à un autre de notre vie, que ce soit en famille, avec des amis ou au travail. Lorsque vous ressentez des émotions profondes, on vous dit que vous êtes trop sensible. Le succès est synonyme d'acharnement à tout prix.

Je me souviens d'une publicité de Cadillac (https://www.youtube.com/watch?v=xNzXze5Yza8) qui célébrait cette façon de penser et renforçait un stéréotype malsain sur le travail aux États-Unis. À l'époque, je me souviens d'avoir été repoussé par cette publicité. Pour l'anecdote, je le suis toujours ;) Nous vivons dans une culture du "bootstrap" où nous sommes censés simplement renforcer notre détermination et nous débrouiller, quel que soit le prix à payer pour notre bien-être mental et physique.

Ten Things to Unlearn
1. Rest = Laziness
2. Your Worth = Productivity
3. Conflict = Bad
4. Saying Yes = Being Kind
5. Feeling Deeply = Overreacting
6. Happiness = The End Goal
7. Vulnerability = Weakness
8. Success = Hustle At All Costs
9. Seeking Help = Failure
10. Healing = Getting Over It

am. ;) We live in a bootstrap culture where we're supposed to simply strengthen our resolve and figure it out, regardless of the cost to our mental and physical well-being.

We are bombarded every day by images, words, sounds, voices, stories, videos, etc., that reinforce many of the above cliches and beliefs. How could we not learn to think this way? But this way of thinking isn't healthy. And it certainly doesn't reflect the journey – the real journey – of nearly every human being on this planet.

We need time to heal, space to be vulnerable, opportunity for healthy conflict, support and help from our communities, and the chance to rest and recharge. In other words, we simply need to be human.

"Until next week... Cheers, Andy!" Ω

ABOUT THE AUTHOR

Andy Prince *currently provides consulting services to companies of all sizes looking to build human-based communications strategies for both internal and external audiences. Additionally, he writes a weekly newsletter (https://liveunvarnished.beehiiv.com/) on being OK with being human – and writes and speaks regularly on the topic of humanity.*

About two years ago, he and his wife moved to Bismarck, ND from Austin, TX to be closer to her family as her parents age. He has five dogs and one cat.

Nous sommes bombardés chaque jour d'images, de mots, de sons, de voix, d'histoires, de vidéos, etc. qui renforcent bon nombre des clichés et croyances susmentionnés. Comment ne pas apprendre à penser ainsi ? Mais cette façon de penser n'est pas saine. Et elle ne reflète certainement pas le voyage - le vrai voyage - de presque tous les êtres humains sur cette planète.

Dix choses à désapprendre
1. Repos = paresse
2. Votre valeur = productivité
3. Conflit = mauvais
4. Dire oui = être gentil
5. Ressentir profondément = réagir de manière excessive
6. Bonheur = objectif final
7. Vulnérabilité = faiblesse
8. Succès = se démener à tout prix
9. Demander de l'aide = échec
10. Guérison = Surmonter

Nous avons besoin de temps pour guérir, d'espace pour être vulnérables, d'occasions de conflits sains, de soutien et d'aide de la part de nos communautés, et de la possibilité de nous reposer et de nous ressourcer. En d'autres termes, nous avons tout simplement besoin d'être humains.

"À la semaine prochaine... Santé, Andy !" Ω

À PROPOS DE L'AUTEUR

Andy Prince *fournit actuellement des services de conseil à des entreprises de toutes tailles qui cherchent à mettre en place des stratégies de communication axées sur l'humain, tant pour leur public interne qu'externe. Il rédige également une newsletter hebdomadaire (https://liveunvarnished.beehiiv.com/) sur le thème « être humain, c'est OK » et écrit et intervient régulièrement sur le sujet de l'humanité.*

Il y a environ deux ans, lui et sa femme ont quitté Austin, au Texas, pour s'installer à Bismarck, dans le Dakota du Nord, afin de se rapprocher de la famille de sa femme, dont les parents prennent de l'âge. Il possède cinq chiens et un chat.

A Student's Perspective of AI

Le point de vue d'un étudiant sur l'IA

By/Par Katelyn Holowachuk

As a second-year university student studying at the Université de Saint-Boniface to become a teacher, I have been reflecting a lot about how artificial intelligence (AI) is changing education. Over the past few years, tools like ChatGPT have become more common in classrooms and universities. While tools such as ChatGPT can make learning more efficient and accessible, they also raise important questions about academic honesty, student engagement, and the role of teachers. From the perspective of a future educator, AI has the potential to improve learning in powerful ways, but only if it is used thoughtfully and ethically.

I am a student at the Université de St-Boniface in Winnipeg, where I am studying to become a public-school teacher. Last year, I volunteered in my home community of the RM of Springfield to join the Emergency Social Services team. I am one of a group who will help operate a reception centre if there is an evacuation in our community.

When we did our first exercise and learned how to take information and determine the needs of people, I came to understand that their job was about more than just filling out a registration form. Working with people in a crisis depends

En tant qu'étudiante de deuxième année à l'Université de Saint-Boniface en vue de devenir enseignante, j'ai beaucoup réfléchi à la manière dont l'intelligence artificielle (IA) modifie l'éducation. Au cours des dernières années, des outils tels que ChatGPT sont devenus plus courants dans les salles de classe et les universités. Si ces outils peuvent rendre l'apprentissage plus efficace et plus accessible, ils soulèvent également des questions importantes sur l'honnêteté académique, l'engagement des étudiants et le rôle des enseignants. Du point de vue d'un futur éducateur, l'IA a le potentiel d'améliorer l'apprentissage de manière puissante, mais seulement si elle est utilisée de manière réfléchie et éthique.

Je suis étudiante à l'Université de St-Boniface à Winnipeg, où j'étudie pour devenir enseignante dans les écoles publiques. L'année dernière, je me suis portée volontaire pour rejoindre l'équipe des services sociaux d'urgence de ma communauté, la MR de Springfield. Je fais partie d'un groupe qui aidera à gérer un centre d'accueil en cas d'évacuation dans notre communauté.

Lorsque nous avons fait notre premier exercice et que nous avons appris à recueillir des informations et à déterminer les besoins des personnes, j'ai compris que leur travail ne se limitait pas à remplir

on human interaction and knowing what the person needs. There's no substitute for looking a person in the eyes to understand the most important things, which are often unspoken.

If we depend on AI in situations when there is a critical human need, we will miss the things that are unsaid. I think that's true of both my volunteer work in Emergency Social Services, and in my intended career as a teacher. People will be depending on me and trusting me with a lot of responsibility, and I owe it to them to take that responsibility seriously rather than trusting a machine.

Like every tool, AI has its place, and the challenge is to figure out how and when it can be used responsibly. One of the many benefits of using AI in education is its ability to support personalized learning. This can be applied both in the classroom setting, where I plan to work, and in Continuity Management, where training is a critical part of building a program. Traditional classrooms often follow a one-size-fits-all model, but every student learns differently. AI tools can adjust to each student's individual pace, style, and level of understanding. For example, some students may grasp concepts quickly, while others may need more time and repeated practice. With AI, students can review lessons, get instant feedback, and move forward when they're ready. This kind of personalized support can help boost student confidence and improve overall learning outcomes. But AI can't become a substitute for teaching and dialogue in a group setting. Learning in any setting occurs as a private activity and a group activity. I can see the place for AI to support learning for an individual working on their own, but struggle to see how it can be used to the same extent for the learning and exploration that happens in a group setting.

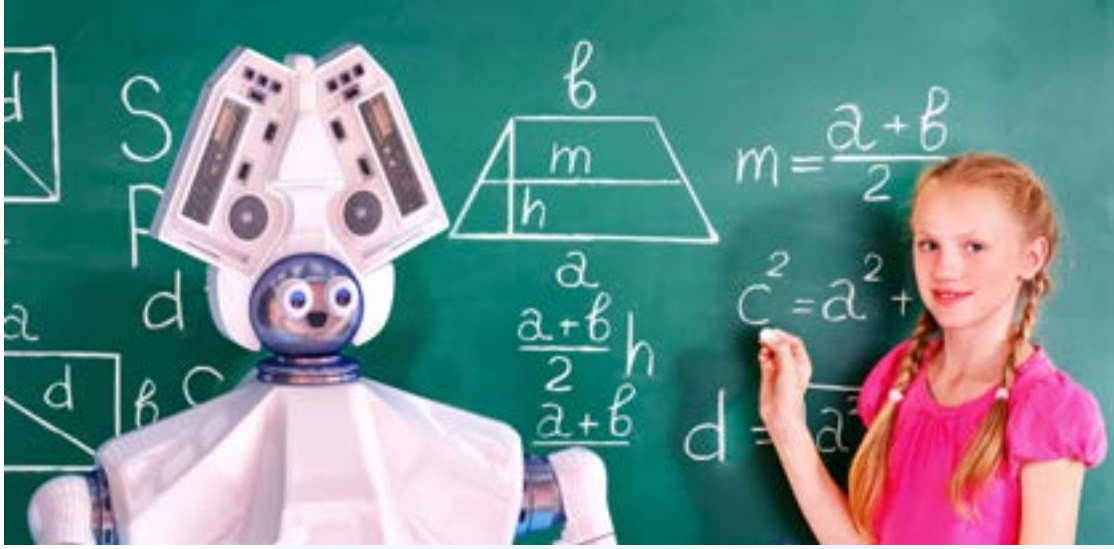
In addition to helping students, AI can greatly support teachers in their daily work. Tasks like grading assignments, planning lessons, and creating practice quizzes can be time-consuming. AI tools can take on many of

un formulaire d'inscription. Travailler avec des personnes en situation de crise dépend de l'interaction humaine et de la connaissance des besoins de la personne. Rien ne remplace le fait de regarder une personne dans les yeux pour comprendre les choses les plus importantes, qui sont souvent inexprimées.

Si nous dépendons de l'IA dans des situations où il y a un besoin humain critique, nous manquerons les choses qui ne sont pas dites. Je pense que c'est vrai à la fois pour mon travail bénévole dans les services sociaux d'urgence et pour la carrière d'enseignant que j'envisage. Les gens dépendront de moi et me confieront beaucoup de responsabilités, et je leur dois de prendre cette responsabilité au sérieux plutôt que de faire confiance à une machine.

Comme tout outil, l'IA a sa place, et le défi consiste à déterminer comment et quand elle peut être utilisée de manière responsable. L'un des nombreux avantages de l'utilisation de l'IA dans l'éducation est sa capacité à soutenir l'apprentissage personnalisé. Cela peut s'appliquer à la fois aux salles de classe, où j'ai l'intention de travailler, et à la gestion de la continuité, où la formation est un élément essentiel de la mise en place d'un programme. Les salles de classe traditionnelles suivent souvent un modèle unique, mais chaque élève apprend différemment. Les outils d'IA peuvent s'adapter au rythme, au style et au niveau de compréhension de chaque élève. Par exemple, certains élèves peuvent saisir rapidement des concepts, tandis que d'autres ont besoin de plus de temps et d'exercices répétés. Grâce à l'IA, les élèves peuvent revoir les leçons, obtenir un retour d'information instantané et avancer lorsqu'ils sont prêts. Ce type de soutien personnalisé peut contribuer à renforcer la confiance des élèves et à améliorer les résultats globaux de l'apprentissage. Mais l'IA ne peut pas se substituer à l'enseignement et au dialogue en groupe. L'apprentissage, quel que soit le contexte, est à la fois une activité privée et une activité de groupe. Je comprends que l'IA puisse soutenir l'apprentissage d'un individu travaillant seul, mais j'ai du mal à voir comment elle peut être utilisée dans la même mesure pour l'apprentissage et l'exploration qui ont lieu dans un contexte de groupe.

En plus d'aider les élèves, l'IA peut grandement aider les enseignants dans leur travail quotidien. Des tâches telles que la correction des devoirs, la planification des cours et la création de questionnaires d'entraînement peuvent prendre beaucoup de temps. Les outils d'IA



these responsibilities, giving teachers more time to focus on connecting with students and offering extra help where needed. AI can also analyze individual students' problems to identify patterns, such as who is falling behind in certain topics. With this information, teachers can make more informed decisions and offer targeted support to individuals or groups, and that is where we need to apply judgement based on relationships and our personal knowledge of the person and the group. Teachers provide emotional support, build relationships, and create a sense of community with their students in the classroom, something AI cannot understand. It's important to find a balance between using technology and maintaining meaningful teacher-student interactions.

Overall, the use of AI in education creates opportunities for a more flexible, responsive, and supportive learning environment. When used correctly, AI can strengthen both teaching and learning by making it easier to meet each student's needs while also reducing the workload on educators by taking on mundane or repetitive tasks. AI can know a subject by looking at patterns in data, but it can't know the person or the group. We will fail those who are depending on us if we misunderstand the limitations of this tool.

One major issue with AI is academic honesty, and I think about that a lot as a student. With the rise of AI tools, it's easier than ever for students to complete assignments without truly understanding the value and meaning of the assignment. Some may rely on AI to write essays or complete assignments for them, which can make

peuvent prendre en charge une grande partie de ces responsabilités, ce qui laisse aux enseignants plus de temps pour se concentrer sur le contact avec les élèves et offrir une aide supplémentaire en cas de besoin. L'IA peut également analyser les problèmes de chaque élève afin d'identifier des schémas, par exemple les élèves qui ont pris du retard dans certaines matières. Grâce à ces informations, les enseignants peuvent prendre des décisions plus éclairées et offrir un soutien ciblé à des individus ou à des groupes, et c'est là que nous devons faire preuve de jugement en nous basant sur les relations et notre connaissance personnelle de la personne et du groupe. Les enseignants apportent un soutien émotionnel, établissent des relations et créent un sentiment de communauté avec leurs élèves dans la salle de classe, ce que l'IA ne peut pas comprendre. Il est important de trouver un équilibre entre l'utilisation de la technologie et le maintien d'interactions significatives entre l'enseignant et l'élève.

Dans l'ensemble, l'utilisation de l'IA dans l'éducation crée des opportunités pour un environnement d'apprentissage plus flexible, plus réactif et plus favorable. Utilisée correctement, l'IA peut renforcer à la fois l'enseignement et l'apprentissage en permettant de répondre plus facilement aux besoins de chaque élève, tout en réduisant la charge de travail des éducateurs en prenant en charge des tâches banales ou répétitives. L'IA peut connaître un sujet en observant des modèles dans les données, mais elle ne peut pas connaître la personne ou le groupe. Nous laisserons tomber ceux qui dépendent de nous si nous ne comprenons pas les limites de cet outil.

it harder for teachers to assess what students actually comprehend from the lessons. This can lead to gaps in learning that are difficult to notice until it's possibly too late. Another concern is the growing dependence on technology in classrooms. When students rely too much on AI, it can weaken important skills such as critical thinking, creativity, and problem-solving.

So, if the misuse of AI amounts to academic dishonesty, it seems to me that the same errors in a professional setting amount to professional dishonesty. AI can be used to help with research, or it can be used to do all the work to generate a final product. If a student were to depend on AI to completely write an assignment it is a short-cut that means the student isn't applying the knowledge, judgement or thinking that they are expected to have. It wouldn't be hard to understand why the student failed, and I would say the same standard should be applied to professionals.

