

**In this Issue:**

- **NETWORK ENDGAME**  
and more...

**Dans ce numéro :**

- **FIN DE PARTIE DU RÉSEAU**  
et plus encore...



CERTIFYING PROFESSIONALS IN CANADA FOR 25 YEARS



## **Certifying Business Continuity Professionals in Canada for 25 Years**

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. These professionals empower Canadian organizations, communities and businesses to be resilient and better prepared for any emergency or disaster.

Established 25 years ago, DRI Canada has grown from a small number of certified professionals to more than 1500 across Canada. Over the next six months we will be celebrating this milestone through a variety of initiatives.

## **Certification des professionnels de la continuité des activités au Canada pour 25 ans**

DRI Canada est un organisme sans but lucratif qui offre une formation et une certification reconnues à l'échelle internationale aux professionnels de la continuité des activités, de la reprise après sinistre et de la gestion des urgences au Canada. Ces professionnels permettent aux organisations, aux collectivités et aux entreprises canadiennes d'être résilientes et mieux préparées à toute urgence ou catastrophe.

Fondée il y a 25 ans, DRI Canada est passée d'un petit nombre de professionnels certifiés à plus de 1500 à travers le Canada. Au cours des six prochains mois, nous célébrerons cette étape importante au moyen de diverses initiatives.

# Contents | Le Sommaire

**President's Message**..... 5  
**Message du président**  
*Nancy Holloway-White, CBCP, CBCA*

**Editors' Desk**..... 7  
**Bureau des redacteurs**  
*Garth Tucker, CBCP, CORP*

**An Expert's Impression**..... 10  
**L'impression d'un expert**  
*Alexandra Hoffmann, Jason Firlotte, Kevin Powers, Emad Aziz, and Cynthia Wenn*

## **FEATURE ARTICLE • ARTICLE VEDETTE**

**Network & Endpoint Security  
Challenges – the lack of endgame**..... 17  
**Défis en matière de sécurité des  
réseaux et des points finaux - l'absence  
de finalité**  
*Randy Bucking*

## **DEPARTMENT: PROFESSIONAL PRACTICES • DES PRATIQUES PROFESSIONNELLES**

**From Confusion to Clarity: Four Tips  
to Building a Better Plan**..... 24  
**De la confusion à la clarté : quatre  
conseils pour bâtir un meilleur plan**  
*Jason Firlotte, MBCP, CBRM, MBCI, CSP,  
CBCV*

**Crises Communications**..... 28  
**Communications de crise**  
*Mark Hoffman, CBCP, MBCI*

**The Vitality of Emergency Preparedness  
and Business Continuity Management  
in Healthcare Sectors**..... 36

**La vitalité de la préparation aux  
situations d'urgence et de la gestion  
de la continuité des activités dans les  
secteurs de la santé**  
*Nix George, ABCP*

**Comprehensive Risk Assessment- A  
Dual Approach for Organizational  
Resilience**..... 42

**Évaluation globale des risques - Une  
double approche pour la résilience  
organisationnelle**  
*Ray Unrau*

**Interim Report on Resilience and  
Preparedness – Canadian Journal  
of Emergency Management MINDS  
Initiative**..... 48

**Rapport Intermédiaire sur la Résilience  
et la Préparation – Initiative MINDS de  
la Revue canadienne de la Gestion des  
Urgences**  
*Sara Kallas*

**The Role of the OHS Professional in  
Business Continuity**..... 59

**Le rôle du professionnel de la santé  
dans la continuité des activités**  
*V J McNeilly, MRSC, CFIOSH*

**Implications of a Cyber Breach**..... 62

**Répercussions d'une cyberattaque**  
*Garth Tucker, CBCP, CORP*

<b>Advertisers' Index</b>		<b>Index des annonceurs</b>
<b>Sponsor</b>	<b>Website</b>	<b>Page</b>
Benoit Racette Services-conseils inc	<a href="http://racetteconseils.com">racetteconseils.com</a>	18
Continuity & Resilience Today	<a href="http://CRTDEMCON.ca">CRTDEMCON.ca</a>	21
DRIC Upcoming Symposiums	<a href="http://DRIC.ca">DRIC.ca</a>	71
Mid-Range Computer Group Inc	<a href="http://mid-range.ca">mid-range.ca</a>	9
Vanguard EMC Inc.	<a href="http://vanguardemergency.com">vanguardemergency.com</a>	12

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](mailto:editors@dri.ca)  
Toll Free: 1-844-228-8135  
Local: 416-646-2750

©2024 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.

©2024 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](mailto: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](mailto:editors@dri.ca), ou par courrier ordinaire à : DRIC, 701 Rossland Road East, Suite 375, Whitby, ON, L1N 8Y9.



**Printed in Canada**

# TRUE NORTH RESILIENCE RÉSILIENCE DU VRAI NORD

DRI Canada's magazine / Magazine de DRI 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

**Brock Holowachuk**, CBCP  
Treasurer & Director Central Region

**Brenda Escribano**, CBCP  
Secretary & Privacy Officer

**Steve Palubiski**, MBCP  
Certification Commission Chair

**Rejean Pesant**, CBCP  
Education Commission Chair

**Troy McQuinn**, CEM, ABCP  
Director Atlantic Region

**Patrick Leduc**, CBCP  
Director Quebec Region

**Jason Firlotte**, MBCP, CBRM, MBCI, CSP, CBCV  
Director Ontario Region

**Jeff Hortobagyi**, CBCP  
Director Pacific Region

**Andrea Buchholz**, CBCLA  
Director at Large

**Alexander Landry**, CBCP  
Director at Large

**Scott Leavitt**, CBCP  
Director at Large

**Jeremy Paulis**, CBCP  
Director at Large

**Greg Solecki**, CBCP  
Director at Large

## 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 Canada, in Canada and other countries.



Graphic Design  
Eclipse Technologies Inc.  
416-219-8790  
[e-clipse.ca](http://e-clipse.ca)



Printing, Binding, Lettershop  
Canmark Communicatrions  
416.553.8228  
[canmarkcommunications.com](http://canmarkcommunications.com)



# President's Message Message du président

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



**I hope everyone had a fun and enjoyable summer!**

**W**hile it was quite hot, we found ways to adapt and enjoy the sunshine. We had some chats about maybe needing to adopt different ways of managing summer days; early morning and early evening outings and save the heat of the afternoon for indoor activities, or near water activities. This seems almost second nature to a Business Continuity Professional – adaptation is what we are all about.

However, it's not intuitive to adapt to all things, and what one person can adapt to easily may be more challenging for another (and vice versa). A Business Continuity Professional is consistently challenged by the need to adapt; to their various clients (whether internal or external), business partners, situations, knowledge of processes, and so on. It's impossible for a Business Continuity Professional to know all processes in an organization and inflows and outflows of the organization (this is why BIAs are one of the essential Professional Practices).