AI is changing the role of the teacher, whether in a public-school classroom or whether the task is to teach people how to work in an emergency. While AI can support educators, it cannot replace the human connection that is so important in learning. AI can help us find answers to questions, but it can't help people understand in a way that helps us develop motivated, curious, and knowledgeable learners. If we depend on AI to build relationships and care about students, we will have failed those who are trusting in us as teachers. Ω

L'un des principaux problèmes liés à l'IA est l'honnêteté académique, et j'y pense beaucoup en tant qu'étudiant. Avec l'essor des outils d'IA, il est plus facile que jamais pour les étudiants de réaliser des travaux sans vraiment en comprendre la valeur et la signification. Certains peuvent compter sur l'IA pour rédiger des essais ou faire des devoirs à leur place, ce qui peut compliquer la tâche des enseignants pour évaluer ce que les élèves ont réellement compris des leçons. Il peut en résulter des lacunes dans l'apprentissage qu'il est difficile de remarquer avant qu'il ne soit trop tard. La dépendance croissante à l'égard de la technologie dans les salles de classe est un autre sujet de préoccupation. Lorsque les élèves dépendent trop de l'IA, cela peut affaiblir des compétences importantes telles que la pensée critique, la créativité et la résolution de problèmes.

Par conséquent, si l'utilisation abusive de l'IA relève de la malhonnêteté académique, il me semble que les mêmes erreurs dans un cadre professionnel relèvent de la malhonnêteté professionnelle. L'IA peut être utilisée pour aider à la recherche ou pour effectuer tout le travail nécessaire à la création d'un produit final. Si un étudiant se fie à l'IA pour rédiger entièrement un devoir, il s'agit d'un raccourci qui signifie que l'étudiant n'applique pas les connaissances, le jugement ou la réflexion qu'il est censé avoir. Il ne serait pas difficile de comprendre pourquoi l'étudiant a échoué, et je dirais que la même norme devrait être appliquée aux professionnels.

L'IA modifie le rôle de l'enseignant, qu'il s'agisse d'une classe d'école publique ou d'une tâche consistant à enseigner aux gens comment travailler dans une situation d'urgence. Si l'IA peut aider les éducateurs, elle ne peut pas remplacer le lien humain qui est si important dans l'apprentissage. L'IA peut nous aider à trouver des réponses à des questions, mais elle ne peut pas aider les gens à comprendre d'une manière qui nous aide à développer des apprenants motivés, curieux et bien informés. Si nous dépendons de l'IA pour établir des relations et nous soucier des étudiants, nous aurons déçu ceux qui nous font confiance en tant qu'enseignants. Ω

ABOUT THE AUTHOR

***Katelyn Holowachuk** is a second year student studying at the Université de Saint-Boniface in Winnipeg she lives in Oakbank, Manitoba with her parents, her sister, and dog Sammy. She is studying to become a teacher.*

À PROPOS DE L'AUTEUR

***Katelyn Holowachuk** est étudiante en deuxième année à l'Université de Saint-Boniface à Winnipeg. Elle vit à Oakbank, au Manitoba, avec ses parents, sa sœur et son chien Sammy. Elle étudie pour devenir enseignante.*

Notice:

The articles presented in ***True North Resilience*** reflect the viewpoints of their respective authors and do not necessarily represent the official stance of DRI Canada. Each author brings their unique perspective, shaped by their experiences and insights within the industry. The purpose of these articles is to foster respectful discourse and encourage critical examination of various aspects of our field.

We believe that promoting thought leadership and encouraging progressive thinking is essential for the growth and evolution of our industry. Readers are invited to interpret the content thoughtfully, considering diverse opinions and ideas. We encourage constructive dialogue, as it is through such discussions that we can enhance our understanding and drive positive change.

DRI Canada is committed to creating an inclusive environment where varying viewpoints can be shared and debated. However, we remind readers that the interpretations and conclusions drawn from these articles are the responsibility of the reader, and we encourage an open-minded approach to all discussions. Ω

Avis :

Les articles présentés dans ***True North Resilience*** reflètent les points de vue de leurs auteurs respectifs et ne représentent pas nécessairement la position officielle de DRI Canada. Chaque auteur apporte son point de vue unique, façonné par ses expériences et ses connaissances au sein de l'industrie. L'objectif de ces articles est de favoriser un discours respectueux et d'encourager l'examen critique des divers aspects de notre domaine.

Nous pensons que la promotion d'un leadership éclairé et l'encouragement d'une pensée progressiste sont essentiels à la croissance et à l'évolution de notre secteur. Les lecteurs sont invités à interpréter le contenu de manière réfléchie, en tenant compte des diverses opinions et idées. Nous encourageons un dialogue constructif, car c'est grâce à ces discussions que nous pouvons améliorer notre compréhension et susciter des changements positifs.

DRI Canada s'engage à créer un environnement inclusif où les différents points de vue peuvent être partagés et débattus. Cependant, nous rappelons aux lecteurs que les interprétations et les conclusions tirées de ces articles relèvent de leur responsabilité, et nous encourageons une approche ouverte à toutes les discussions. Ω

Modernizing Resilience

Integrating Criticality Score (CS) with Recovery Time Objective (RTO)

Moderniser la résilience

Intégration du score de criticité (CS) et de l'objectif de temps de récupération (RTO)

By/Par Nancy Holloway-White, Emad Aziz, & Garth Tucker

For many years now, it has been a fact of life that businesses are fully dependent on IT. We are immersed in the Matrix

Honestly, how many businesses or industries still have paper forms, manual processes, or more importantly, make payments by cheque?

This makes for significant risk to disruptions in business processes or IT systems, which can have severe impacts, e.g. lost revenue, negative reputational impacts, etc.

History

The concepts of RTO and Recovery Point Objective (RPO) originated from the disciplines of disaster recovery planning, within the information technology and data management professions in the 1980s and 90s.

Who developed RTO and RPO?

There is no single individual credited with inventing RTO and RPO, but these concepts were:

- First formalized as part of IT disaster recovery frameworks
- Popularized by early enterprise IT vendors, such as IBM, Sun Microsystems, and EMC, as they developed mainframe recovery strategies and data backup systems

Depuis de nombreuses années, la dépendance des entreprises à l'égard des technologies de l'information est une réalité. Nous sommes immergés dans la matrice

Honnêtement, combien d'entreprises ou d'industries utilisent encore des formulaires papier, des processus manuels ou, plus important encore, effectuent des paiements par chèque ?

Il en résulte un risque important d'interruption des processus d'entreprise ou des systèmes informatiques, qui peut avoir de graves conséquences : perte de revenus, atteinte à la réputation, etc.

Historique

Les concepts de RTO et d'objectif de point de reprise (RPO) sont issus des disciplines de la planification de la reprise après sinistre, au sein des professions des technologies de l'information et de la gestion des données dans les années 1980 et 1990.

Qui a développé la RTO et la RPO ?

Aucune personne n'a inventé la RTO et la RPO, mais ces concepts l'ont été :

- Standardized and codified in frameworks like:
  - o NIST SP 800-34
  - o ISO 22301
  - o EMC
  - o NFPA 1600
  - o BS 25999
  - o DRI International
  - o ITIL v4
  - o Gartner
  - o ISO/IEC 27031:2011

Why RTO and RPO were needed?

As businesses became increasingly dependent on IT systems, there was a need to:

- Define how quickly systems must be restored after a failure (RTO)
- Define how much data loss is acceptable in terms of time (RPO)

These metrics helped organizations prioritize recovery efforts, plan infrastructure investments, and define service level agreements.

Essentially, RTO is the target time within which an application, function, or business unit must be restored following an event to minimize negative effects on the organization.

This metric is typically determined by:

- Revenue impact: How much revenue could the company lose during downtime?
- Business needs: How critical is the service to business operations?
- Customer expectations: How long can customers tolerate service disruptions?

For instance, RTO for customer-facing functions like login systems might be measured in hours, minutes, or seconds, while back-office operations may have far longer recovery times.

This correlates to qualitative (reputational) and quantitative (financial) risk and is the basis for an organization's posture with disaster recovery.

The Challenge

Not all systems, functions, resources, and processes within an organization are of equal importance. Some functions are critical to daily operations, while others may have a lesser impact if disrupted during a low usage period, but become high impact at certain times, e.g. Payroll. Its function is critical two or three times a month in most organizations. This means, if an outage occurs during an off-pay week, it's not a great inconvenience, but if an outage occurs during a payroll run, its pretty critical, especially to those living paycheque to paycheque. RTO is both good and not so good for building resilience when viewed through that lens.

The Good – It lays out the basis of recovery posture for the business' IT.

The Not So Good – It doesn't prioritize recovery efforts efficiently.

The Way Forward – Businesses should consider integrating a CS with the RTO value.

How They Relate

CS measures the importance of a function, application, business unit, or resource to the business, informing the RTO which executes based on this priority.

The CS is calculated first for strategic reasons. It assists in assessing and ranking the importance of systems based on business impact, including financial, customer, compliance, and operational

---

[1] NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, 2010. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

[2] ISO 22301:2019, Security and resilience - Business continuity management systems - Requirements. https://www.iso.org/standard/75106.html

[3] EMC Corporation, information Availability and Business Continuity White Papers, early 2000s.

[4] NFPA 1600, Standard on Continuity, Emergency, and Crisis Management, NFPA, 2016. https://www.nfpa.org/1600

[5] BS 25999-2:2007, Business Continuity Management — Specification, British Standards Institution

[6] DRI International, Professional Practices for Business Continuity Management https://www.drii.org

[7] ITIL v4 – Service Continuity Management, Axelos. https://www.axelos.com/best-practice-solutions/itil

[8] Gartner, Business Continuity Management Program Methodology

[9] ISO/IEC 27031:2011, ICT Readiness for Business Continuity

- formalisés pour la première fois dans le cadre des cadres de reprise après sinistre informatique
- popularisés par les premiers fournisseurs de solutions informatiques d'entreprise, tels qu'IBM, Sun Microsystems et EMC, alors qu'ils développaient des stratégies de reprise des ordinateurs centraux et des systèmes de sauvegarde des données
- Normalisés et codifiés dans des cadres tels que
  - o NIST SP 800-34
  - o ISO 22301
  - o EMC
  - o NFPA 1600
  - o BS 25999
  - o DRI International
  - o ITIL v4
  - o Gartner
  - o ISO/IEC 27031:2011

Pourquoi les RTO et RPO étaient-ils nécessaires ?

Les entreprises devenant de plus en plus dépendantes des systèmes informatiques, il était nécessaire de :

- définir la rapidité avec laquelle les systèmes doivent être restaurés après une panne (RTO)
- Définir le niveau de perte de données acceptable en termes de temps (RPO).

Ces mesures ont aidé les organisations à hiérarchiser les efforts de restauration, à planifier les investissements dans l'infrastructure et à définir des accords sur les niveaux de service.

Essentiellement, le RTO est le délai cible dans lequel une application, une fonction ou une unité commerciale doit être restaurée à la suite d'un événement afin de minimiser les effets négatifs sur l'organisation.

Cette mesure est généralement déterminée par

- L'impact sur le chiffre d'affaires : combien de chiffre d'affaires l'entreprise pourrait-elle perdre pendant le temps d'arrêt ?
- Les besoins de l'entreprise : Dans quelle mesure le service est-il essentiel aux opérations de l'entreprise ?
- Les attentes des clients : Combien de temps les clients peuvent-ils tolérer les interruptions de service ?

Par exemple, le RTO pour les fonctions en contact avec la clientèle, comme les systèmes de connexion, peut être mesuré en heures, minutes ou secondes, alors que les opérations de back-office peuvent avoir des temps de récupération beaucoup plus longs.

Cela correspond à un risque qualitatif (réputation) et quantitatif (financier) et constitue la base de la position d'une organisation en matière de reprise après sinistre.

Le défi

Tous les systèmes, fonctions, ressources et processus d'une organisation n'ont pas la même importance. Certaines fonctions sont essentielles aux opérations quotidiennes, tandis que d'autres peuvent avoir un impact moindre si elles sont interrompues pendant une période de faible utilisation, mais deviennent très importantes à certains moments, par exemple la paie. Cette fonction est critique deux ou trois fois par mois dans la plupart des organisations. En d'autres termes, si une panne survient pendant une semaine sans paie, ce n'est pas très gênant, mais si une panne survient pendant une paie, c'est assez critique, en particulier pour ceux qui vivent d'un chèque de paie à l'autre. Dans cette optique, la RTO est à la fois bonne et moins bonne pour renforcer la résilience.

Le bon point - Il pose les bases d'une posture de reprise pour les technologies de l'information de l'entreprise.

Le moins bon - Il ne permet pas de hiérarchiser efficacement les efforts de reprise.

La voie à suivre - Les entreprises devraient envisager d'intégrer un CS à la valeur du RTO.

Liens entre les deux

La CS mesure l'importance d'une fonction, d'une application, d'une unité opérationnelle ou d'une ressource pour l'entreprise, et informe le RTO qui s'exécute en fonction de cette priorité.

factors. It also provides justification for assigning a short RTO to certain elements.

Criticality scores determine what requires protection, while RTO defines the speed of that protection. These concepts are sequential rather than conflicting.

Moving Forward

What is a Criticality Score? A CS is an assessment of the importance of a system, application, function, or process within an organization. It considers how essential that function is to the continuity of business operations, customer satisfaction, and revenue generation.

Functions or systems with high criticality have a significant impact on the organization if disrupted. When combined with RTO, it creates a better, more strategic approach to resilience, allowing us to recover the most critical functions first while optimizing resources.

The criticality of each function is often assessed based on several factors, including:

- **Revenue dependence:** How closely tied is the function to the company's income stream?
- **Customer impact:** How much will the disruption affect customers or their experience with the service?
- **Regulatory requirements:** Are there legal or compliance-related consequences if the function is disrupted?
- **Operational importance:** Does the function support core business processes that are necessary for day-to-day operations?
- **Recovery complexity:** How difficult / complicated is the recovery process? How long does it take?
- **Dependencies:** How many upstream and downstream applications are dependant on the application?
- **Data sensitivity:** Does the application's database contain PHI or PII data?

Critical functions will have a high criticality score, indicating that they must be prioritized in recovery plans. Conversely, non-essential systems might have a low criticality score, allowing more time for recovery without significant impact.

Le CS est calculé en premier lieu pour des raisons stratégiques. Il permet d'évaluer et de classer l'importance des systèmes en fonction de leur impact sur l'activité, y compris les facteurs financiers, les clients, la conformité et les opérations. Il justifie également l'attribution d'un RTO court à certains éléments.

Les scores de criticité déterminent ce qui doit être protégé, tandis que le RTO définit la vitesse de cette protection. Ces concepts sont séquentiels et non contradictoires.

Aller de l'avant

Qu'est-ce qu'une note de criticité ? Une note de criticité est une évaluation de l'importance d'un système, d'une application, d'une fonction ou d'un processus au sein d'une organisation. Il prend en compte le caractère essentiel de cette fonction pour la continuité des opérations commerciales, la satisfaction des clients et la génération de revenus.

Les fonctions ou systèmes à haute criticité ont un impact significatif sur l'organisation en cas d'interruption. Combiné au RTO, il crée une meilleure approche, plus stratégique, de la résilience, nous permettant de récupérer les fonctions les plus critiques en premier tout en optimisant les ressources.

La criticité de chaque fonction est souvent évaluée sur la base de plusieurs facteurs, notamment

- La dépendance à l'égard des revenus : Dans quelle mesure la fonction est-elle étroitement liée au flux de revenus de l'entreprise ?
- L'impact sur les clients : dans quelle mesure la perturbation affectera-t-elle les clients ou leur expérience du service ?
- Les exigences réglementaires : L'interruption de la fonction a-t-elle des conséquences juridiques ou liées à la conformité ?
- Importance opérationnelle : La fonction soutient-elle les processus opérationnels fondamentaux nécessaires aux activités quotidiennes ?
- Complexité du rétablissement : quel est le degré de difficulté ou de complexité du

Integrating Criticality Score with RTO

When a crisis event occurs, not all systems and processes need to be restored immediately. Some functions can be down for a longer period without causing significant disruption to the business. However, other systems, especially those with a high criticality score, require rapid recovery to minimize operational or customer service disruption.