**How is a Business Continuity Professional to adapt to all things?**

How can a Business Continuity Professional guide, advise, and consult on building business continuity plans for a process which is new to them? Of course, the plan-building formula is that a Business Continuity Professional provides the business continuity know-how, and the process subject matter expert (SME) brings the process knowledge. Each person shares their expertise to produce the outcome. However, as any experienced

**J'espère que tout le monde a passé un été agréable et plaisant.**

**B**ien qu'il ait fait assez chaud, nous avons trouvé des moyens de nous adapter et de profiter du soleil. Nous avons discuté de la nécessité d'adopter différentes façons de gérer les journées d'été : sorties tôt le matin et en début de soirée, et garder la chaleur de l'après-midi pour des activités à l'intérieur ou près de l'eau. Pour un professionnel de la continuité des activités, cela semble être une seconde nature - l'adaptation est notre raison d'être.

Cependant, il n'est pas intuitif de s'adapter à tout, et ce à quoi une personne peut s'adapter facilement peut s'avérer plus difficile pour une autre (et vice versa). Un professionnel de la continuité des activités est constamment confronté à la nécessité de s'adapter à ses différents clients (internes ou externes), partenaires commerciaux, situations, connaissances des processus, etc. Il est impossible pour un professionnel de la continuité des activités de connaître tous les processus d'une organisation ainsi que les flux entrants et sortants de l'organisation (c'est pourquoi les BIA sont l'une des pratiques professionnelles essentielles).

Comment un professionnel de la continuité des activités peut-il s'adapter à tout ? Comment un professionnel de la continuité des activités peut-il guider, conseiller et assister à l'élaboration de plans de continuité des activités dans le cadre d'un processus nouveau pour lui ? Bien sûr, la formule de construction d'un plan est la suivante : un professionnel de la continuité des activités apporte son savoir-faire en matière de continuité des activités et l'expert en la matière apporte sa connaissance du processus. Chaque personne partage son expertise pour

Business Continuity Professional knows, sometimes, building a solid Business Continuity Plan takes several rounds, and sometimes requires the Business Continuity Professional to have some knowledge of the process to get the SME over the finish line for a truly good Plan. This is where a Certified Business Continuity Professional is a good choice. A Certified Business Continuity Professional requires continuing education points to maintain their certification. The best Certified Business Continuity Professionals also strive to go beyond that; they learn about processes around them, what is going on in the workplace, business-world/NGO world, understand organizational cultural context, HR practices, security practices, the organization's stance on risk management, and so on. Understanding context around each of us (i.e., not just within our own cultural context) also helps us understand the greater world; it helps us have a better appreciation of the perspectives of those that we interact with and just as importantly, don't interact with. To build good processes, we need to be inclusive of all those internal and external that will use the processes.

With the continuous-learning-journey in mind, I hope that this edition of the True North Resilience brings you new information, new perspectives and contributes to your constant learning journey.

From here at DRI Canada, wishing all the aspiring and current Certified Business Continuity Professionals out there the very best as they strive to make Canada a more resilient nation.

Best,

Nancy Holloway-White, CBCP, CBCA

President, DRI Canada



produire le résultat. Cependant, comme le sait tout professionnel expérimenté en continuité d'activité, l'élaboration d'un plan de continuité d'activité solide prend parfois plusieurs tours et nécessite parfois que le professionnel en continuité d'activité ait une certaine connaissance du processus pour amener l'expert en processus à franchir la ligne d'arrivée afin d'obtenir un plan vraiment satisfaisant. C'est là qu'un professionnel certifié de la continuité des activités est un bon choix. Un professionnel certifié en continuité d'activité doit obtenir des points de formation continue pour conserver sa certification. Les meilleurs professionnels certifiés en continuité des activités s'efforcent d'aller plus loin ; ils s'informent sur les processus qui les entourent, sur ce qui se passe sur le lieu de travail, dans le monde des affaires ou des ONG, ils comprennent le contexte culturel de l'organisation, les pratiques en matière de ressources humaines, les pratiques en matière de sécurité, la position de l'organisation sur la gestion des risques, etc. Comprendre le contexte autour de chacun d'entre nous (c'est-à-dire pas seulement dans notre propre contexte culturel) nous aide également à comprendre le monde dans son ensemble ; cela nous aide à mieux apprécier les perspectives de ceux avec qui nous interagissons et, ce qui est tout aussi important, avec qui nous n'interagissons pas. Pour élaborer de bons processus, nous devons inclure toutes les personnes, internes et externes, qui les utiliseront.

En gardant à l'esprit la notion d'apprentissage continu, j'espère que cette édition du True North Resilience vous apportera de nouvelles informations, de nouvelles perspectives et qu'elle contribuera à votre parcours d'apprentissage continu.


DRI Canada souhaite à tous les professionnels certifiés en continuité des affaires, actuels et futurs, le meilleur des succès dans leurs efforts pour faire du Canada une nation plus résiliente.

Meilleures salutations,

Nancy Holloway-White, CBCP, CBCA

Présidente, DRI Canada





# Editors' Desk Bureau des rédacteurs

By/Par *Garth Tucker, CBCP, CORP*

**T**hank you to all readers for your support and encouragement to continue spreading resilience knowledge to DRI Canada Certified Professionals everywhere, it's a labour of love for all of us involved and it means a lot to hear people say how much they enjoy getting the magazine in the spring and fall.

In this issue we have a new feature, “**An Expert's Impression**” which poses a question about a recent event that affects practitioners to industry experts in various fields and we can discuss the answers on the DRI Canada website.

**Nix George** will give us an inside view, based on his extensive experience, of BC in Healthcare in an article that opens up some interesting aspects of business continuity that few of us in the profession ever get to analyze.

Our regular look into the Professional Practices continues with articles from **Mark Hoffman** discussing Professional Practice #9 Crisis Communications, and **Jason Firlotte**, sharing some of his expertise on how to build better plans in a very insightful article.

**M**erci à tous les lecteurs pour leur soutien et leur encouragement à continuer de diffuser les connaissances sur la résilience aux professionnels certifiés de DRI Canada partout dans le monde. C'est un travail d'amour pour nous tous et cela signifie beaucoup d'entendre les gens dire à quel point ils apprécient de recevoir le magazine au printemps et à l'automne.

Dans ce numéro, nous avons une nouvelle rubrique, “**L'impression d'un expert**”, qui pose une question sur un événement récent affectant les praticiens à des experts de l'industrie dans divers domaines, et nous pouvons discuter des réponses sur le site web de DRI Canada.

**Nix George** nous donne un aperçu, basé sur sa vaste expérience, de la Colombie-Britannique dans le secteur des soins de santé dans un article qui aborde certains aspects intéressants de la continuité des activités que peu d'entre nous dans la profession ont l'occasion d'analyser.