By combining the Criticality Score with the RTO, businesses can create a more tailored DR plan that reflects the requirements of individual systems, functions, or processes.

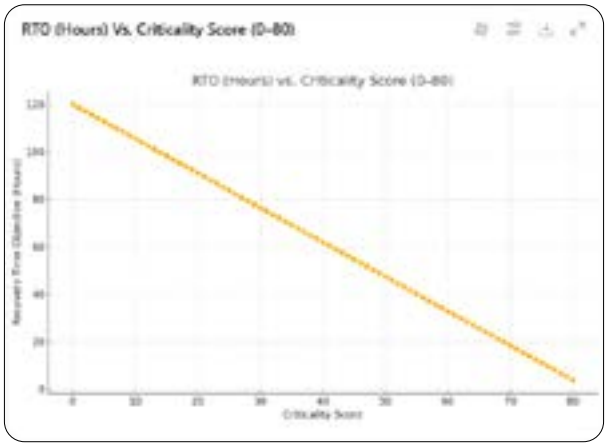
Integration Methodology

1. Assessing Criticality

The first step is to assess the criticality of all business functions as High, Medium, or Low. This involves evaluating each system, process, or application based on the factors listed previously. Rate them on whatever scale you prefer, we've chosen 1 (low) and 5 (high).

Example:

- High criticality: Customer-facing services (e.g., payment systems, user authentication, etc.) that directly impact revenue and customer trust. (4 – 5 on our scale)
- Medium criticality: Internal applications (e.g., HR or accounting software) that are important but not immediately essential for revenue generation. (2.1 – 3.9 on our scale)
- Low criticality: Non-essential systems (e.g., internal reporting tools or non-critical



processus de rétablissement ? Combien de temps cela prend-il ?

- Dépendances : Combien d'applications en amont et en aval dépendent de l'application ?
- Sensibilité des données : La base de données de l'application contient-elle des données PHI ou PII ?

Intégration du score de criticité dans le RTO

En cas de crise, il n'est pas nécessaire de rétablir immédiatement tous les systèmes et processus. Certaines fonctions peuvent rester hors service pendant une période plus longue sans causer de perturbations importantes pour l'entreprise. En revanche, d'autres systèmes, en particulier ceux dont le score de criticité est élevé, nécessitent une restauration rapide afin de minimiser les perturbations des opérations ou du service à la clientèle.

En combinant le score de criticité et le RTO, les entreprises peuvent créer un plan de reprise d'activité mieux adapté qui reflète les exigences des systèmes, fonctions ou processus individuels.

Méthodologie d'intégration

1. Évaluation de la criticité

La première étape consiste à évaluer la criticité de toutes les fonctions de l'entreprise (élevée, moyenne ou faible).

Il s'agit d'évaluer chaque système, processus ou application sur la base des facteurs énumérés précédemment. Notez-les sur l'échelle de votre choix, nous avons choisi 1 (faible) et 5 (élevé).

Exemple :

- Criticité élevée : Services en contact avec la clientèle (systèmes de paiement, authentification des utilisateurs, etc.) qui ont un impact direct sur le chiffre d'affaires et la confiance des clients.) qui ont un impact direct sur le chiffre d'affaires et la confiance des clients. (4 - 5 sur notre échelle)
- Criticité moyenne : Applications internes (par exemple, logiciels de

databases) that have a minimal impact on daily operations. (1 – 2 on our scale)

Assigning weights to a criticality score category is all about reflecting your organization's priorities and risk appetite. Each category (like Financial Impact, Operational Impact, Compliance Risk, etc.) contributes to the overall score based on its assigned weight, which amplifies or reduces its influence. Weighting is based on your organization and what you've agreed on with your risk group, leadership, and SMEs, as long as the total weight equals 100.

Tips for Assigning Weights

1. Use expert judgment from risk, IT, and business leaders/SMEs.
2. Keep it simple and transparent for consistency.
3. Review weights annually or after significant business changes.

2. Assigning RTOs Based on Criticality

Once each function, application, business unit, or resource has been assigned a Criticality Score, the next step is to determine the RTO for each function. The RTO should be set according to the criticality of the system, ensuring that high-priority functions are restored first.

- High criticality systems should have a short RTO, often measured in minutes, or seconds, depending on their importance to the business. These systems require near-instant recovery to prevent revenue loss, customer dissatisfaction, or regulatory non-compliance.
- Medium criticality systems may afford slightly longer RTOs, ranging from several hours to a day. These systems support business operations but may not directly affect customer experience or revenue generation in the short term.
- Low criticality systems can have longerRTOs, ranging from a day to several days, without causing significant disruptions to business operations.

3. Prioritizing Recovery Efforts

Integrating RTO with criticality ensures that businesses can prioritize recovery efforts effectively. When a disruption occurs, the recovery process should focus first on restoring high-criticality systems with the shortest RTOs, such as:

- Customer-facing applications: E-commerce sites, payment processing, account access, and any services directly linked to customer interaction.
- Revenue-generating systems: Core business applications that process transactions or handle client data.

Once these high-priority systems are restored, the recovery process can move on to systems with lower criticality, ensuring that recovery time aligns with business impact.

4. Optimizing Resources

By integrating RTO with criticality, organizations can allocate recovery resources more effectively. High-priority systems may require more backup infrastructure, redundant systems, and faster recovery mechanisms, while low-priority systems can afford more time and fewer resources. This ensures that the recovery plan is both efficient and cost-effective.

Criticality Score Matrix

System/Function	Revenue Impact (×X)	Customer Impact (×X)	Compliance Risk (×X)	Operational Impact (×X)	Recovery Complexity (×X)	Dependencies (×X)	Data Sensitivity (×X)	Total Score
Function 1	4	5	2	5	5	3	3	??
Function 2	2	4	5	4	5	3	3	??
Application 1	3	2	2	6	5	4	5	??
Finance	3	5	5	5	2	2	5	??
HR	5	2	5	4	2	5	5	??
Laptop	1	2	2	4	2	5	3	??

gestion des ressources humaines ou de comptabilité) qui sont importantes mais pas immédiatement essentielles pour la génération de revenus. (2,1 - 3,9 sur notre échelle)

- Faible criticité : Systèmes non essentiels (par exemple, outils de reporting internes ou bases de données non critiques) qui ont un impact minimal sur les opérations quotidiennes. (1 - 2 sur notre échelle)

L'attribution d'une pondération à une catégorie de score de criticité permet de refléter les priorités et l'appétit pour le risque de votre organisation. Chaque catégorie (comme l'impact financier, l'impact opérationnel, le risque de conformité, etc.) contribue au score global en fonction de la pondération qui lui est attribuée, ce qui amplifie ou réduit son influence. La pondération est fonction de votre organisation et de ce que vous avez convenu avec votre groupe de risque, votre direction et vos PME, pour autant que la pondération totale soit égale à 100.

Conseils pour l'attribution des poids

1. S'appuyer sur le jugement d'experts en matière de risques, d'informatique et de dirigeants d'entreprise/PME.
2. Veiller à la simplicité et à la transparence pour assurer la cohérence.
3. Réviser les pondérations chaque année ou après des changements importants dans l'entreprise.

2. Attribution des RTO en fonction de la criticité

Une fois qu'une note de criticité a été attribuée à chaque fonction, application, unité opérationnelle ou ressource, l'étape suivante consiste à déterminer le RTO pour chaque fonction. Le RTO doit être fixé en fonction de la criticité du système, de manière à ce que les fonctions prioritaires soient restaurées en premier.

- Les systèmes à haute criticité doivent avoir un RTO court, souvent mesuré en minutes ou en secondes, en fonction de leur importance pour l'entreprise. Ces systèmes nécessitent une reprise quasi instantanée pour éviter les pertes de revenus, le mécontentement des clients ou la non-conformité aux réglementations.
- Les systèmes de criticité moyenne peuvent se permettre des RTO un peu plus longs, allant de plusieurs heures à une journée. Ces systèmes soutiennent les activités de l'entreprise mais peuvent ne pas avoir d'incidence directe sur l'expérience des clients ou la génération de revenus à court terme.
- Les systèmes de faible criticité peuvent avoir des RTO plus longs, allant d'un jour à plusieurs jours, sans causer de perturbations significatives des activités de l'entreprise.

3. Hiérarchisation des efforts de reprise

L'intégration du RTO et de la criticité permet aux entreprises de hiérarchiser efficacement les efforts de reprise. Lorsqu'une perturbation se

Matrice des scores de criticité

Système/Fonction	Impact sur les revenus(×X)	Impact sur les clients(×X)	Risque de non-conformité (×X)	Impact opérationnel(×X)	Complexité de la reprise(×X)	Dépendances (×X)	Sensibilité des données(×X)	Score total
Fonction 1	4	5	2	5	5	3	3	??
Fonction 2	2	4	5	4	5	3	3	??
Application 1	3	2	2	6	5	4	5	??
Finances	3	5	5	5	2	2	5	??
RH	5	2	5	4	2	5	5	??
Ordinateur portable	1	2	2	4	2	5	3	??

Example: A payment processing system for your organization may require advanced failover capabilities and cloud-based redundancy to meet its aggressive RTO. Meanwhile, a non-critical employee portal can be restored with minimal resources, perhaps relying on scheduled backups and longer recovery windows.

5. Testing and Monitoring

Once a disaster recovery runbook is developed, it is important to regularly test the recovery of both high and low criticality systems to ensure that RTOs are achievable. This includes testing both the recovery speed and the prioritization of systems based on their criticality score.

You should conduct periodic DR exercises that simulate disruptions and validate recovery times across different systems, ensuring that high-priority systems meet their RTO and that all functions are restored within acceptable timeframes.

Where do we Gather the Data to Calculate These Numbers?

There are different methods to gather the data required to identify criticality and RTO, but the most efficient is through the Business Impact Analysis (BIA.)

The BIA is a centralized set of data about the organization that identifies all functions, processes, resources, and most importantly for CS / RTO, impacts to the business for various outage scenarios.

produit, le processus de reprise doit d'abord se concentrer sur la restauration des systèmes à haute criticité ayant les RTO les plus courts, tels que

- Les applications orientées client : Les sites de commerce électronique, le traitement des paiements, l'accès aux comptes et tous les services directement liés à l'interaction avec les clients.
- Systèmes générateurs de revenus : Applications commerciales de base qui traitent les transactions ou les données des clients.

Une fois ces systèmes prioritaires restaurés, le processus de reprise peut passer à des systèmes moins critiques, ce qui permet d'aligner le temps de reprise sur l'impact de l'activité.

4. Optimisation des ressources

En intégrant le RTO à la criticité, les entreprises peuvent allouer les ressources de reprise plus efficacement. Les systèmes hautement prioritaires peuvent nécessiter davantage d'infrastructures de sauvegarde, de systèmes redondants et de mécanismes de reprise plus rapides, tandis que les systèmes faiblement prioritaires peuvent bénéficier de plus de temps et de moins de ressources. Ainsi, le plan de reprise est à la fois efficace et rentable.

Exemple : Un système de traitement des paiements pour votre organisation peut nécessiter des capacités de basculement

How They Work Together

Aspect	Criticality Score	RTO
Type	Qualitative/Quantitative score	Quantitative time metric (hours)
Focus	Business importance	Business tolerance for downtime
Based on	Impact dimensions (financial, customer)	Risk and operational dependencies
Used for	Prioritization of DR planning	Designing recovery timelines
Output	Tiered ranking (e.g., 1–10)	Specific hours or minutes

Note* A high criticality score should generally translate to a shorter RTO, though business context may refine that.

avancées et une redondance basée sur le cloud pour répondre à son RTO agressif.

Dans le même temps, un portail d'employés non critique peut être restauré avec un minimum de ressources, en s'appuyant peut-être sur des sauvegardes programmées et des fenêtres de récupération plus longues.

5. Tests et surveillance

Une fois le plan de reprise d'activité élaboré, il est important de tester régulièrement la reprise des systèmes de haute et de basse criticité afin de s'assurer que les délais de récupération sont réalisables. Il s'agit notamment de tester la vitesse de reprise et la hiérarchisation des systèmes en fonction de leur degré de criticité.

Vous devez effectuer des exercices périodiques de reprise après sinistre qui simulent des perturbations et valident les délais de reprise pour différents systèmes, en veillant à ce que les systèmes hautement prioritaires respectent leur RTO et que toutes les fonctions soient rétablies dans des délais acceptables.

Où recueillir les données nécessaires au calcul de ces chiffres ?

Il existe différentes méthodes pour recueillir les données nécessaires à l'identification de la criticité et du RTO, mais la plus efficace est l'analyse de l'impact sur l'entreprise (BIA).

Le BIA est un ensemble centralisé de données sur l'organisation qui identifie toutes les fonctions, tous les processus, toutes les ressources et, ce qui est le plus important pour le CS / RTO, les impacts sur l'entreprise de divers scénarios de panne.

Ajoutez les mesures nécessaires à votre formulaire/feuille de calcul BIA et alignez ces chiffres avec votre matrice CS/RTO et utilisez l'algorithme et les calculs pour déterminer les chiffres RTO qui répondent aux exigences de votre organisation.

Les avantages commerciaux de l'intégration de la note de criticité au RTO

Les données recueillies dans le BIA, lorsqu'elles sont passées par l'algorithme de notation, calculent les numéros CS, qui, à leur tour, informent les numéros RTO et identifient les fonctions, les processus et les ressources qui doivent être restaurés en premier.

Vous pouvez avoir plusieurs éléments avec des RTO identiques, mais les scores CS sont différents, ce qui définit l'ordre de restauration, garantissant que les applications, les fonctions,

Comment ils fonctionnent ensemble

Aspect	Score de criticité	RTO
Type	Score qualitatif/quantitatif	Mesure quantitative du temps (heures)
Priorité	Importance commerciale	Tolérance commerciale en cas d'indisponibilité
Basé sur	Dimensions de l'impact (financier, client)	Risques et dépendances opérationnelles
Utilisé pour	Hiérarchisation de la planification de la reprise après sinistre	Conception des délais de reprise
Résultat	Classement par niveaux (par exemple, 1 à 10)	Heures ou minutes spécifiques

Remarque* Un score de criticité élevé devrait généralement se traduire par un RTO plus court, bien que le contexte commercial puisse affiner cela.

Add the required metrics to your BIA form/ spreadsheet and align those numbers with your CS to RTO matrix and use the algorithm and calculations to determine RTO numbers that suit your organization's requirements.

The Business Benefits of Integrating Criticality Score with RTO

The data gathered in the BIA, when run through the scoring algorithm, calculates CS numbers, which, in turn, inform the RTO numbers and identify the functions, processes, and resources that must be restored first.

You may have several items with identical RTOs, but the CS scores are different, and this defines the restoration order, ensuring the highest impact applications, functions, processes, and resources are brought back online first.

This is the most efficient use of recovery resources and should be how you structure your crisis response posture to ensure effective, timely, and cost-efficient recovery.

Here are some other benefits you can include when pitching the process to executive leadership.

1. Optimized Resource Allocation: By aligning recovery efforts with the criticality of systems, businesses can allocate recovery resources more efficiently, focusing on high-priority systems first and minimizing unnecessary spending on low-priority systems.
2. Reduced Downtime: With the right focus on critical systems, organizations can restore the most important functions faster, minimizing downtime and reducing the financial and operational impact of outages.
3. Improved Customer Experience: Restoring critical customer-facing systems as quickly as possible ensures that customer experience is minimally affected during disruptions. This helps retain customer trust and loyalty, particularly in industries where uptime is crucial.
4. Compliance and Risk Management: For businesses in regulated industries, meeting RTOs for critical systems ensures compliance with industry standards and regulations, reducing the risk of legal penalties or reputational damage.
5. Increased Business Resilience: A disaster recovery plan that integrates RTO with criticality fosters a more resilient organization, prepared to handle disruptions effectively and recover rapidly to continue business operations without significant loss.

Conclusion

Integrating Criticality Scoring with RTO metrics creates a strategic, efficient, and business-oriented approach to resilience. By ensuring that high-priority systems are restored first within the necessary RTO, businesses can minimize downtime, optimize recovery resources, and mitigate risks to their operations, customers, and revenue.

This integration helps businesses prioritize recovery efforts based on actual business impact rather than a one-size-fits-all approach, ensuring that critical functions are always restored promptly and effectively. With the right combination of RTO and criticality scores, organizations can build a more resilient infrastructure and ensure continuity even in the face of unexpected disruptions. Ω

Example Combined View

System	Criticality Score	RTO
Payment Gateway	9	1 hour
Internal HR Portal	4	24 hours
Customer Support Chatbot	7	4 hours

All photos are licensed under CC BY-SA

les processus et les ressources ayant le plus d'impact sont remis en ligne en premier.

Il s'agit de l'utilisation la plus efficace des ressources de restauration et c'est ainsi que vous devriez structurer votre dispositif de réponse aux crises afin de garantir une restauration efficace, rapide et rentable.

Voici d'autres avantages que vous pouvez inclure lorsque vous présentez le processus à la direction générale.

1. Allocation optimisée des ressources : En alignant les efforts de reprise sur la criticité des systèmes, les entreprises peuvent allouer les ressources de reprise plus efficacement, en se concentrant d'abord sur les systèmes hautement prioritaires et en minimisant les dépenses inutiles sur les systèmes peu prioritaires.
2. Réduction des temps d'arrêt : En se concentrant sur les systèmes critiques, les entreprises peuvent rétablir les fonctions les plus importantes plus rapidement, en minimisant les temps d'arrêt et en réduisant l'impact financier et opérationnel des pannes.
3. Amélioration de l'expérience client : En rétablissant le plus rapidement possible les systèmes critiques en contact avec les clients, on s'assure que l'expérience client est le moins affectée possible pendant les interruptions. Cela permet de conserver la confiance et la fidélité des clients, en particulier dans les secteurs où le temps de fonctionnement est crucial.
4. Conformité et gestion des risques : Pour les entreprises des secteurs réglementés, le respect des RTO pour les systèmes critiques garantit la conformité avec les normes et réglementations du secteur, réduisant ainsi le risque de sanctions légales ou d'atteinte à la réputation.
5. Amélioration de la résilience de l'entreprise : Un plan de reprise après sinistre qui intègre le RTO et la criticité favorise une organisation plus résiliente, préparée à gérer efficacement les perturbations et à se rétablir rapidement pour poursuivre ses activités sans perte importante.

Conclusion

L'intégration de la notation de la criticité avec les mesures du RTO crée une approche stratégique, efficace et orientée métier de la résilience. En s'assurant que les systèmes prioritaires sont restaurés en premier dans le délai de récupération nécessaire, les entreprises peuvent minimiser les temps d'arrêt, optimiser les ressources de récupération et atténuer les risques pour leurs opérations, leurs clients et leur chiffre d'affaires.

Cette intégration aide les entreprises à hiérarchiser les efforts de restauration en fonction de l'impact réel sur l'activité plutôt que d'adopter une approche unique, garantissant ainsi que les fonctions critiques sont toujours restaurées rapidement et efficacement. Avec la bonne combinaison de RTO et de scores de criticité, les entreprises peuvent construire une infrastructure plus résiliente et assurer la continuité même face à des perturbations inattendues. Ω

Exemple de vue combinée

Système	Score de criticité	RTO
Passerelle de paiement	9	1 heure
Portail RH interne	4	24 heures
Chatbot d'assistance à la clientèle	7	4 heures

Toutes les photos sont sous licence CC BY-SA.

ABOUT THE AUTHORS

***Nancy Holloway-White**, CBCP, CBCA (she/her), is currently serving as the President DRI Canada and has been volunteering for DRI Canada in various capacities for over a decade. Nancy works in financial services risk management, specializing in internal controls, process and governance, with a concentration in business continuity.*

***Emad Aziz**, MBCP is a certified Master Business Continuity Professional (MBCP), with 17+ years of collective experience in the private and public sector business continuity, risk management, emergency management and disaster recovery. His strengths are influencing, coaching and advising senior leadership. He has built a reputation and trust with clients who consult with him on time sensitive matters affecting all types of critical business disruptions. He is sought for exercising strong judgement and "out-of- the-box" problem solving in high pressure situations. He is also the recipient of the internationally recognized Disaster Recovery Institute International (DRII) – International Award of Excellence, 2015.*

Garth Tucker *is the Director, Business Continuity for ESO, Editor-in-Chief of the True North Resilience magazine, a member of the DRI Canada (dri.ca) Board of Directors, and a Certified Business Continuity Professional (CBCP). His career focus is on the development and management of holistic resiliency programs as well as effective management of crisis events. The path to his current position began with software development, project and program management, and as an IT technology educator worldwide for IBM in the late 1990s and early 2000s. He transitioned to disaster recovery, business continuity, and crisis management beginning in 2002. Significant formal, and self-education throughout his career has ensured he remains relevant and effective.*

A PROPOS DES AUTERS

***Nancy Holloway-White**, CBCP, CBCA (elle/elle), est actuellement présidente d'IRN Canada et fait du bénévolat pour DRI Canada à divers titres depuis plus d'une décennie. Nancy travaille dans la gestion des risques des services financiers, se spécialisant dans les contrôles internes, les processus et la gouvernance, avec une concentration dans la continuité des activités.*

***Emad Aziz**, MBCP est un maître professionnel de la continuité des activités certifié (MBCP), avec plus de 17 ans d'expérience collective dans la continuité des activités des secteurs privé et public, la gestion des risques, la gestion des urgences et la reprise après sinistre. Ses forces sont d'influencer, d'encadrer et de conseiller la haute direction. Il s'est bâti une réputation et une confiance auprès des clients qui le consultent sur des questions urgentes touchant tous les types de perturbations commerciales critiques. Il est recherché pour exercer un jugement fort et la résolution de problèmes « hors des sentiers battus » dans des situations de haute pression. Il est également récipiendaire du Prix international d'excellence 2015 de l'Institut international de reprise après sinistre (DRII), reconnu à l'échelle internationale.*

Garth Tucker *est directeur de la continuité des activités d'ESO, rédacteur en chef du magazine True North Resilience, membre du conseil d'administration de DRI Canada (dri.ca) et professionnel certifié de la continuité des activités (CBCP). Sa carrière est axée sur l'élaboration et la gestion de programmes de résilience holistiques ainsi que sur la gestion efficace des événements de crise. Le chemin vers son poste actuel a commencé par le développement de logiciels, la gestion de projets et de programmes, et en tant qu'éducateur en technologie informatique dans le monde entier pour IBM à la fin des années 1990 et au début des années 2000. Il est passé à la reprise après sinistre, à la continuité des activités et à la gestion de crise à partir de 2002. Tout au long de sa carrière, il a fait l'objet d'une importante éducation formelle et auto-éducative qui lui a permis de rester pertinent et efficace.*

By/Par Brock Holowachuck

DRI Canada holds Lunch and Learns in Winnipeg and Regina

Students weren't the only people who got back to learning at the beginning of September.

DRI Canada hosted Lunch and Learn events in Winnipeg and Regina at the beginning of September to provide educational and networking opportunities for Certified Professionals in the Central Region. These well-attended events included presentations from expert voices including **Ray Unrau** of Fortress Consulting, **Bob Brown** from SaskPower, **Garth Tucker** with ESO, and **James Gulack** from the Royal Canadian Mounted Police.

DRI Canada organise des déjeuners-causeries à Winnipeg et à Regina

Les étudiants ne sont pas les seuls à avoir repris le chemin de l'apprentissage au début du mois de septembre.

DRI Canada a organisé des déjeuners-causeries à Winnipeg et à Regina au début du mois de septembre afin d'offrir des occasions de formation et de réseautage aux professionnels agréés de la région centrale. Ces événements, qui ont attiré beaucoup de monde, comprenaient des présentations d'experts, notamment **Ray Unrau** de Fortress Consulting, **Bob Brown** de SaskPower, **Garth Tucker** de l'ESO et **James Gulack** de la Gendarmerie royale du Canada.

DRI Canada Lunch and Learn - September 2025 - Regina, Saskatchewan

Ray Unrau brought over four decades of experience as a first responder and emergency manager to his discussion on the effective use of the Incident Command System to multi-agency emergencies. ICS is deeply ingrained in much of our thinking and planning, and it's also something where its foundational elements are not closely applied. Ray's thought-provoking discussion focused on a number of key historic events that have seen the development of ICS, and how our practice and thinking might evolve to focus more on key functional activities that it promotes, rather than a strict application of the structure.

Ray Unrau

Resilience is a word and an idea that has evolved how Continuity Management looks and works. It's also been used so often and in so many ways that it's sometimes hard to understand what exactly it means, and how we can work with it in practical ways that leads to better preparedness. **Garth Tucker**'s presentation spoke to how to pull together planning considerations and data points in a way that makes a more consistent and structured continuity plan.

Ray Unrau a apporté plus de quarante ans d'expérience en tant que premier intervenant et gestionnaire d'urgence à sa discussion sur l'utilisation efficace du système de commandement des incidents dans les situations d'urgence impliquant plusieurs agences. Le SCI est profondément ancré dans notre façon de penser et de planifier, mais c'est aussi quelque chose où ses éléments fondamentaux ne sont pas étroitement appliqués. La discussion de Ray, qui incite à la réflexion, s'est concentrée sur un certain nombre d'événements historiques clés qui ont vu le développement du SCI, et sur la manière dont notre pratique et notre réflexion pourraient évoluer pour se concentrer davantage sur les activités fonctionnelles clés qu'il promeut, plutôt que sur une application stricte de la structure.

Garth Tucker

La résilience est un mot et une idée qui ont fait évoluer l'aspect et le fonctionnement de la gestion de la continuité. Il a également été utilisé si souvent et de tant de façons qu'il est parfois difficile de comprendre ce qu'il signifie exactement et comment nous pouvons l'utiliser de façon pratique pour mieux nous préparer. La présentation de **Garth Tucker** a porté sur la manière de rassembler les considérations de planification et les points de données de manière à obtenir un plan de continuité plus cohérent et plus structuré.

The effective response to an emergency depends on close interaction between every critical system and element within an organization. **Bob Brown**'s discussion at the Regina symposium looked at how the DRI International Professional Practices provide a proven and structured approach that pieces together the very different components of complex organizations in a way that builds culture, cohesion, and leadership throughout all levels.

Robert (Bob) Brown

No matter where you work or what your line of business, continuity managers are wrestling with cybercrime as a growing component of our threat environment. Through decades of work focused on critical infrastructure, **James Gulack** brings both a historic and contemporary perspective to his current position with the Royal Canadian Mounted Police at the National Cybercrime Coordination Centre. James spoke about the national and international activities that are involved with this dynamic and complex threat.

L'efficacité de la réponse à une situation d'urgence dépend de l'interaction étroite entre chaque système et élément critique au sein d'une organisation. Lors du symposium de Regina, **Bob Brown** a expliqué comment les pratiques professionnelles internationales de la DRI constituent une approche éprouvée et structurée qui permet d'assembler les différentes composantes d'organisations complexes de manière à renforcer la culture, la cohésion et le leadership à tous les niveaux.

James Gulak

Quel que soit l'endroit où vous travaillez ou votre secteur d'activité, les responsables de la continuité sont confrontés à la cybercriminalité, une composante de plus en plus importante de notre environnement de menace. Après avoir travaillé pendant des décennies sur les infrastructures critiques, **James Gulack** apporte une perspective à la fois historique et contemporaine à son poste actuel au Centre national de coordination de la lutte contre la cybercriminalité de la Gendarmerie royale du Canada. James a parlé des activités nationales et internationales liées à cette menace dynamique et complexe.

DRI Canada Lunch and Learn - September 2025 - Winnepeg, Manitoba

DRI Canada Lunch and Learn - September 2025 - Regina, Saskatchewan

---

As part of its larger strategy in support of Certified Professionals across the country, DRI Canada has hosted Lunch and Learns and online webinars to provide learning and networking opportunities no matter where you are in the country. Please be sure that your contact information is updated at dri.ca to be sure you get notices of these events, and don't forget that participation counts for points toward your recertification. Ω

Dans le cadre de sa stratégie globale de soutien aux professionnels agréés certifiés à travers le pays, DRI Canada a organisé des déjeuners-conférences et des webinaires en ligne afin d'offrir des opportunités d'apprentissage et de réseautage, où que vous soyez dans le pays. Assurez-vous que vos coordonnées sont à jour sur dri.ca afin de recevoir les avis de ces événements, et n'oubliez pas que votre participation compte pour des points dans le cadre de votre recertification. Ω

ABOUT THE AUTHOR

***Brock Holowachuck**, CBCP, has been a member of the Board of Directors since 2012, and lives and works on Treaty 1 near Winnipeg, Manitoba.*

À PROPOS DE L'AUTEUR

***Brock Holowachuck,** CBCP, est membre du conseil d'administration depuis 2012. Il vit et travaille sur le Traité 1 près de Winnipeg, au Manitoba.*

Student Award and Scholarship

Prix de l'étudiant et bourses d'études

STUDENT AWARD WINNERS
LAURÉATS DU PRIX ÉTUDIANT

DRI CANADA Train. Prepare. Recover.

The Student Award and Scholarship recognizes a post-secondary student who, in the past year, has presented an exceptional project or scholarly work—such as an academic paper, report, or presentation—that is relevant to and adds value to the business continuity, disaster recovery, or emergency management industries.

Eligibility and Requirements

To qualify for this award, nominees must:

- Have been enrolled in a relevant post-secondary program within the past year.
- Submit a completed nomination form.
- Provide an executive summary of their scholarly work (maximum 750 words).
- Submit an essay (maximum 250 words) explaining their inspiration to join the business continuity, disaster recovery, or emergency management professions.
- Obtain an endorsement from a professor, instructor, or senior institutional member confirming the nominee's educational program and achievements.
- Self-nominate by submitting their application.

Award Benefits

This award includes a $2000 scholarship and complimentary enrollment in a BCLE 2000 course. In addition, all applicants will be entered into a draw for admission to the BCLE 2000 course.

Le prix étudiant et la bourse d'études récompensent un étudiant de l'enseignement supérieur qui, au cours de l'année écoulée, a présenté un projet ou un travail universitaire exceptionnel – tel qu'un article, un rapport ou une présentation – qui est pertinent et apporte une valeur ajoutée aux secteurs de la continuité des activités, de la reprise après sinistre ou de la gestion des situations d'urgence.