Notre examen régulier des pratiques professionnelles se poursuit avec des articles de **Mark Hoffman** sur la pratique professionnelle n° 9 - Communication de crise, et de **Jason Firlotte**, qui partage son expertise sur la manière d'élaborer de meilleurs plans dans un article très perspicace.

While the technical side of cybersecurity is performed by IT professionals with specialized training and experience, it falls to us as professional resilience planners to integrate the response and crisis management of these events into our programs, so we'll look at the cyber with an article from a leading network security expert, **Randy Bucking**, and some of the impacts of a cyber event in an article by one of our editors, **Garth Tucker**.

Our first Occupational Health and Safety (OHS) article appears in this issue, from V J McNeilly MRSC. CFIOSH to further help us break down the barriers between practice areas. Looking forward to more from that practice area in time.

And, last, but certainly not least, **Ray Unrau** – a recognized leader in Emergency Management and good friend to many of us at DRI Canada – will discuss Risk with the All-Hazards approach favoured by EM vs Operational Risk and how he integrated them in the Province of Saskatchewan.

As always, thanks to the authors who take the time to craft insightful, well written articles that are the backbone of this magazine and if you have an article or an idea for an article, but aren't sure where to begin, please reach out to us at [editors@dri.ca](mailto:editors@dri.ca) and we'll help guide you to a successful end, and you would like to see your views and experience on these pages, please submit it and we'll make you famous-ish. Ω

Thanks!

The DRIC True North Resilience Editors

- Ron Andrews
- Alexander Landry
- Charlie Shymko
- Brady Podloski
- Garth Tucker
- Steve Palubiski



Alors que l'aspect technique de la cybersécurité est assuré par des professionnels de l'informatique ayant une formation et une expérience spécialisées, il nous incombe, en tant que planificateurs de la résilience professionnelle, d'intégrer la réponse et la gestion de crise de ces événements dans nos programmes. Nous examinerons donc le cyber avec un article d'un expert en sécurité des réseaux, **Randy Bucking**, et certains des impacts d'un cyber-événement dans un article de l'un de nos rédacteurs en chef, **Garth Tucker**.

Notre premier article sur la santé et la sécurité au travail (SST) paraît dans ce numéro, tiré de V J McNeilly MRSC. La SSSTPC pour nous aider davantage à éliminer les obstacles entre les domaines de pratique. Nous attendons avec impatience d'autres de ce domaine de pratique dans le temps.

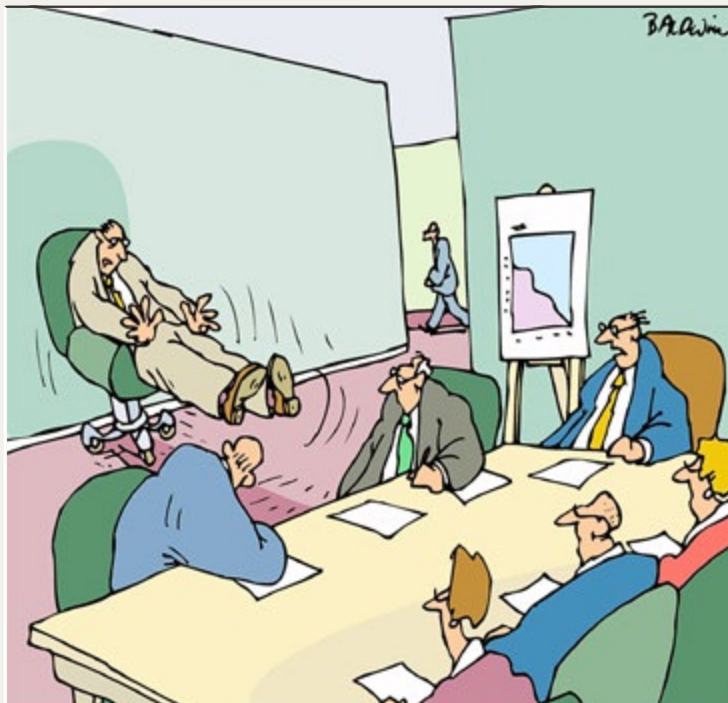
Enfin, **Ray Unrau** - un chef de file reconnu dans le domaine de la gestion des urgences et un bon ami pour bon nombre d'entre nous à DRI Canada - discutera du risque avec l'approche tous risques privilégiée par la gestion des urgences par rapport au risque opérationnel et de la façon dont il les a intégrés dans la province de la Saskatchewan.

Comme toujours, nous remercions les auteurs qui prennent le temps de rédiger des articles pertinents et bien écrits qui constituent l'épine dorsale de ce magazine. Si vous avez un article ou une idée d'article, mais que vous ne savez pas par où commencer, n'hésitez pas à nous contacter à l'adresse [editors@dri.ca](mailto:editors@dri.ca) et nous vous aiderons à le mener à bien, et si vous souhaitez que votre point de vue et votre expérience figurent dans ces pages, n'hésitez pas à nous le soumettre et nous vous rendrons célèbre. Ω

Merci de votre attention !

Les rédacteurs du DRIC Résilience du vrai nord

- Ron Andrews
- Alexander Landry
- Charlie Shymko
- Brady Podloski
- Garth Tucker
- Steve Palubiski



*That's it? That's your  
backup plan?*

*“You’re only as  
good as your  
last good backup!”*

~ Dan Duffy,  
President, Mid-Range

**DR Hot Sites** ▲

**BUaaS** ▲

**DRaaS** ▲

**High Availability** ▲

**Testing** ▲



[www.midrange.ca](http://www.midrange.ca)

[Retour au sommaire](#)





# An Expert's Impression

## L'impression d'un expert

**W**e are excited to introduce a new feature in the Autumn 2024 issue of True North Resilience called: **“An Expert's Impression.”**

In this ongoing series, we will present a question related to a recent event impacting the resilience industry and invite various experts to share their perspectives. By gathering diverse opinions, we aim to foster a deeper understanding of significant events and stimulate meaningful discussions on improving industry practices.

Each expert's response will be independent, with no coordination between them, ensuring a wide range of viewpoints.

In this inaugural issue, we will focus on the recent CrowdStrike outage, exploring its causes and implications. Our experts will provide insights into the incident, shedding light on key factors and offering their assessments.

### **Thank you very much to this issue's Experts.**

They are very diverse, geographically and professionally, but all have excellent insights into this event and we're grateful to them all for taking the time to give us the benefit of their experience.

If you would like to be considered for your input in future issues, please email your credentials with a bio and profile picture to [editors@dri.ca](mailto:editors@dri.ca) and we will reach out when the upcoming issue has a question which falls in your area of expertise.

Thanks!