Éligibilité et conditions

Pour pouvoir prétendre à ce prix, les candidats doivent

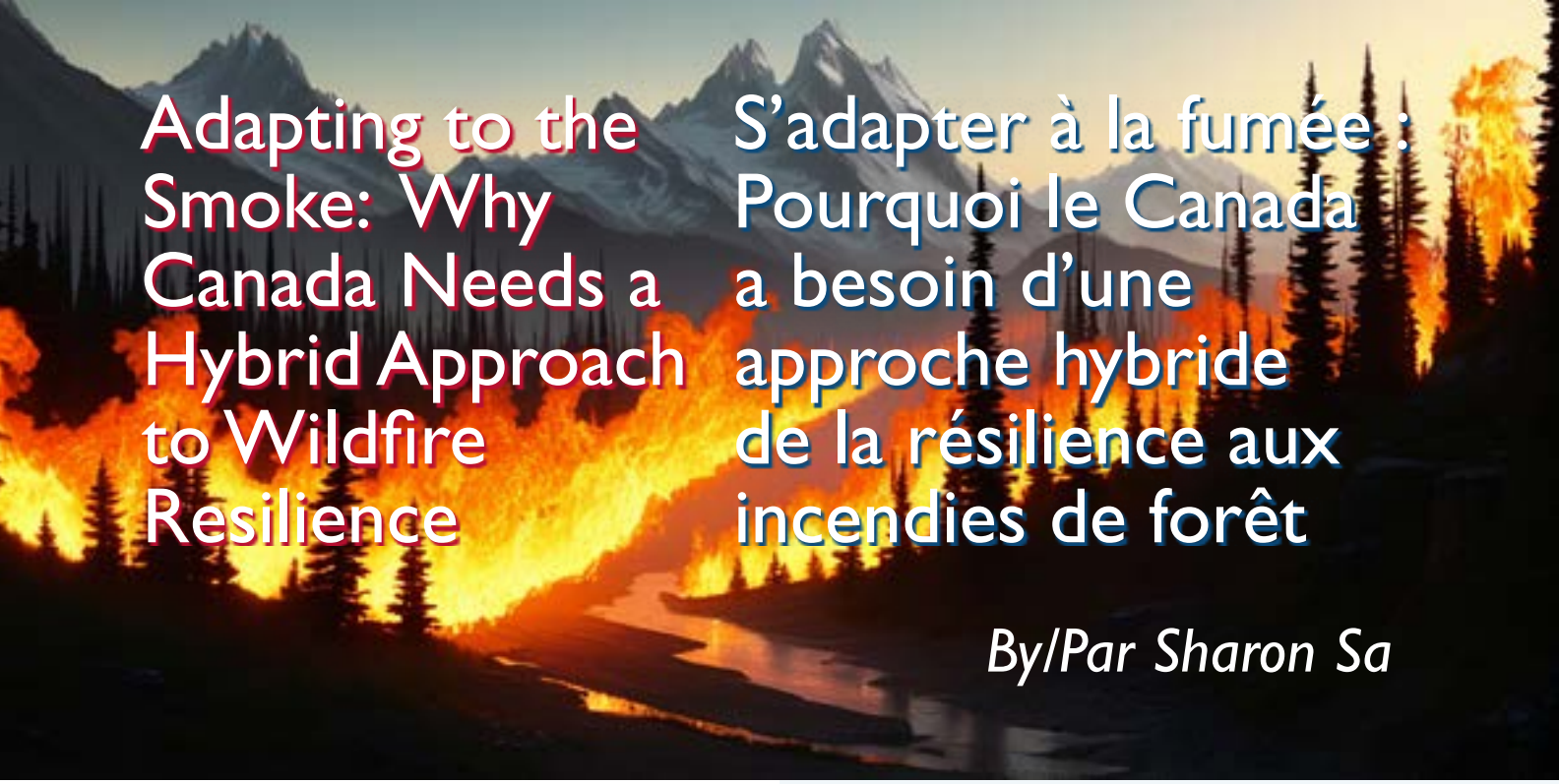
- Avoir été inscrits à un programme d'études postsecondaires pertinent au cours de l'année écoulée.
- Soumettre un formulaire de nomination dûment rempli.
- Fournir un résumé de leurs travaux d'érudition (750 mots maximum).
- Soumettre un essai (250 mots maximum) expliquant leur motivation à rejoindre les professions de la continuité des affaires, de la reprise après sinistre ou de la gestion des urgences.
- Obtenir l'aval d'un professeur, d'un instructeur ou d'un membre éminent de l'institution confirmant le programme d'études et les réalisations du candidat.
- Se porter candidat en soumettant leur dossier de candidature.

Avantages du prix

Ce prix comprend une bourse de 2 000 dollars et une inscription gratuite à un cours BCLE 2000. En outre, tous les candidats seront inscrits à un tirage au sort pour l'admission au cours BCLE 2000.

NB. DRIC invited this year's winners to submit articles. See their submissions on the following pages...

NB. Le DRIC a invité les lauréats de cette année à soumettre des articles. Vous trouverez leurs articles dans les pages suivantes...



Adapting to the Smoke: Why Canada Needs a Hybrid Approach to Wildfire Resilience

S'adapter à la fumée : Pourquoi le Canada a besoin d'une approche hybride de la résilience aux incendies de forêt

By/Par Sharon Sa

STUDENT AWARD WINNER
LAURÉAT DU PRIX DE L'ÉTUDIANT

How do we adapt when the air itself becomes the hazard?

In recent summers, wildfire smoke has turned British Columbia's skies into a familiar, sombre orange. Once understood as a natural part of forest cycles, wildfires are now being supercharged by climate change, transforming smoke into a recurring public-health crisis. Experts anticipate hotter, drier summers will further intensify wildfire activity and smoke in the years ahead and the trend is undeniable (Jain et al., 2024). In 2023, BC endured its most destructive fire season on record, with more than 28,900 km² burned (over twice the area of the next worst year); a stark marker of a new era of extreme wildfires.

Why PM2.5 Is So Harmful – and Why No One Is Safe

The health burden of wildfire smoke is largely attributed to fine particulate matter known as particulate matter 2.5 or PM2.5. These microscopic particles are small enough to penetrate deep into the lungs and even enter the bloodstream, triggering inflammation in organs far from the initial exposure (Chrobak, 2025).

Health authorities recognize PM2.5 as a serious threat, linking it to a wide range of problems

Comment s'adapter lorsque l'air lui-même devient un danger ?

Au cours des derniers étés, la fumée des incendies de forêt a transformé le ciel de la Colombie-Britannique en un orange sombre et familier. Autrefois considérés comme un élément naturel des cycles forestiers, les incendies de forêt sont aujourd'hui suralimentés par le changement climatique, transformant la fumée en une crise récurrente pour la santé publique. Les experts prévoient que des étés plus chauds et plus secs intensifieront encore l'activité et la fumée des feux de forêt dans les années à venir, et la tendance est indéniable (Jain et al., 2024). En 2023, la Colombie-Britannique a connu sa saison d'incendies la plus destructrice jamais enregistrée, avec plus de 28 900 km² brûlés (plus de deux fois la superficie de l'année suivante la plus défavorable), ce qui est un signe frappant d'une nouvelle ère d'incendies de forêt extrêmes.

Pourquoi les PM2,5 sont-elles si nocives et pourquoi personne n'est à l'abri ?

Le fardeau sanitaire de la fumée des incendies de forêt est largement attribué aux particules fines, connues sous le nom de particules 2,5 ou PM2,5. Ces particules microscopiques sont suffisamment petites pour pénétrer profondément dans les poumons et même dans la circulation sanguine, déclenchant une inflammation dans des organes éloignés de l'exposition initiale (Chrobak, 2025).

from breathing difficulties to heart attacks and strokes (Government of Canada, 2024). Short-term exposure can also strain hospitals: during a heavy smoke episode in Baltimore in June 2023, cardiopulmonary visits rose nearly 20 percent (Maldarelli et al., 2024).

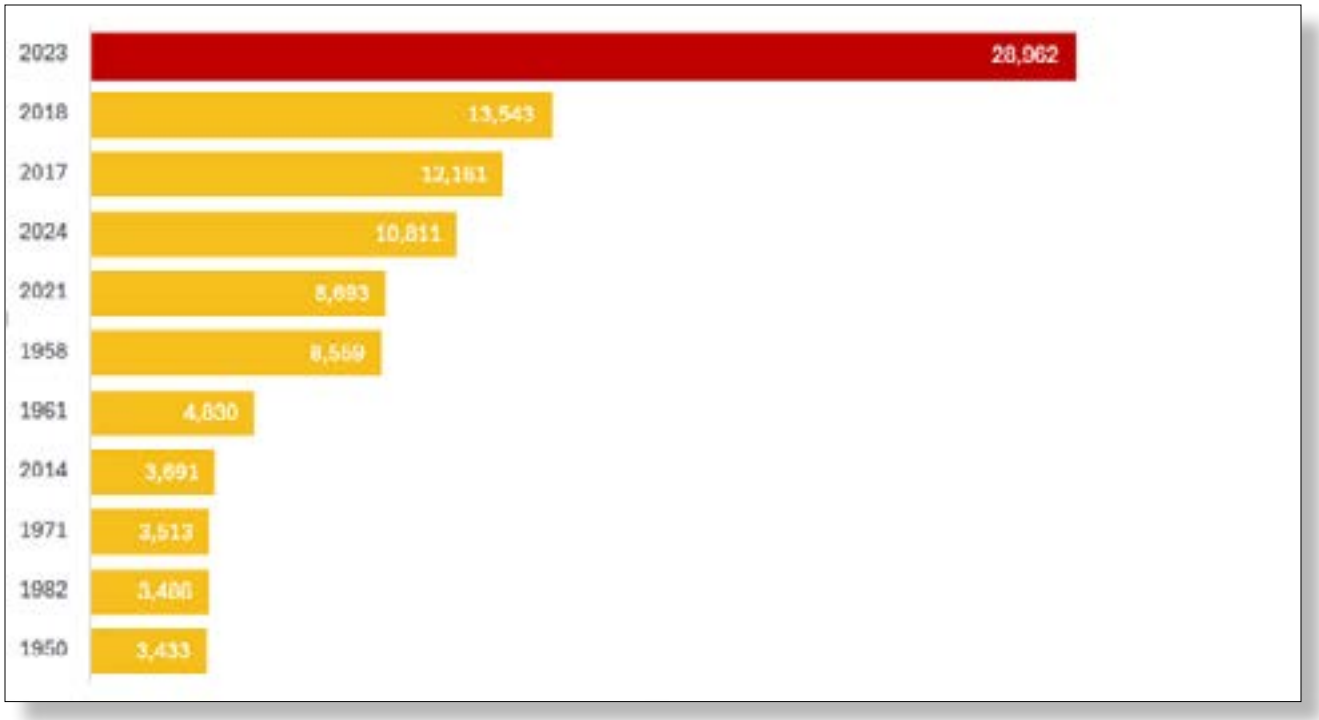
Over longer periods, exposure is associated with chronic respiratory diseases, cardiovascular disease, cognitive impairment, and even adverse pregnancy outcomes such as low birth weight and preterm birth. In fact, a recent study found a 3.4% increase in risk of preterm birth after just one week of elevated wildfire smoke, even when air quality was only in the "moderate" range (Garthwaite, 2021).

The World Health Organization's air quality guidelines emphasize that no amount of PM2.5 is considered safe; even low exposure can carry

Sur de plus longues périodes, l'exposition est associée à des maladies respiratoires chroniques, à des maladies cardiovasculaires, à des troubles cognitifs et même à des issues défavorables de la grossesse telles que l'insuffisance pondérale à la naissance et les naissances prématurées. En fait, une étude récente a révélé une augmentation de 3,4 % du risque de naissance prématurée après seulement une semaine d'exposition élevée à la fumée des incendies de forêt, même lorsque la qualité de l'air n'était que "modérée" (Garthwaite, 2021).

Les lignes directrices de l'Organisation mondiale de la santé relatives à la qualité de l'air soulignent qu'aucune quantité de PM2,5 n'est considérée comme sûre ; même une faible exposition peut avoir des effets sur la santé. En d'autres termes, personne n'est totalement à l'abri de la fumée des incendies de forêt. Même les personnes jeunes et en bonne santé peuvent tousser, souffrir de maux de tête ou voir leurs performances cognitives diminuer (Cleland et al., 2022) lors d'épisodes de fumée importants. Bien entendu,

Top fire seasons in B.C. since 1950 by square kilometeres burned
Principales saisons des incendies en Colombie-Britannique depuis 1950, en fonction du nombre de kilomètres carrés brûlés



Note. Figure adapted from McElroy (2023). Data sourced from the BC Wildfire Service. Excludes current 2025 data, false alarms, nuisance fires, and training fires.
Note. Figure adaptée de McElroy (2023). Données provenant du BC Wildfire Service. Ne comprend pas les données actuelles de 2025, les fausses alarmes, les incendies de nuisance et les incendies d'entraînement.

health impacts. Simply put, no one is completely safe with wildfire smoke. Even young and healthy individuals may experience coughing, headaches, or reduced cognitive performance (Cleland et al., 2022) during major smoke events. And of course, certain groups are especially vulnerable: children, seniors, pregnant women, and people with pre-existing heart or lung conditions face higher risks. Those of lower socio-economic status are also at greater risk due to factors like substandard housing and limited access or awareness to protective measures. The harm of PM2.5 is pervasive and indiscriminate, meaning our resilience strategies must account for everyone.

The Limits of Individual Adaptation

For professionals in disaster recovery and risk management, wildfire smoke is an emerging challenge that demands attention. Unlike sudden hazards like earthquakes or floods, smoke is diffuse, prolonged, and transboundary in nature, making it difficult to contain and costly to ignore.

Public health agencies increasingly acknowledge that different groups experience smoke in different ways, yet the prevailing approach continues to place responsibility on individuals.

The advice is familiar: stay indoors, close your windows, run an air purifier. These steps can reduce personal exposure, but in practice the logic often runs backwards. In reality, not everyone can reduce exposure. Older homes often have leaky ventilation. Portable air purifiers and replacement filters are costly. Smoky air can seep into shared spaces like schools, community centers or shelters if buildings aren't equipped with dated filtration systems. Above all, the people least able to take protective actions, such as outdoor workers, are often the ones most at risk.

This gap between guidance and reality became the crux of my recent Master's capstone project at Simon Fraser University, which set out to examine how decision-makers understand wildfire smoke adaptation and whether socio-economic factors (like income disparities) are being accounted for in policies.

certains groupes sont particulièrement vulnérables : les enfants, les personnes âgées, les femmes enceintes et les personnes souffrant de troubles cardiaques ou pulmonaires préexistants courent des risques plus élevés. Les personnes au statut socio-économique inférieur sont également plus exposées en raison de facteurs tels que les logements insalubres et l'accès limité aux mesures de protection ou la méconnaissance de ces dernières. La nocivité des PM2,5 est omniprésente et aveugle, ce qui signifie que nos stratégies de résilience doivent tenir compte de tout le monde.

Les limites de l'adaptation individuelle

Pour les professionnels de la reprise après sinistre et de la gestion des risques, la fumée des incendies de forêt est un nouveau défi qui demande de l'attention. Contrairement aux risques soudains tels que les tremblements de terre ou les inondations, la fumée est diffuse, prolongée et transfrontalière par nature, ce qui la rend difficile à contenir et coûteuse à ignorer.

Les agences de santé publique reconnaissent de plus en plus que les fumées ne sont pas ressenties de la même manière par tous les groupes, mais l'approche dominante continue de faire porter la responsabilité sur les individus.

Les conseils sont connus : restez à l'intérieur, fermez vos fenêtres, utilisez un purificateur d'air. Ces mesures peuvent réduire l'exposition personnelle, mais dans la pratique, la logique est souvent inversée. En réalité, tout le monde ne peut pas réduire son exposition. Les maisons anciennes sont souvent mal ventilées. Les purificateurs d'air portables et les filtres de remplacement sont coûteux. L'air enfumé peut s'infiltrer dans des espaces partagés comme les écoles, les centres communautaires ou les refuges si les bâtiments ne sont pas équipés de systèmes de filtration récents. Surtout, les personnes les moins à même de prendre des mesures de protection, comme les travailleurs en extérieur, sont souvent les plus exposées.