- GAT

**N**ous sommes ravis de présenter une nouvelle fonctionnalité dans le numéro d'automne 2024 de True North Resilience intitulée : **« An Expert's Impression ».**

Dans cette série en cours, nous présenterons une question liée à un événement récent ayant un impact sur l'industrie de la résilience et inviterons divers experts à partager leurs points de vue. En recueillant des opinions diverses, nous visons à favoriser une meilleure compréhension des événements importants et à stimuler des discussions significatives sur l'amélioration des pratiques de l'industrie.

La réponse de chaque expert sera indépendante, sans coordination entre eux, assurant un large éventail de points de vue.

Dans ce numéro inaugural, nous nous concentrerons sur la récente panne de CrowdStrike, en explorant ses causes et ses implications. Nos experts fourniront des informations sur l'incident, en faisant la lumière sur les facteurs clés et en offrant leurs évaluations.

### **Merci beaucoup aux experts de cette question.**

Ils sont très diversifiés, géographiquement et professionnellement, mais tous ont d'excellents aperçus de cet événement et nous leur sommes reconnaissants à tous d'avoir pris le temps de nous donner le bénéfice de leur expérience.

Si vous souhaitez être pris en considération pour votre contribution dans les prochains numéros, veuillez envoyer vos informations d'identification avec une photo de biographie et de profil à [editors@dri.ca](mailto:editors@dri.ca) et nous vous contacterons lorsque le prochain numéro aura une question qui relève de votre domaine d'expertise.

Merci !

- GAT

This issue's question is:

**WHAT DO YOU FEEL WAS THE CAUSE OF THE IMPACT TO BUSINESS OF THE CROWDSTRIKE OUTAGE? NOT THE ACTUAL EVENT WHICH WE ARE AWARE WAS A FAULTY PATCH IN THE SOFTWARE, BUT THE REASON WHY AND HOW IT CAUSED SO MUCH HAVOC TO SO MANY ORGANIZATIONS?**

La question de ce problème est la suivante :

**SELON VOUS, QUELLE A ÉTÉ LA CAUSE DE L'IMPACT DE LA PANNE CROWDSTRIKE SUR LES ENTREPRISES ? PAS L'ÉVÉNEMENT RÉEL DONT NOUS SOMMES CONSCIENTS ÉTAIT UN CORRECTIF DÉFECTUEUX DANS LE LOGICIEL, MAIS LA RAISON POUR LAQUELLE ET COMMENT IL A CAUSÉ TANT DE RAVAGES À TANT D'ORGANISATIONS ?**

© Karine Kong All Rights Reserved



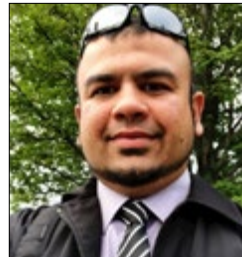
Alexandra Hoffmann, MBA  
CEO, Crisis Ally



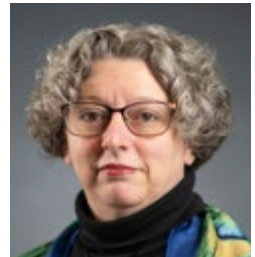
Jason Firlotte  
MBCP, CBRM, MBCI, CSP, CBCV  
President, Sentinel BCM



Kevin Powers  
Team Leader, Applications  
Goodmans LLP



Emad Aziz, MBCP



Cynthia Wenn,  
CBCP, CBCA

## Alexandra Hoffmann

The CROWDSTRIKE incident that struck on July 19th, 2024, underscored a critical issue with our heavy reliance on digital tools. The breach affected multiple areas, including IT operations, security, business continuity, brand reputation, employee experience, customer experience, and financial stability. As technology becomes more embedded in our operations, even minor glitches can lead to significant disruptions, revealing our vulnerability to single points of failure in our tech systems. However, the issue is broader.

In recent years, expectations have shifted dramatically. We now assume that nothing should go wrong and that we should experience no impact from unforeseen events. This mindset reflects not just risk aversion but impact aversion. We desire zero disruptions and expect no consequences when problems arise. While some may label this as resilience, it is not. The truth lies in the middle. True resilience involves embracing and adapting to disruptions and changes, recognizing our capacity to manage and overcome challenges rather than expecting a flawless system.

## Alexandra Hoffmann

L'incident de CROWDSTRIKE survenu le 19 juillet 2024 a souligné un problème critique lié à notre dépendance excessive aux outils numériques. L'incident a impacté plusieurs domaines, y compris les opérations IT, la sûreté, la continuité des affaires, la réputation, l'expérience des employés et client, ainsi que la stabilité financière. À mesure que la technologie devient de plus en plus intégrée dans nos organisations, même des dysfonctionnements mineurs peuvent entraîner des perturbations importantes, révélant notre vulnérabilité aux points de défaillance uniques dans nos systèmes technologiques. Cependant, le problème est plus large.

Ces dernières années, les attentes ont considérablement évolué. Nous supposons maintenant que rien ne devrait mal tourner et que nous ne devrions pas subir d'impact des événements imprévus. Cet état d'esprit reflète non seulement une aversion au risque, mais aussi une aversion à l'impact.



To build genuine resilience, we need to implement more redundancies, both within our technology and human roles. Additionally, while tech tools enhance our productivity, communication, innovation, automation, and insights capabilities, they demand ongoing human oversight and interaction to ensure effectiveness and accuracy. Lastly, organizations should avoid promising zero-risk or zero-impact solutions. Instead, they should educate stakeholders about potential risks and the realities of disruption. Transparent communication will help set realistic expectations and foster a more resilient approach to managing (technological) challenges.

Some of our clients were affected by the shutdown, but the impact was minimal. This highlights the need for a case-by-case examination, as each organization faces unique circumstances and stakeholders that influence the extent of the disruption. ❖

### Jason Firlotte

I believe this outage points to larger concerns in the industry, specifically a reliance on a relatively

Nous désirons zéro perturbation et attendons aucune conséquence lorsque des problèmes surviennent. Bien que certains puissent qualifier cela de résilience, ce n'en est pas. La vérité se trouve au milieu. La véritable résilience consiste à accepter et à s'adapter aux perturbations et aux changements, en reconnaissant notre capacité à gérer et à surmonter les défis plutôt que de s'attendre à un système parfait.

Pour construire un système résilient, nous devons mettre en place davantage de redondances, tant au niveau de notre technologie que de nos rôles humains.

De plus, bien que les outils technologiques améliorent notre productivité, notre communication, notre capacité à innover, à automatiser et à obtenir des informations, ils nécessitent une supervision et une interaction humaines constantes pour garantir leur efficacité et leur précision.

Enfin, les organisations devraient éviter de promettre des solutions et des services sans risque ou sans impact. Au lieu de cela, elles devraient éduquer les parties prenantes sur les risques potentiels et les réalités de la perturbation.

Une communication transparente aidera à fixer des attentes réalistes et à favoriser une approche plus résiliente pour gérer les défis (technologiques).

Certains de nos clients ont été affectés par l'arrêt des systèmes ce jour-là, mais l'impact a été minime. Cela souligne la nécessité d'un examen au cas par cas, chaque organisation faisant face à des circonstances et à des parties prenantes uniques qui influencent l'étendue de l'impact. ❖

### Jason Firlotte

Je crois que cette panne souligne des préoccupations plus larges dans l'industrie, en particulier une dépendance à l'égard d'un groupe relativement petit de fournisseurs de logiciels / logiciels, et l'absence de

**Exercise in a Box**

**An economical way to deliver a tabletop exercise.**

This kit contains over 40 comprehensive tools. Leverage our plans, templates, and checklists to coach your team with confidence.

**INCLUDES:**

- Scope and Objectives
- Participant Guidelines
- Scenario
- Injects
- Evaluator Package
- Report Templates
- And much more...

**\$1499**

**Vanguard**  
emergency.com

training@vanguardemergency.com  
Mitigation • Response • Continuity • Recovery

small group of software / software providers, and the absence of alternative processing capabilities in the event of an outage. With the largest market share in the segment, any issue impacting a vendor like CrowdStrike was going to have massive impacts on business, and this is not a unique situation.

How many common tools are used extensively through multiple businesses and would have the same impact? Look to the recent ransomware attack on CDK Global, which impacted some 15,000 car dealers for multiple days. The absence of variety is by its very nature the thing that makes them vulnerable.

Which brings us to the second point, the inability of these businesses to pivot to alternative process methods. Businesses need to be aware of these potential vulnerabilities and have suitable plans and technology in place to restore/maintain their key functions. They need proactive measures to ensure that even if a key piece of vendor software is unavailable, they still have the ability to provide their critical services. ❖

### Kevin Powers

“Keys to the kingdom”. About 8.5 million keys actually. That collectively sums up what was given to CrowdStrike. In the ever-increasing battle between malicious actors, the collective “we” have had to turn to more sophisticated software to help stay ahead of “the bad guys”. In doing so we gave CrowdStrike the one thing that Sysadmins are told to never give to anyone: root access. A possibly misplaced trust was given to an outside entity based on a promise to protect. While updates to fight malicious actors must come as quickly as the attacks themselves, there is no excuse for an untested patch to be deployed. This fault should have been easily caught through testing. CrowdStrike should have been extra diligent considering this was their third such incident this year, albeit the first two only (and I say that sarcastically) impacted Debian and Rocky Linux machines in April and May.

CrowdStrike failed in their due diligence, however I honestly think we must shoulder some of the blame. We were the ones who handed over the keys to a company run by CEO George Kurtz, the same person who in 2009 (while CTO at McAfee) deployed an update that caused Windows XP

capacités de traitement alternatives en cas de panne. Avec la plus grande part de marché dans le segment, tout problème ayant un impact sur un fournisseur comme CrowdStrike allait avoir des impacts massifs sur les affaires, et ce n'est pas une situation unique.

Combien d'outils communs sont largement utilisés par plusieurs entreprises et auraient le même impact ? Regardez la récente attaque de ransomware sur CDK Global, qui a touché quelque 15 000 concessionnaires automobiles pendant plusieurs jours. L'absence de variété est par sa nature même la chose qui les rend vulnérables.

Ce qui nous amène au deuxième point, l'incapacité de ces entreprises à se tourner vers d'autres méthodes de processus. Les entreprises doivent être conscientes de ces vulnérabilités potentielles et avoir des plans et une technologie appropriés en place pour restaurer / maintenir leurs fonctions clés. Ils ont besoin de mesures proactives pour s'assurer que même si un élément clé du logiciel du fournisseur n'est pas disponible, ils ont toujours la capacité de fournir leurs services essentiels. ❖

### Kevin Powers

« Keys to the kingdom ». Environ 8,5 millions de clés en fait. Cela résume collectivement ce qui a été donné à CrowdStrike. Dans la bataille sans cesse croissante entre les acteurs malveillants, le collectif « nous » ont dû se tourner vers des logiciels plus sophistiqués pour aider à garder une longueur d'avance sur « les méchants ». Ce faisant, nous avons donné à CrowdStrike la seule chose qu'on dit aux administrateurs système de ne jamais donner à personne : l'accès root. Une confiance peut-être mal placée a été accordée à une entité externe sur la base d'une promesse de protection. Bien que les mises à jour pour lutter contre les acteurs malveillants doivent venir aussi rapidement que les attaques elles-mêmes, il n'y a aucune excuse pour qu'un correctif non testé soit déployé. Ce défaut aurait dû être facilement détecté par des tests. CrowdStrike aurait dû être très diligent étant donné qu'il s'agissait de leur troisième incident de ce type cette année, bien que les deux premiers seulement (et je le dis sarcastiquement) aient eu un impact sur les machines Debian et Rocky Linux en avril et mai.

machines to bluescreen and boot loop. While I don't blame George directly, management styles may have had a say in why this update was deployed without proper validation. Going forward, I hope we have learned a hard lesson. Vetting access to our keys is essential to protecting our kingdom. ❖

### Emad Aziz

While the province of Nova Scotia was not directly impacted by the outage (except for flight delays), the incident exposes vulnerabilities that organizations need to be aware of.

The phrase "CrowdStrike" was relatively unknown until the incident. When organizations are handing over controls of their IT systems, assurances are given at executive presentations and in Service Level Agreements, but there is no way of knowing what's really going on behind the curtain. Too-big-to-fail thinking and subsequent let's-save-money-by-re-outsourcing shows the fragility of IT service delivery. One broken link in the service delivery chain can crash the entire system. Do you know who your service provider relies on? The longer the chain, the more worried you should be.

We must also acknowledge that despite the most robust controls and exhaustive testing processes, any technology is most susceptible to its weakest link: human error. That's what caused the global outage – the glitchy software did exactly what it was programmed to do, it was human(s) who executed the code. BCM professionals must plan for and create realistic exercise scenarios that consider inadvertent impacts resulting from human error.