Ce fossé entre les orientations et la réalité est devenu le point central de mon récent projet de maîtrise à l'université Simon Fraser, qui visait à examiner comment les décideurs comprennent l'adaptation à la fumée des incendies de forêt et si les facteurs socio-économiques (tels que les disparités de revenus) sont pris en compte dans les politiques.

Des entretiens avec quinze décideurs et experts ont révélé que si la fumée des incendies de forêt est effectivement reconnue comme un grave problème de santé publique, elle est également considérée comme un défi en

Interviews with fifteen policymakers and experts revealed that while wildfire smoke is indeed recognized as a serious public health concern, but it is also viewed as a governance challenge. Adaptation efforts remain fragmented across jurisdictions – particularly for rural and remote communities. Some communities have far better access than others to tools like local air quality monitoring, public clean-air spaces, or multilingual health messaging. These resources can build stronger community resilience, yet without clear provincial leadership and sustainable funding, responsibilities can easily slip through the cracks. In short, leaving adaptation to individual efforts or ad-hoc local initiatives has led to patchwork progress at best, and dangerous blind spots at worst.

A Hybrid Approach to Wildfire Smoke Resilience

So, what would a better model look like? The research points to a hybrid approach. This means pairing strong top-down investment in clean air infrastructure with bottom-up, community-led outreach. Both pieces are essential and complementary.

On the structural side, provincial and federal governments must lay the groundwork by bolstering the clean-air infrastructure that individuals alone cannot secure. This can include funding ventilation upgrades in schools and public buildings (for example, the B.C. government spent $2.5 million in 2023 to install 1,914 HEPA filtration units in classrooms lacking mechanical ventilation), providing rebates or grants for home air cleaners, and setting up designated "clean air" spaces in libraries or community centers. Such measures create a baseline of protection, or a resiliency floor, that benefits everyone.

Indeed, infrastructure investments carry a price tag, but the costs of inaction are far higher. Health Canada estimates that wildfire smoke already contributes to hundreds of premature deaths and up to $1.8 billion in short-term health costs in Canada each year.

These staggering impacts underscore why investing in cleaner air is a matter of public safety

matière de gouvernance. Les efforts d'adaptation restent fragmentés d'une juridiction à l'autre, en particulier pour les communautés rurales et isolées. Certaines communautés ont un bien meilleur accès que d'autres à des outils tels que la surveillance de la qualité de l'air au niveau local, les espaces publics d'air pur ou les messages sanitaires multilingues. Ces ressources peuvent renforcer la résilience des communautés, mais en l'absence d'un leadership provincial clair et d'un financement durable, les responsabilités peuvent facilement passer entre les mailles du filet. En bref, laisser l'adaptation aux efforts individuels ou aux initiatives locales ad hoc a conduit au mieux à des progrès disparates, et au pire à de dangereuses zones d'ombre.

Une approche hybride de la résistance aux fumées des incendies de forêt

À quoi ressemblerait donc un meilleur modèle ? Les recherches montrent qu'il faut adopter une approche hybride. Cela signifie qu'il faut combiner des investissements importants dans l'infrastructure d'assainissement de l'air et des actions de sensibilisation menées par les collectivités locales. Ces deux éléments sont essentiels et complémentaires.

Sur le plan structurel, les gouvernements provinciaux et fédéral doivent préparer le terrain en renforçant l'infrastructure de l'air pur que les individus seuls ne peuvent pas assurer. Il peut s'agir de financer l'amélioration de la ventilation dans les écoles et les bâtiments publics (par exemple, le gouvernement de la Colombie-Britannique a dépensé 2,5 millions de dollars en 2023 pour installer 1 914 unités de filtration HEPA dans des salles de classe dépourvues de ventilation mécanique), d'accorder des remises ou des subventions pour les purificateurs d'air à domicile et de créer des espaces "air pur" dans les bibliothèques ou les centres communautaires. De telles mesures créent une base de protection, ou un plancher de résilience, qui profite à tous.

En effet, les investissements dans les infrastructures ont un coût, mais les coûts de l'inaction sont bien plus élevés. Santé Canada estime que la fumée des incendies de forêt contribue déjà à des centaines de décès prématurés et à des coûts de santé à court terme pouvant atteindre 1,8 milliard de dollars par an au Canada.

Ces impacts stupéfiants soulignent pourquoi l'investissement dans un air plus pur est une question de sécurité publique et de prudence économique. Comme le décrit un ingénieur en CVC, l'utilisation de filtres à haute

and economic prudence. As one HVAC engineer describes, using high-efficiency filters and other protections "is really something we need to do moving forward" (Eltherington, 2023). Yet currently, indoor air quality standards are mostly voluntary, as is providing protections for outdoor workers. Public health experts are calling for stronger standards to ensure shared spaces have safe air even when wildfire smoke rolls in. Advocating for these structural interventions is a key role resilience professionals can play.

On the community side, local organizations and networks play a role that centralized government programs cannot easily replicate. Community-based groups bring trust, cultural knowledge, and on-the-ground agility that make adaptation efforts more effective. They can tailor outreach to the people most at risk and "meet residents where they are." Whether it's delivering multilingual smoke risk messaging in non-English speaking communities, lending out portable air filters to lower-income households, or installing community-run air quality sensors in a remote town, these efforts ensure solutions that reach those who need them most.

During the research interviews, experts repeatedly stressed that without local voices and partnerships, top-down strategies risk being too abstract or inaccessible to make a real difference. Community leaders, including Indigenous communities, non-profits, health clinics, religious spaces, and libraries, should be equal partners in planning and decision-making, not an afterthought. They often know best who in the community requires extra help during a smoke event and how to get it to them. By empowering local initiatives (with funding), local governments can vastly extend the reach of adaptation measures.

Taken together, this hybrid model offers a practical and equitable path forward. It acknowledges that wildfire smoke is both a structural challenge and a community-level challenge. This synergy can close the gaps that an individual-centric approach leaves open. Crucially, a hybrid model also builds trust; communities see that higher authorities are investing in

efficacité et d'autres protections "est vraiment quelque chose que nous devons faire à l'avenir" (Eltherington, 2023). Pourtant, à l'heure actuelle, les normes de qualité de l'air intérieur sont essentiellement volontaires, tout comme la protection des travailleurs extérieurs. Les experts en santé publique réclament des normes plus strictes pour garantir que les espaces partagés disposent d'un air sain, même lorsque la fumée des incendies de forêt s'y infiltre. Les professionnels de la résilience peuvent jouer un rôle clé en plaidant en faveur de ces interventions structurelles.

Du côté des communautés, les organisations et les réseaux locaux jouent un rôle que les programmes gouvernementaux centralisés ne peuvent pas facilement reproduire. Les groupes communautaires apportent la confiance, les connaissances culturelles et l'agilité sur le terrain qui rendent les efforts d'adaptation plus efficaces. Ils peuvent adapter les actions de sensibilisation aux personnes les plus exposées et "rencontrer les habitants là où ils sont". Qu'il s'agisse de diffuser des messages multilingues sur les risques liés à la fumée dans les communautés non anglophones, de prêter des filtres à air portables aux ménages à faibles revenus ou d'installer des capteurs de qualité de l'air gérés par la communauté dans une ville isolée, ces efforts garantissent des solutions qui atteignent ceux qui en ont le plus besoin.

Au cours des entretiens de recherche, les experts ont souligné à plusieurs reprises que sans les voix et les partenariats locaux, les stratégies descendantes risquent d'être trop abstraites ou inaccessibles pour faire une réelle différence. Les dirigeants communautaires, y compris les communautés indigènes, les organisations à but non lucratif, les dispensaires, les lieux de culte et les bibliothèques, devraient être des partenaires à part entière dans la planification et la prise de décision, et non pas être considérés après coup. Ils sont souvent les mieux placés pour savoir qui, au sein de la communauté, a besoin d'une aide supplémentaire lors d'un épisode de fumée et comment la lui apporter. En renforçant les initiatives locales (avec des fonds), les gouvernements locaux peuvent étendre considérablement la portée des mesures d'adaptation.

Dans l'ensemble, ce modèle hybride offre une solution pratique et équitable. Il reconnaît que la fumée des incendies de forêt est à la fois un défi structurel et un défi communautaire. Cette synergie peut combler les lacunes qu'une approche centrée sur l'individu laisse subsister. Les communautés voient que les autorités supérieures

their safety, and authorities see community organizations as vital allies.

Implications for Practitioners

For professionals in disaster recovery and risk management, several lessons emerge:

- **Treat wildfire smoke as a recurring hazard.** It requires the same level of planning as other climate hazards like floods or earthquakes.
- **Center equity in preparedness.** A "one-size-fits-all" approach leaves systemic gaps. Incorporate socioeconomic and geographic factors into risk assessments.
- **Build partnerships early.** Pre-establish networks for communication and resource-sharing. For example, agreements with local centres to serve as cleaner air spaces, or volunteer groups ready to check on vulnerable residents during smoke advisories. Collaborative relationships forged in advance lead to far more effective response and recovery efforts.
- **Advocate for structural investment.** Use your voice to highlight the economic and health costs of inaction. Quantify for decision-makers the economic and health costs of inaction to make the case for government support.

The urgency is clear. The 2023 season was not an outlier but a preview of a future shaped by more frequent and intense fires. Without a course correction, inequalities will deepen, and communities already stretched thin will bear the brunt. The question is whether wildfire smoke remains an individual burden or becomes a shared responsibility. My research points to the latter. By combining provincial leadership with community-driven adaptation, we can shift to a model that secures clean indoor air, supports local organizations, and ensures protection is not determined by income or geography. The air we breathe is collective. Our response should be too. Ω

investissent dans leur sécurité, et les autorités considèrent les organisations communautaires comme des alliés essentiels.

Implications pour les praticiens

Plusieurs enseignements se dégagent pour les professionnels de la reprise après sinistre et de la gestion des risques :

- Traiter la fumée des incendies de forêt comme un risque récurrent. Ils nécessitent le même niveau de planification que les autres risques climatiques tels que les inondations ou les tremblements de terre.
- Centrer l'équité dans la préparation. Une approche "unique" laisse des lacunes systémiques. Intégrer les facteurs socio-économiques et géographiques dans l'évaluation des risques.
- Établir des partenariats dès le début. Préétablissez des réseaux de communication et de partage des ressources. Par exemple, des accords avec des centres locaux pour servir d'espaces d'air pur, ou des groupes de bénévoles prêts à surveiller les résidents vulnérables pendant les avis de fumée. Les relations de collaboration établies à l'avance permettent d'améliorer considérablement l'efficacité de la réponse et des efforts de récupération.
- Plaidez en faveur d'investissements structurels. Utilisez votre voix pour mettre en évidence les coûts économiques et sanitaires de l'inaction. Quantifiez pour les décideurs les coûts économiques et sanitaires de l'inaction afin d'obtenir le soutien des pouvoirs publics.

L'urgence est évidente. La saison 2023 n'était pas une anomalie, mais un aperçu d'un avenir marqué par des incendies plus fréquents et plus intenses. Si l'on ne rectifie pas le tir, les inégalités s'aggraveront et les communautés, déjà très sollicitées, en feront les frais. La question est de savoir si la fumée des incendies de forêt reste un fardeau individuel ou si elle devient une responsabilité partagée. Mes recherches tendent vers cette dernière solution. En combinant le leadership provincial et l'adaptation communautaire, nous pouvons passer à un modèle qui garantisse un air intérieur pur, soutienne les organisations locales et garantisse que la protection n'est pas déterminée par les revenus ou la géographie. L'air que nous respirons est collectif. Notre réponse doit l'être aussi. Ω

References

BC Hydro. (n.d.). Energy Star® Air Purifiers. https://www.bchydro.com/content/dam/BCHydro/customer-portal/documents/power-smart/residential/programs/air-purifiers-fact-sheet-spring-summer-2025.pdf

Chrobak, U. (2025, July 14). 5 key facts about wildfires and clean air policies | Stanford Doerr School of Sustainability. Stanford University. https://sustainability.stanford.edu/news/5-key-facts-about-wildfires-and-clean-air-policies

Cleland, S. E., Wyatt, L. H., Wei, L., Paul, N., Serre, M. L., West, J. J., Henderson, S. B., & Rappold, A. G. (2022). Short-Term Exposure to Wildfire Smoke and PM2.5 and Cognitive Performance in a Brain-Training Game: A Longitudinal Study of U.S. Adults. Environmental Health Perspectives, 130(6), 067005. https://doi.org/10.1289/EHP10498

Eltherington, W. (2023, July 21). Wildfire smoke highlights need for better ventilation in public spaces, experts say. CityNews Calgary. https://calgary.citynews.ca/2023/07/21/wildfire-smoke-highlights-need-for-better-ventilation-in-public-spaces-experts-say/

Garthwaite, J. (2021, August 23). Wildfire smoke exposure during pregnancy increases preterm birth risk, study finds | Stanford Doerr School of Sustainability. Stanford University. https://sustainability.stanford.edu/news/wildfire-smoke-exposure-during-pregnancy-increases-preterm-birth-risk-study-finds

Health Canada. (2024, June 6). Human health effects of wildfire smoke report summary [Blog]. Government of Canada. https://www.canada.ca/en/services/health/healthy-living/environment/air-quality/wildfire-smoke/human-health-effects-report-summary.html

Housing Infrastructure and Communities Canada. (2024, March 15). Ventilation upgrades for schools across B.C. [News releases]. Government of Canada. https://www.canada.ca/en/housing-infrastructure-communities/news/2024/03/ventilation-upgrades-for-schools-across-bc.html

Jain, P., Barber, Q. E., Taylor, S. W., Whitman, E., Castellanos Acuna, D., Boulanger, Y., Chavardès, R. D., Chen, J., Englefield, P., Flannigan, M., Girardin, M. P., Hanes, C. C., Little, J., Morrison, K., Skakun, R. S., Thompson, D. K., Wang, X., & Parisien, M.-A. (2024). Drivers and Impacts of the Record-Breaking 2023 Wildfire Season in Canada. Nature Communications, 15(1), 6764. https://doi.org/10.1038/s41467-024-51154-7

Maldarelli, M. E., Song, H., Brown, C. H., Situt, M., Reilly, C., Mahurkar, A.A., Felix, V., Crabtree, J., Ellicott, E., Jurczak, M. O., Pant, B., Gumel, A., Zafari, Z., D'Souza, W., Sapkota, A., & Maron, B.A. (2024). Polluted Air from Canadian Wildfires and Cardiopulmonary Disease in the Eastern US. JAMA Network Open, 7(12), e2450759. https://doi.org/10.1001/jamanetworkopen.2024.50759

McElroy, J. (2023, July 18). The 2023 wildfire season is now B.C's most destructive on record—And it's only mid-July. CBC News. https://www.cbc.ca/news/canada/british-columbia/bc-wildfire-july-18-1.6909596

Sa, S. (2025, April 15). Adapting to the smoke: Policymaker responses to wildfire-induced air pollution in Metro Vancouver [Library Archive]. SFU Summit Library; Simon Fraser University. https://summit.sfu.ca/item/39408

World Health Organization. (2021). WHO Global Air Quality Guidelines: Particulate Matter (PM2. 5 and PM10), Ozone, Nitrogen Dioxide, Sulfur Dioxide and Carbon Monoxide (1st ed). World Health Organization. https://iris.who.int/bitstream/handle/10665/345329/9789240034228-eng.pdf

Références

BC Hydro. (s.d.). Energy Star® Air Purifiers. https://www.bchydro.com/content/dam/BCHydro/customer-portal/documents/power-smart/residential/programs/air-purifiers-fact-sheet-spring-summer-2025.pdf