Finally, if an organisation believes a \$10 Uber Eats voucher (that also doesn't work) is going to regain trust with clients losing millions of dollars, its time to seriously think about business continuity and hire a professional. ❖

CrowdStrike a échoué dans leur diligence raisonnable, mais je pense honnêtement que nous devons assumer une partie du blâme. C'est nous qui avons remis les clés à une entreprise dirigée par le PDG George Kurtz, la même personne qui, en 2009 (alors qu'il était directeur technique chez McAfee), a déployé une mise à jour qui a provoqué l'écran bleu et la boucle de démarrage des ordinateurs Windows XP. Bien que je ne blâme pas directement George, les styles de gestion ont peut-être eu leur mot à dire sur la raison pour laquelle cette mise à jour a été déployée sans validation appropriée. À l'avenir, j'espère que nous aurons appris une dure leçon. Le contrôle de l'accès à nos clés est essentiel pour protéger notre royaume. ❖

### Emad Aziz

Bien que la province de la Nouvelle-Écosse n'ait pas été directement touchée par la panne (à l'exception des retards de vol), l'incident révèle des vulnérabilités dont les organisations doivent être conscientes.

L'expression « CrowdStrike » était relativement inconnue jusqu'à l'incident. Lorsque les organisations remettent les contrôles de leurs systèmes informatiques, des assurances sont données lors des présentations exécutives et dans les accords de niveau de service, mais il n'y a aucun moyen de savoir ce qui se passe vraiment derrière le rideau. La pensée too-big-to-fail et les let's-save-money-by-re-outsourcing ultérieurs montrent la fragilité de la prestation de services informatiques. Un maillon brisé dans la chaîne de prestation de services peut planter l'ensemble du système. Savez-vous sur qui votre fournisseur de services compte ? Plus la chaîne est longue, plus vous devriez être inquiet.

Nous devons également reconnaître que malgré les contrôles les plus robustes et les processus de test exhaustifs, toute technologie est la plus sensible à son maillon le plus faible : l'erreur humaine. C'est ce qui a causé la panne mondiale - le logiciel glitchy a fait exactement ce qu'il a été programmé pour faire, c'est l'homme (s) qui a exécuté le code. Les professionnels de la GCA doivent planifier et créer des scénarios d'exercice réalistes qui tiennent compte des impacts involontaires résultant d'une erreur humaine.

Enfin, si une organisation estime qu'un bon Uber Eats de 10 \$ (qui ne fonctionne pas non plus) va regagner la confiance avec des clients qui perdent des millions de dollars, il est temps de réfléchir sérieusement à la continuité des activités et d'embaucher un professionnel. ❖


## Cynthia Wenn

The current techno-economic ecosystem has been built on consolidation, interconnectedness, and speed. These factors work together to make disruptions like the CrowdStrike outage inevitable and business continuity and disaster recovery plans essential.

While the CrowdStrike outage only impacted Microsoft's Windows operating systems, in 2024 they account for nearly 70% of the world's desktop, tablet, and console OS market. Apple and Linux machines were not affected by the CrowdStrike software update. Vulnerability exists within every ecosystem organic or inorganic when sufficient diversity no longer exists. The trend has been toward greater consolidation within the technology industry rather than diversification.

The CrowdStrike outage was related to a faulty Windows kernel-level driver, which is software installed at the deepest levels of a computer. The benefits of interconnectivity depend on often unwarranted trust in third party organizations and workplaces. The COVID-19 pandemic exposed how interconnected our supply chains had become. This outage demonstrates how our technological systems are even more interconnected and vulnerable.

The flawed CrowdStrike update was released and pulled back within an hour and a half but managed to cause disruption globally. The speed at which an error can move through the global technology system is astonishing.

For most organizations, private or public, it is impossible to circumvent the consolidated, interconnected, and speed of our current techno-economic ecosystem. Given this inevitability, it is reasonable to consider low-tech short-term business continuity solutions for our organizations or disaster recovery plans which account for these considerations. 


## Cynthia Wenn

L'écosystème techno-économique actuel a été construit sur la consolidation, l'interconnexion et la rapidité. Ces facteurs fonctionnent ensemble pour rendre les perturbations comme la panne de CrowdStrike inévitables et les plans de continuité des activités et de reprise après sinistre essentiels.

Bien que la panne de CrowdStrike n'ait eu d'impact que sur les systèmes d'exploitation Windows de Microsoft, en 2024, ils représentent près de 70% du marché mondial des systèmes d'exploitation pour ordinateurs de bureau, tablettes et consoles. Les machines Apple et Linux n'ont pas été affectées par la mise à jour logicielle CrowdStrike. La vulnérabilité existe au sein de chaque écosystème organique ou inorganique lorsque la diversité ne suffit plus. La tendance a été à une plus grande consolidation au sein de l'industrie de la technologie plutôt qu'à une diversification.

La panne de CrowdStrike était liée à un pilote défectueux au niveau du noyau Windows, qui est un logiciel installé aux niveaux les plus profonds d'un ordinateur. Les avantages de l'interconnectivité dépendent d'une confiance souvent injustifiée dans des organisations et des lieux de travail tiers. La pandémie de COVID-19 a révélé à quel point nos chaînes d'approvisionnement étaient devenues interconnectées. Cette panne démontre à quel point nos systèmes technologiques sont encore plus interconnectés et vulnérables.

La mise à jour défectueuse de CrowdStrike a été publiée et retirée en une heure et demie, mais a réussi à causer des perturbations à l'échelle mondiale. La vitesse à laquelle une erreur peut se déplacer dans le système technologique mondial est étonnante.

Pour la plupart des organisations, privées ou publiques, il est impossible de contourner la consolidation, l'interconnexion et la rapidité de notre écosystème techno-économique actuel. Compte tenu de cette inévitabilité, il est raisonnable d'envisager des solutions de continuité des activités à court terme de faible technologie pour nos organisations ou des plans de reprise après sinistre qui tiennent compte de ces considérations. 



## ABOUT THE EXPERTS

---

### **Alexandra Hoffmann, MBA –**

Alexandra is the CEO of CRISIS ALLY. Her extensive career spans the French government, multinational corporations, and NGOs, offering a wealth of experience in organizations resilience. A certified coach and yoga teacher, she holds degrees in Corporate Security, Criminal Law, and an MBA.

---

### **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.

---

### **Kevin Powers –**

Kevin is a seasoned IT leader with over 20 years of experience supporting a prominent Bay Street law firm in Toronto, an avid shade-tree mechanic, and an advocate for those with Down syndrome.

---

### **Emad Aziz, MBCP –**

Emad 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.

---

### **Cynthia Wenn, CBCP, CBCA –**

Cynthia currently offers subject matter expertise at the Public Health Agency of Canada as a member of the Emergency Management Plans, Exercises and Continuous Improvement unit. For fourteen years at Vanguard Emergency Management Consulting Inc., Cynthia provided professional services and advice to many organizations on risk, emergency, and business continuity management, reimagined, designed, and delivered professional industry-specific course material, and assisted clients with all steps of plan development and exercise design and delivery. She has obtained the Certified Business Continuity Professional (CBCP) and the Certified Business Continuity Auditor (CBCA), from Disaster Recovery Institute Canada and is currently pursuing a Doctor of Social Sciences from Royal Roads University.