Chrobak, U. (2025, 14 juillet). 5 key facts about wildfires and clean air policies | Stanford Doerr School of Sustainability. Stanford University. https://sustainability.stanford.edu/news/5-key-facts-about-wildfires-and-clean-air-policies

Cleland, S. E., Wyatt, L. H., Wei, L., Paul, N., Serre, M. L., West, J. J., Henderson, S. B. et Rappold, A. G. (2022). Short-Term Exposure to Wildfire Smoke and PM2.5 and Cognitive Performance in a Brain-Training Game : A Longitudinal Study of U.S. Adults. Environmental Health Perspectives, 130(6), 067005. https://doi.org/10.1289/EHP10498

Eltherington, W. (2023, 21 juillet). Wildfire smoke highlights need for better ventilation in public spaces, experts say. CityNews Calgary. https://calgary.citynews.ca/2023/07/21/wildfire-smoke-highlights-need-for-better-ventilation-in-public-spaces-experts-say/

Garthwaite, J. (2021, 23 août). L'exposition à la fumée des incendies de forêt pendant la grossesse augmente le risque de naissance prématurée, selon une étude. Stanford University. https://sustainability.stanford.edu/news/wildfire-smoke-exposure-during-pregnancy-increases-preterm-birth-risk-study-finds

Santé Canada. (2024, 6 juin). Résumé du rapport sur les effets de la fumée des feux de forêt sur la santé humaine [Blog]. Gouvernement du Canada. https://www.canada.ca/en/services/health/healthy-living/environment/air-quality/wildfire-smoke/human-health-effects-report-summary.html

Logement, infrastructure et collectivités Canada. (2024, 15 mars). Amélioration de la ventilation dans les écoles de la Colombie-Britannique [Communiqués de presse]. Gouvernement du Canada. https://www.canada.ca/en/housing-infrastructure-communities/news/2024/03/ventilation-upgrades-for-schools-across-bc.html

Jain, P., Barber, Q. E., Taylor, S. W., Whitman, E., Castellanos Acuna, D., Boulanger, Y., Chavardès, R. D., Chen, J., Englefield, P., Flannigan, M., Girardin, M. P., Hanes, C. C., Little, J., Morrison, K., Skakun, R. S., Thompson, D. K., Wang, X., & Parisien, M.-A. (2024). Facteurs et impacts de la saison record des incendies de forêt de 2023 au Canada. Nature Communications, 15(1), 6764. https://doi.org/10.1038/s41467-024-51154-7

Maldarelli, M. E., Song, H., Brown, C. H., Situt, M., Reilly, C., Mahurkar, A.A., Felix, V., Crabtree, J., Ellicott, E., Jurczak, M. O., Pant, B., Gumel, A., Zafari, Z., D'Souza, W., Sapkota, A., & Maron, B.A. (2024). Polluted Air from Canadian Wildfires and Cardiopulmonary Disease in the Eastern US (Air pollué par les incendies de forêt au Canada et maladies cardio-pulmonaires dans l'est des États-Unis). JAMA Network Open, 7(12), e2450759. https://doi.org/10.1001/jamanetworkopen.2024.50759

McElroy, J. (2023, 18 juillet). La saison des feux de forêt de 2023 est maintenant la plus destructrice jamais enregistrée en Colombie-Britannique – et nous ne sommes qu'à la mi-juillet. CBC News. https://www.cbc.ca/news/canada/british-columbia/bc-wildfire-july-18-1.6909596

Sa, S. (2025, 15 avril). S'adapter à la fumée : Policymaker responses to wildfire-induced air pollution in Metro Vancouver [Library Archive]. SFU Summit Library ; Simon Fraser University. https://summit.sfu.ca/item/39408

Organisation mondiale de la santé. (2021). Directives mondiales de qualité de l'air de l'OMS : Matières particulaires (PM2.5 et PM10), ozone, dioxyde d'azote, dioxyde de soufre et monoxyde de carbone (1ère édition). Organisation mondiale de la santé. https://iris.who.int/bitstream/handle/10665/345329/9789240034228-eng.pdf

My Inspiration to Join the Industry

Sharon Sa - Emergency management is not just about responding to crisis. It is a forward-looking field rooted in the interconnected pillars of mitigation, preparedness, response, and recovery. It recognizes how climate hazards magnify existing social, ecological, and health vulnerabilities, and calls for policy responses that are not only technically sound but grounded in equity and care.

My interest in this work began during my undergraduate studies, when a nursing course on planetary health introduced me to the ways climate-related hazards directly influence human health. Since then, I have pursued this connection with focus and intention. I completed a Master of Public Policy, during which I spent eight months with the Ministry of Emergency Management and Climate Readiness as a Policy Analyst, supporting legislative research and regulatory development on Disaster Financial Assistance. My capstone, funded by a Canada Graduate Scholarship (SSHRC), examined income-based disparities in wildfire smoke adaptation across British Columbia. I presented my findings at a policy symposium and now work as a research assistant with the Pacific Institute for Climate Solutions under Dr. Nancy Olewiler, contributing to research on wildfire adaptation strategies, community resilience, and culturally grounded approaches to emergency planning in partnership with rural, remote, and Indigenous communities. My goal is to strengthen emergency adaptation policy that meets people where they are. As a former personal care aide, I've seen how extreme weather compounds harm. I carry that urgency forward. Emergency management, to me, is not about control. It is about care, partnership, and building a future worth staying for. Ω

Ce qui m'a poussé à rejoindre l'industrie

Sharon Sa - La gestion des urgences ne consiste pas seulement à réagir à une crise. Il s'agit d'un domaine tourné vers l'avenir, ancré dans les piliers interconnectés de l'atténuation, de la préparation, de la réponse et du rétablissement. Elle reconnaît que les risques climatiques amplifient les vulnérabilités sociales, écologiques et sanitaires existantes, et appelle à des réponses politiques non seulement techniquement solides, mais aussi fondées sur l'équité et l'attention.

Mon intérêt pour ce travail a commencé pendant mes études de premier cycle, lorsqu'un cours d'infirmière sur la santé planétaire m'a fait découvrir les façons dont les risques liés au climat influencent directement la santé humaine. Depuis lors, j'ai poursuivi ce lien de manière ciblée et intentionnelle. J'ai obtenu une maîtrise en politique publique, au cours de laquelle j'ai passé huit mois au ministère de la gestion des urgences et de la préparation au changement climatique en tant qu'analyste des politiques, pour soutenir la recherche législative et l'élaboration de la réglementation sur l'aide financière en cas de catastrophe. Mon mémoire de fin d'études, financé par une bourse d'études supérieures du Canada (CRSH), portait sur les disparités de revenus dans l'adaptation à la fumée des incendies de forêt en Colombie-Britannique. J'ai présenté mes conclusions lors d'un symposium sur les politiques et je travaille maintenant comme assistante de recherche au Pacific Institute for Climate Solutions sous la direction de Nancy Olewiler, contribuant à la recherche sur les stratégies d'adaptation aux incendies de forêt, la résilience des communautés et les approches culturelles de la planification des urgences en partenariat avec les communautés rurales, éloignées et indigènes. Mon objectif est de renforcer les politiques d'adaptation aux situations d'urgence qui répondent aux besoins des personnes là où elles se trouvent. En tant qu'ancienne aide-soignante, j'ai vu comment les conditions météorologiques extrêmes aggravent les dommages. C'est ce sentiment d'urgence qui m'anime. Pour moi, la gestion des urgences n'est pas une question de contrôle. Il s'agit de soins, de partenariats et de la construction d'un avenir pour lequel il vaut la peine de rester. Ω

STUDENT AWARD WINNER
LAURÉAT DU PRIX DE L'ÉTUDIANT

Closing the Gaps: Strengthening the Emergency Management Act for Equitable Disaster Resilience

Combler les lacunes : Renforcer la loi sur la gestion des urgences pour une résilience équitable face aux catastrophes

By Oscar Vicente, PhD

STUDENT AWARD WINNER
LAURÉAT DU PRIX DE L'ÉTUDIANT

In May 2016, as wildfires surged toward Fort McMurray, Alberta, over 80,000 residents were forced to evacuate in just a matter of hours. It was one of the largest evacuations in Canadian history, and it succeeded because governments, private industry, and non-profit organizations all moved in concert. At the heart of this coordination stood the Emergency Management Act (EMA), Canada's legislative framework for disaster preparedness and response.

Yet even as the EMA unites stakeholders during crises, it contains a critical fault line: it does not clearly define federal responsibilities for Indigenous communities. Jurisdictional ambiguity has repeatedly delayed aid, fractured recovery efforts, and undermined trust. In a century marked by rising climate hazards, these gaps are not just bureaucratic — they are a threat to national resilience.

The EMA's Strength: Fostering Coordinated Action

The EMA's primary strength lies in promoting multi-level, cross-sectoral cooperation. It mandates collaboration among federal, provincial, territorial, and

En mai 2016, alors que les feux de forêt progressaient vers Fort McMurray, en Alberta, plus de 80 000 habitants ont été contraints d'évacuer en quelques heures seulement. Cette évacuation, l'une des plus importantes de l'histoire du Canada, a réussi parce que les gouvernements, le secteur privé et les organisations à but non lucratif ont agi de concert. Au cœur de cette coordination se trouvait la loi sur la gestion des urgences (EMA), le cadre législatif canadien pour la préparation et l'intervention en cas de catastrophe.

Pourtant, même si la loi sur la gestion des urgences unit les parties prenantes en cas de crise, elle comporte une faille essentielle : elle ne définit pas clairement les responsabilités fédérales à l'égard des communautés autochtones. L'ambiguïté juridictionnelle a à maintes reprises retardé l'aide, brisé les efforts de rétablissement et miné la confiance. En ce siècle marqué par l'augmentation des risques climatiques, ces lacunes ne sont pas seulement bureaucratiques : elles menacent la résilience nationale.

La force de l'EMA : Favoriser une action coordonnée

La principale force de l'EMA réside dans la promotion d'une coopération multi-niveaux et intersectorielle. Elle prévoit une collaboration entre

Indigenous governments, along with private and non-profit partners, to share resources, expertise, and decision-making (Etkin et al., 2011).

In a country spanning six time zones with hazards ranging from Atlantic storms to Arctic ice melt, this networked approach is essential. The 2016 Fort McMurray wildfire demonstrated the EMA's effectiveness. Within hours, evacuation routes were secured, emergency shelters were set up, federal firefighting resources reinforced provincial crews, and NGOs provided food, water, and counselling (Raikes & McBean, 2016).

Proactive planning is equally crucial. Hazard assessments, stakeholder mapping, and pre-established communication channels allow communities to respond quickly when disaster strikes. Such planning, paired with shared accountability, shortens recovery timelines and reduces vulnerabilities (Botha, 2022).

The Weak Link: Ambiguity for Indigenous Communities

Beneath these successes lies a persistent challenge: the EMA does not clearly define federal responsibilities for First Nations, Inuit, and Métis communities. The result is jurisdictional limbo, where aid is delayed while governments negotiate who should respond.

The 2017 British Columbia wildfire season exposed this problem. Conflicting mandates between federal and provincial authorities delayed evacuation support and access to relief for several First Nations communities (McDougall, 2020). In remote areas, where infrastructure is limited, delayed responses can exacerbate risks to life, property, and long-term recovery.

Research consistently shows that this ambiguity disproportionately harms Indigenous communities, particularly those in isolated regions (Collier, 2015;

les gouvernements fédéral, provinciaux, territoriaux et autochtones, ainsi qu'avec des partenaires privés et à but non lucratif, afin de partager les ressources, l'expertise et la prise de décision (Etkin et al., 2011).

Dans un pays qui s'étend sur six fuseaux horaires et où les risques vont des tempêtes de l'Atlantique à la fonte des glaces de l'Arctique, cette approche en réseau est essentielle. L'incendie de forêt de Fort McMurray en 2016 a démontré l'efficacité de l'EMA. En quelques heures, les voies d'évacuation ont été sécurisées, des abris d'urgence ont été mis en place, les ressources fédérales de lutte contre les incendies ont renforcé les équipes provinciales et les ONG ont fourni de la nourriture, de l'eau et des conseils (Raikes & McBean, 2016).

La planification proactive est tout aussi cruciale. L'évaluation des risques, la cartographie des parties prenantes et les canaux de communication préétablis permettent aux communautés de réagir rapidement en cas de catastrophe. Une telle planification, associée à une responsabilité partagée, raccourcit les délais de rétablissement et réduit les vulnérabilités (Botha, 2022).

Le maillon faible : Ambiguïté pour les communautés autochtones

Derrière ces succès se cache un problème persistant : l'EMA ne définit pas clairement les responsabilités fédérales à l'égard des communautés des Premières nations, des Inuits et des Métis. Il en résulte un flou juridictionnel, où l'aide est retardée pendant que les gouvernements négocient pour savoir qui doit intervenir.

La saison des feux de forêt de 2017 en Colombie-Britannique a mis ce problème en évidence. Des mandats contradictoires entre les autorités fédérales et provinciales ont retardé l'aide à l'évacuation et l'accès aux secours pour plusieurs communautés des Premières nations (McDougall, 2020). Dans les zones reculées, où les infrastructures sont limitées, les réponses tardives peuvent exacerber les risques pour la vie, les biens et le rétablissement à long terme.

Les recherches montrent systématiquement que cette ambiguïté nuit de manière disproportionnée aux communautés autochtones, en particulier à

Kravitz et al., 2013). Delays in evacuations, inadequate shelters, and slower recovery are symptoms of a system that has yet to fully recognize Indigenous self-determination in emergency planning.

Why This Matters: Beyond Government Operations

The consequences of jurisdictional gaps extend beyond emergency management. Delayed responses disrupt local economies, fracture supply chains, and prolong business interruptions. From a national security perspective, resilience is only as strong as its weakest link. Underserved communities compromise the country's overall recovery capacity.

For emergency management professionals, this is a shared responsibility. Inclusive preparedness strengthens the entire system, ensuring that no community is left behind when disasters strike.

A Path Forward: Embedding an Indigenous Emergency Management Framework

Closing this gap requires more than minor adjustments — it demands an Indigenous-focused framework embedded within the EMA. Such a framework should define a clear federal mandate without replacing provincial systems. Key elements could include:

1. **Defined Federal Roles** – Explicit responsibilities for emergency management in First Nations, Inuit, and Métis communities to remove ambiguity during crises.
2. **Sustained Funding** – Dedicated streams for Indigenous-led preparedness, mitigation, and recovery initiatives to ensure stable capacity.
3. **Indigenous-Led Response Units** – Community-based teams trained, equipped, and authorized to collaborate with other jurisdictions during emergencies.

celles qui vivent dans des régions isolées (Collier, 2015 ; Kravitz et al., 2013). Les retards dans les évacuations, les abris inadéquats et le ralentissement du rétablissement sont les symptômes d'un système qui n'a pas encore pleinement reconnu l'autodétermination autochtone dans la planification des situations d'urgence.

Pourquoi c'est important :Au-delà des opérations gouvernementales

Les conséquences des lacunes juridictionnelles vont au-delà de la gestion des urgences. Les retards de réponse perturbent les économies locales, rompent les chaînes d'approvisionnement et prolongent les interruptions d'activité. Du point de vue de la sécurité nationale, la résilience est aussi forte que son maillon le plus faible. Les communautés mal desservies compromettent la capacité de rétablissement globale du pays.

Pour les professionnels de la gestion des urgences, il s'agit d'une responsabilité partagée. Une préparation inclusive renforce l'ensemble du système, en veillant à ce qu'aucune communauté ne soit laissée pour compte en cas de catastrophe.

Une voie à suivre : Intégrer un cadre autochtone de gestion des urgences

Pour combler cette lacune, il faut plus que des ajustements mineurs – il faut un cadre axé sur les Autochtones, intégré à l'EMA. Ce cadre devrait définir un mandat fédéral clair sans remplacer les systèmes provinciaux. Les éléments clés pourraient être les suivants

1. **Rôles fédéraux définis** – Responsabilités explicites en matière de gestion des urgences dans les communautés des Premières nations, des Inuits et des Métis afin d'éliminer toute ambiguïté en cas de crise.
2. **Un financement durable** – Des flux dédiés aux initiatives de préparation, d'atténuation et de rétablissement menées par les autochtones afin de garantir la stabilité des capacités.
3. **Unités d'intervention dirigées par des autochtones** – Équipes communautaires formées, équipées et autorisées à collaborer avec d'autres juridictions en cas d'urgence.
4. **Accords intergouvernementaux contraignants** – Protocoles entre les

4. **Binding Intergovernmental Agreements** – Protocols between federal, provincial, territorial, and Indigenous governments to guarantee rapid, coordinated action.
5. **Cultural Integration** – Recognition of Indigenous knowledge, from traditional fire stewardship to flood forecasting, as integral to hazard mitigation.

This approach aligns with Canada's reconciliation commitments and reflects global best practices, where community-driven resilience has consistently proven effective (May & Burby, 1996).

Why This Matters: Beyond Government Operations

The consequences of jurisdictional gaps extend beyond emergency management. Delayed responses disrupt local economies, fracture supply chains, and prolong business interruptions. From a national security perspective, resilience is only as strong as its weakest link. Underserved communities compromise the country's overall recovery capacity.

For emergency management professionals, this is a shared responsibility. Inclusive preparedness strengthens the entire system, ensuring that no community is left behind when disasters strike.

The Role of Professionals

Emergency management and business continuity professionals play a pivotal role in bridging policy and practice. They can:

- Build trust with Indigenous communities through pre-disaster engagement.
- Integrate equity considerations into risk assessments and continuity plans.
- Advocate for policy reforms that clarify roles and empower local leadership.
- Promote training that incorporates Indigenous perspectives and cultural protocols.

gouvernements fédéral, provinciaux, territoriaux et autochtones pour garantir une action rapide et coordonnée.

5. **Intégration culturelle** – Reconnaissance du savoir autochtone, de la gestion traditionnelle des incendies à la prévision des inondations, comme faisant partie intégrante de l'atténuation des risques.

Cette approche est conforme aux engagements du Canada en matière de réconciliation et reflète les meilleures pratiques mondiales, où la résilience communautaire s'est avérée efficace (May & Burby, 1996).

Pourquoi cela est important :Au-delà des opérations gouvernementales

Les conséquences des lacunes juridictionnelles vont au-delà de la gestion des urgences. Les réponses tardives perturbent les économies locales, brisent les chaînes d'approvisionnement et prolongent les interruptions d'activité. Du point de vue de la sécurité nationale, la résilience est aussi forte que son maillon le plus faible. Les communautés mal desservies compromettent la capacité de rétablissement globale du pays.

Pour les professionnels de la gestion des urgences, il s'agit d'une responsabilité partagée. Une préparation inclusive renforce l'ensemble du système, en veillant à ce qu'aucune communauté ne soit laissée pour compte en cas de catastrophe.

Le rôle des professionnels

Les professionnels de la gestion des situations d'urgence et de la continuité des activités jouent un rôle essentiel en faisant le lien entre la politique et la pratique. Ils peuvent

- Instaurer un climat de confiance avec les communautés autochtones en s'engageant avant la catastrophe.
- Intégrer des considérations d'équité dans l'évaluation des risques et les plans de continuité.
- Plaider en faveur de réformes politiques qui clarifient les rôles et renforcent le leadership local.
- Promouvoir une formation qui intègre les perspectives indigènes et les protocoles culturels.

Professional excellence is not only operational — it ensures that all communities receive timely, culturally informed support when disaster strikes.

Conclusion: Clarity, Cooperation, Inclusion

The EMA has proven its value in coordinating Canada's responses to complex disasters. Yet its silence on federal responsibilities for Indigenous emergency management remains a critical weakness.

By embedding an Indigenous-focused framework into the EMA, Canada can turn this weakness into a strength. Clarity, cooperation, and inclusion would become the foundation of national resilience. In a future defined by a Clarity, Cooperation, Inclusion ccelerating hazards, this foundation could mean the difference between fractured responses and unified recovery. Ω

L'excellence professionnelle n'est pas seulement opérationnelle – elle garantit que toutes les communautés reçoivent un soutien opportun et culturellement informé en cas de catastrophe.

Conclusion : Clarté, coopération, inclusion

L'EMA a prouvé sa valeur en coordonnant les réponses du Canada aux catastrophes complexes. Cependant, son silence sur les responsabilités fédérales en matière de gestion des urgences autochtones reste une faiblesse majeure.

En intégrant à l'EMA un cadre axé sur les populations autochtones, le Canada peut transformer cette faiblesse en force. La clarté, la coopération et l'inclusion deviendraient les fondements de la résilience nationale. Dans un avenir marqué par l'accélération des risques, ces fondements pourraient faire la différence entre des réponses fragmentées et un rétablissement unifié. Ω

References

Botha, J. (2022). Boots on the ground: Disaster response in Canada. University of Toronto Press.

Collier, B. (2015). Emergency management on First Nations reserves. Library of Parliament.

Etkin, D., McBey, K., & Trollope, C. (2011). The military and disaster management: A Canadian perspective on the issue. Academia.edu.

Kravitz, M., Gastaldo, V., Lackenbauer, P.W., & Nicol, H. (2013). Emergency management in the Arctic: The context explained. In Whole of government through an Arctic lens (pp. 269–294).

May, P. J., & Burby, R. J. (1996). Coercive versus cooperative policies: Comparing intergovernmental mandate performance. Journal of Policy Analysis and Management, 15(2), 171–201.

McDougall, A. (2020). Continuity of constitutional government during a pandemic: Considering the concept in Canada's Emergency Management Act. Canadian Journal of Political Science, 53(2), 293–298.

Raikes, J., & McBean, G. (2016). Responsibility and liability in emergency management to natural disasters: A Canadian example. International Journal of Disaster Risk Reduction, 16, 12–18.

Références

Botha, J. (2022). Les bottes sur le terrain : Disaster response in Canada. University of Toronto Press.

Collier, B. (2015). La gestion des urgences dans les réserves des Premières nations. Bibliothèque du Parlement.

Etkin, D., McBey, K. et Trollope, C. (2011). Les militaires et la gestion des catastrophes : Une perspective canadienne sur la question. Academia.edu.

Kravitz, M., Gastaldo, V., Lackenbauer, P.W., & Nicol, H. (2013). Emergency management in the Arctic : The context explained (La gestion des urgences dans l'Arctique : le contexte expliqué). In Whole of government through an Arctic lens (pp. 269-294).

May, P. J., & Burby, R. J. (1996). Coercive versus cooperative policies : Comparing intergovernmental mandate performance. Journal of Policy Analysis and Management, 15(2), 171-201.

McDougall, A. (2020). Continuité du gouvernement constitutionnel pendant une pandémie : Le concept dans la Loi sur la gestion des urgences du Canada. Revue canadienne de science politique, 53(2), 293-298.

Raikes, J. et McBean, G. (2016). Responsibility and liability in emergency management to natural disasters : Un exemple canadien. International Journal of Disaster Risk Reduction, 16, 12-18.

My Inspiration to Join the Industry

Oscar Vincente - My passion for emergency management is grounded in a lifelong commitment to public service, community safety, and evidence-based leadership. In my role with the Canada Border Services Agency, and through graduate studies in disaster and emergency management, I have gained a strong understanding of how effective planning, coordination, and communication reduce risk and strengthen resilience.

My career goal is to serve in a senior federal advisory role, supporting risk-informed decision-making, continuity of operations, and inclusive crisis communication. I am driven by the opportunity to help build systems that protect people, minimize disruption, and support recovery – especially in an era of growing complexity and uncertainty. Outside of work and academics, I actively contribute to the profession. I volunteer as an instructor with Emergency Management Ontario, helping deliver public education and preparedness initiatives. I also serve on the Editorial Board of the Canadian Journal of Emergency Management, where I support knowledge-sharing across the sector. My dedication to public service has been recognized with the Peace Officer Exemplary Service Medal, and the King Charles III Coronation Medal – honours that reflect my deep commitment to serving Canadians with integrity and professionalism. Emergency management is more than a career path for me – it's a calling. I am inspired by the field's broader purpose: protecting lives, supporting vulnerable communities, and enabling recovery with dignity. I am proud to contribute to a profession that helps people prepare for the unexpected and recover with strength. Ω

Ce qui m'a poussé à rejoindre l'industrie

Oscar Vincente - Ma passion pour la gestion des urgences repose sur un engagement de toute une vie en faveur du service public, de la sécurité des communautés et d'un leadership fondé sur des données probantes. Dans le cadre de mes fonctions à l'Agence des services frontaliers du Canada et de mes études supérieures en gestion des catastrophes et des urgences, j'ai acquis une solide compréhension de la manière dont une planification, une coordination et une communication efficaces réduisent les risques et renforcent la résilience.

Mon objectif de carrière est d'occuper un poste de conseiller fédéral de haut niveau, en soutenant la prise de décision fondée sur les risques, la continuité des opérations et la communication de crise inclusive. Je suis motivée par la possibilité de contribuer à la mise en place de systèmes qui protègent les personnes, minimisent les perturbations et favorisent le rétablissement, en particulier à une époque où la complexité et l'incertitude ne cessent de croître. En dehors de mon travail et de mes études, je contribue activement à la profession. Je suis instructeur bénévole auprès de Gestion des situations d'urgence Ontario, où j'aide à mettre en œuvre des initiatives d'éducation et de préparation du public. Je fais également partie du comité de rédaction de la Revue canadienne de gestion des situations d'urgence, où je contribue au partage des connaissances dans l'ensemble du secteur. Mon dévouement au service public a été reconnu par la Médaille pour services distingués des agents de la paix et la Médaille du couronnement du roi Charles III - des distinctions qui reflètent mon profond engagement à servir les Canadiens avec intégrité et professionnalisme. Pour moi, la gestion des urgences est plus qu'un plan de carrière, c'est une vocation. Je suis inspirée par l'objectif plus large de ce domaine : protéger des vies, soutenir les communautés vulnérables et permettre un rétablissement dans la dignité. Je suis fière de contribuer à une profession qui aide les gens à se préparer à l'inattendu et à se relever avec force. Ω

STUDENT AWARD WINNER
LAURÉAT DU PRIX DE L'ÉTUDIANT

TRUE NORTH
RESILIENCE
Résilience du vrai nord
DRI Canada's magazine / Magazine de DRI Canada

Call for Articles

Submissions are welcome where they share best practices, experiences, and opinions that are fact-based, non-partisan, and have been generated without the use of Artificial Intelligence tools. We do not accept articles that promote specific businesses, or products, unless it's intrinsic to the narrative of the article. We are pleased to use this publication to share ideas that will serve professional development and thought leadership through continual improvement in Resilience.

Please make all editorial submissions to editors@dri.ca.

Submission Guidelines

Suggested topics:
- Resilience, Cyber Security, Data Protection, Privacy, Business Continuity, Disaster Recovery, Crisis Management, Emergency Management, OH&S, Risk Management

Word count:
- Preferably 500-2,000 words (maximum 2,500)

Vendor-neutral:
- No mention of any for profit organization product, or service will be published in the magazine (except for paid advertisements).

Copyright:
- Every magazine article published will be copyrighted by DRI Canada.
- Authors are required to sign a copyright agreement.
- Articles must be original and may not be simultaneously submitted to other publications.
- DRI Canada will retain all publishing rights. However, permission will be granted for marketing purposes or any other non-competing publication with attribution.

Required materials: All article submissions must include a short biography and a headshot photo of the author.

Art: Photographs or graphic elements may accompany each article. Graphic submissions are welcome but please refrain from designing your article submission.
- Please submit text and graphic elements separately.
- Photos and graphics must be high resolution (300 dpi at 100% print size) or vector based.

Authors: Articles from DRI Certified Professionals are given preference. Not applicable to student submissions.

Editing: Articles will be edited for length, clarity, style, and improper usage of industry terms. Ω

Appel à articles

Les soumissions sont les bienvenues lorsqu'elles partagent des bonnes pratiques, des expériences et des opinions fondées sur des faits, non partisanes et générées sans l'utilisation d'outils d'intelligence artificielle. Nous n'acceptons pas les articles qui font la promotion d'entreprises ou de produits spécifiques, à moins que cela ne soit intrinsèque à la narration de l'article. Nous sommes heureux d'utiliser cette publication pour partager des idées qui serviront au développement professionnel et au leadership éclairé par l'amélioration continue de la résilience.

Veuillez adresser vos propositions éditoriales à editors@dri.ca.

Lignes directrices pour les soumissions

Sujets proposés :
- Résilience, cybersécurité, protection des données, Protection de la vie privée, Continuité des activités, Reprise après sinistre, Gestion de crise, Gestion des urgences, Santé et sécurité au travail, Gestion des risques

Nombre de mots :
- De préférence entre 500 et 2 000 mots (maximum 2 500)

Neutralité vis-à-vis des fournisseurs :
- Aucune mention d'un produit ou d'un service d'une organisation à but lucratif ne sera publiée dans le magazine (à l'exception des publicités payantes).

Droits d'auteur :
- Chaque article publié dans le magazine sera protégé par les droits d'auteur de DRI Canada.
- Les auteurs sont tenus de signer un accord sur les droits d'auteur.
- Les articles doivent être originaux et ne peuvent être soumis simultanément à d'autres publications.
- DRI Canada conservera tous les droits de publication. Cependant, une permission sera accordée à des fins de marketing ou pour toute autre publication non concurrente, avec mention de la source.

Matériel requis : Toutes les soumissions d'articles doivent inclure une courte biographie et une photo de l'auteur.

Art : Des photographies ou des éléments graphiques peuvent accompagner chaque article. Les propositions graphiques sont les bienvenues, mais nous vous demandons de ne pas concevoir votre article.
- Veuillez soumettre le texte et les éléments graphiques séparément
- Les photos et les graphiques doivent être en haute résolution (300 dpi à 100 % de la taille d'impression) ou vectoriels.

Auteurs : Les articles rédigés par des professionnels certifiés par DRI sont privilégiés. Cette règle ne s'applique pas aux articles soumis par des étudiants.

Révision : Les articles seront édités pour des raisons de longueur, de clarté, de style et d'utilisation incorrecte des termes de l'industrie. Ω

2025 Awards of Excellence
~ prix d'excellence ~

AND THE WINNERS ARE | ET LES GAGNANTS SONT

CITY OF ST ALBERT

MARK PICKFORD | Preparedness & Mitigation
Préparation et attenuation

MUNICIPALITY OF JASPER

LOCAL STAFF | Response & Recovery
Résponse et rétablissement

BENOIT RACETTE | Contributor
Contributeur

STUDENT AWARD WINNERS
LAURÉATS DU PRIX ÉTUDIANT

OSCAR VINCENTE | Royal Roads University

SUSAN SA | Simon Fraser University

VINCENT BODNAR | Lifetime Achievement
Accomplissement d'une vie

DRI CANADA
Train.
Prepare.
Recover.
dri.ca

25 YEARS

DRI CANADA

Train. Prepare. Recover.

ISSN 2816-900X

Return to TOC

Retour au sommaire