---

## À PROPOS DES EXPERTS

---

### **Alexandra Hoffmann, MBA –**

Alexandra est la PDG de CRISIS ALLY. Sa longue carrière couvre le gouvernement français, les multinationales et les ONG, offrant une riche expérience dans la résilience des organisations. Coach certifiée et professeure de yoga, elle est titulaire de diplômes en sécurité d'entreprise, en droit pénal et d'un MBA.

---

### **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.

---

### **Kevin Powers –**

Kevin est un leader chevronné en TI avec plus de 20 ans d'expérience dans le soutien d'un important cabinet d'avocats de Bay Street à Toronto, un fervent mécanicien d'arbres d'ombrage et un défenseur des personnes atteintes du syndrome de Down.

---

### **Emad Aziz, MBCP –**

Emad 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.

---

### **Cynthia Wenn, CBCP, CBCA –**

Cynthia offre actuellement une expertise en la matière à l'Agence de la santé publique du Canada en tant que membre de l'Unité des plans de gestion des urgences, des exercices et de l'amélioration continue. Pendant quatorze ans chez Vanguard Emergency Management Consulting Inc., Cynthia a fourni des services et des conseils professionnels à de nombreuses organisations sur la gestion des risques, des urgences et de la continuité des activités, a réinventé, conçu et fourni du matériel de cours professionnel spécifique à l'industrie, et a aidé les clients à toutes les étapes de l'élaboration du plan et de la conception et de la livraison des exercices. Elle a obtenu le Certified Business Continuity Professional (CBCP) et le Certified Business Continuity Auditor (CBCA), de l'Institut de reprise après sinistre du Canada et poursuit actuellement un doctorat en sciences sociales de l'Université Royal Roads.

---

# Network & Endpoint Security Challenges – the lack of endgame

## Défis en matière de sécurité des réseaux et des points finaux - l'absence de finalité

*By/Par Randy Bucking*

**W**ith the security rollout failure within the CrowdStrike community fresh in our minds and greatly publicized in the media recently, the ongoing in-the-trenches battle for network and end-user security was thrust back into the limelight. Network admins and end-user security teams from airlines to healthcare and government industries scrambled, with blue-screens and idle workers telling the tell.

Most of us have seen a rollout go sideways or errantly beyond control in our careers. They're easy to spot, the damage is widespread, impactful and on a glaring scale. Costs mount but the endgame is likely to just revert/rollback and try again.

But what continues to fly under the radar are the daily, tiny exploits, zero-day threats and seemingly minor nagging anomalies that don't get noticed. The ones that lurk and persist

**L**'échec du déploiement de la sécurité au sein de la communauté CrowdStrike étant encore frais dans nos mémoires et ayant fait l'objet d'une grande publicité dans les médias récemment, la bataille en cours dans les tranchées pour la sécurité des réseaux et des utilisateurs finaux a été ramenée sous les feux de la rampe. Les administrateurs de réseau et les équipes chargées de la sécurité des utilisateurs finaux, qu'il s'agisse de compagnies aériennes, de services de santé ou d'industries gouvernementales, se sont précipités, avec des écrans bleus et des travailleurs désœuvrés qui racontent l'histoire.

La plupart d'entre nous ont vu, au cours de leur carrière, un déploiement déraiper ou échapper à tout contrôle. Ils sont faciles à repérer, les dommages sont étendus, ont un impact et sont d'une ampleur flagrante. Les coûts augmentent, mais la finalité est probablement de revenir en arrière et de recommencer.

without much, if any detection until they are more widespread and eventually a larger problem.

With post-COVID workers demanding hybrid and cloud based remote work solutions, the edge of the network and the devices used just beyond that edge have turned the once secure corporate tree into a ragged overgrown dark forest – a jungle of VPN's, firewalls, LTE and 5G and users on tablets, phones and laptops running various OS's and application security endpoint platforms on top of them. All of which need to be constantly updated.

It's difficult, now more than ever, to find unity. The core network, at the local hosting company or in the cloud, represents what seems to be an ever smaller piece of this forest.

While network admins are well versed in core device and threat updates, patches and

firewall management, it's beyond the edge and the user realm that seems to be where most attacks are now targeted. The end-users come under phishing attacks, app hijacking, MAC address spoofing and other forms of breach, all while on the road, at the cottage or working from home where distractions bely that focus on staying on top of OS updates, app patches and system firewall updates.

### **They're supposed to be automatic. Right?**

Your implicit trust that the next rollout from your security vendor will end without disaster is assumed.

That trust is supposed to be your endgame to the absolutely endless stream of new daily exploits and attacks. Yet in order to tackle this plethora of mobile network devices and users, it's been proven that one vendor, and implicit trust in that vendor isn't enough.



**EN CAS D'INCIDENT MAJEUR,  
QUEL EST  
VOTRE PLAN ?**

**NOUS SOMMES LA RÉFÉRENCE**

- CONTINUITÉ DES AFFAIRES
- MESURES D'URGENCE
- GESTION DE CRISE
- RELÈVE DE DÉSASTRÉ

*We are located in Quebec but our services are available in English across Canada.  
Get in touch with us!*



N'attendez pas avant qu'il soit trop tard  
**CONTACTEZ-NOUS POUR EN SAVOIR PLUS**

**BR** Benoit Racette  
Services-conseils inc.  
Continuité des affaires | Mesures d'urgence  
Gestion de crise | Relève de désastre

**RACETTECONSEILS.COM**

514 312-8474

info@racetteconseils.com



**With this plethora of mobile network devices, implicit trust in one vendor isn't enough...**

**Avec cette pléthore d'appareils de réseau mobile, la confiance implicite dans un seul fournisseur ne suffit pas...**

Mais ce qui continue à passer inaperçu, ce sont les petits exploits quotidiens, les menaces de type “zéro jour” et les anomalies apparemment mineures qui ne sont pas remarquées. Ce sont celles qui se cachent et persistent sans être détectées, ou presque, jusqu'à ce qu'elles soient plus répandues et finissent par poser un problème plus important.

Les travailleurs post-COVID exigeant des solutions de travail à distance hybrides et basées sur le cloud, la périphérie du réseau et les appareils utilisés juste au-delà de cette périphérie ont transformé l'arbre de l'entreprise autrefois sécurisé en une forêt sombre envahie par la végétation - une jungle de VPN, de pare-feu, de LTE et de 5G et d'utilisateurs sur des tablettes, des téléphones et des ordinateurs portables exécutant divers systèmes d'exploitation et plates-formes de points finaux de sécurité des applications. Toutes ces plateformes doivent être constamment mises à jour.

Il est difficile, aujourd'hui plus que jamais, de trouver une unité. Le réseau central, chez l'hébergeur local ou dans le nuage, représente ce qui semble être un morceau de plus en plus petit de cette forêt.

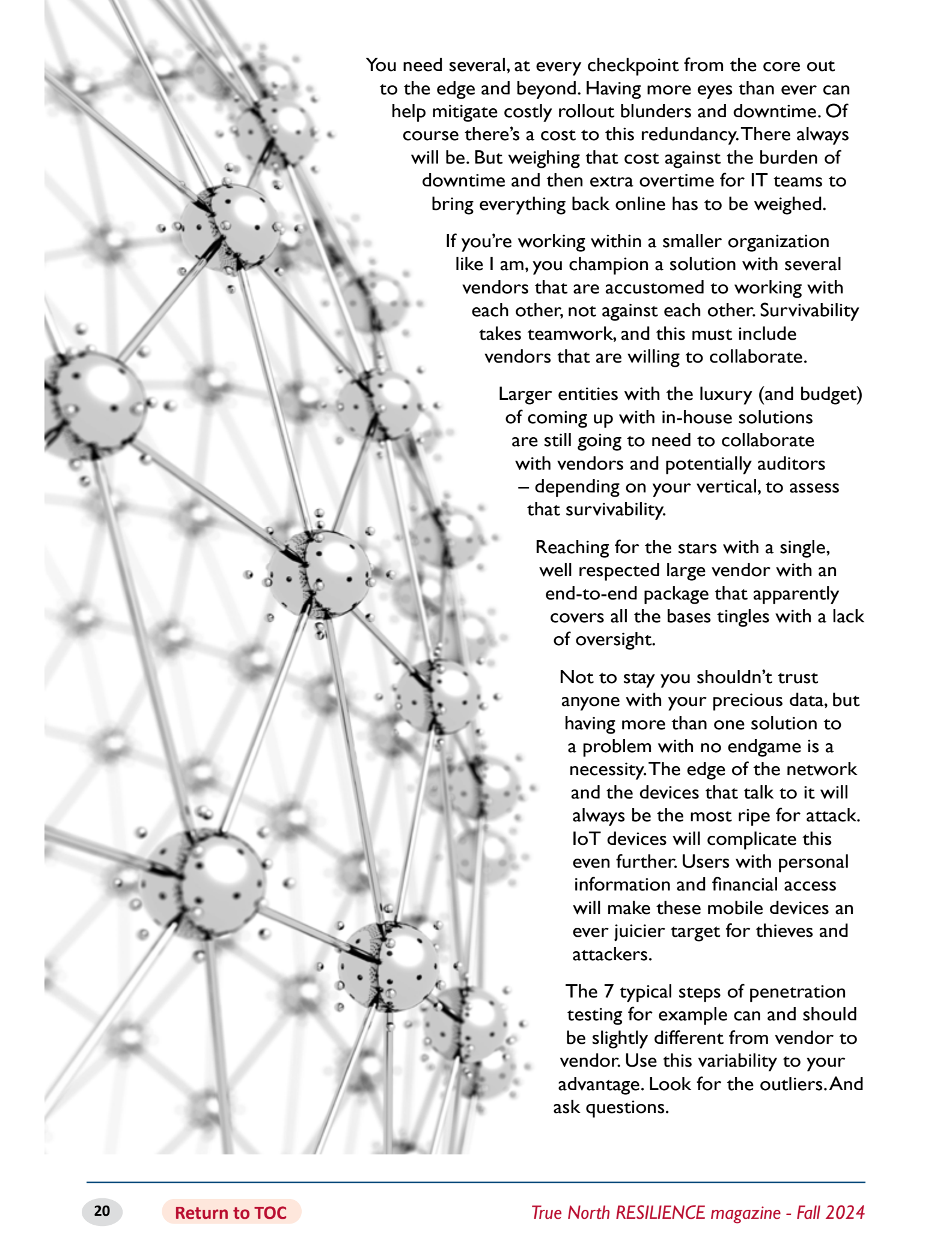
Alors que les administrateurs de réseau sont bien au fait des mises à jour des appareils de base et des menaces, des correctifs et de la gestion des pare-feux, c'est au-delà de la périphérie et du domaine de l'utilisateur que semblent être ciblées la plupart des attaques. Les utilisateurs finaux sont victimes d'attaques de phishing, de détournement d'applications, d'usurpation d'adresse MAC et d'autres formes d'intrusion, tout cela alors qu'ils sont en déplacement, au chalet ou qu'ils travaillent à domicile, où les distractions empêchent de se concentrer sur les mises à jour du système d'exploitation, les correctifs d'applications et les mises à jour du pare-feu du système.

### **Ils sont censés être automatiques. C'est vrai ?**

Vous vous attendez implicitement à ce que le prochain déploiement de votre fournisseur de sécurité se déroule sans désastre.

Cette confiance est censée être la finalité de la lutte contre le flot ininterrompu de nouveaux exploits et d'attaques quotidiennes. Pourtant, pour faire face à cette pléthore d'appareils et d'utilisateurs de réseaux mobiles, il a été prouvé qu'un seul fournisseur et la confiance implicite qu'il inspire ne suffisent pas.





You need several, at every checkpoint from the core out to the edge and beyond. Having more eyes than ever can help mitigate costly rollout blunders and downtime. Of course there's a cost to this redundancy. There always will be. But weighing that cost against the burden of downtime and then extra overtime for IT teams to bring everything back online has to be weighed.

If you're working within a smaller organization like I am, you champion a solution with several vendors that are accustomed to working with each other, not against each other. Survivability takes teamwork, and this must include vendors that are willing to collaborate.

Larger entities with the luxury (and budget) of coming up with in-house solutions are still going to need to collaborate with vendors and potentially auditors – depending on your vertical, to assess that survivability.

Reaching for the stars with a single, well respected large vendor with an end-to-end package that apparently covers all the bases tangles with a lack of oversight.

Not to stay you shouldn't trust anyone with your precious data, but having more than one solution to a problem with no endgame is a necessity. The edge of the network and the devices that talk to it will always be the most ripe for attack. IoT devices will complicate this even further. Users with personal information and financial access will make these mobile devices an ever juicier target for thieves and attackers.

The 7 typical steps of penetration testing for example can and should be slightly different from vendor to vendor. Use this variability to your advantage. Look for the outliers. And ask questions.

Il en faut plusieurs, à chaque point de contrôle, du cœur de l'entreprise jusqu'à la périphérie et au-delà. Le fait d'avoir plus d'yeux que jamais permet d'atténuer les erreurs de déploiement et les temps d'arrêt coûteux. Bien sûr, cette redondance a un coût. Il y en aura toujours un. Mais il faut mettre ce coût en balance avec le fardeau que représentent les temps d'arrêt et les heures supplémentaires des équipes informatiques pour tout remettre en ligne.

Si, comme moi, vous travaillez au sein d'une petite organisation, vous êtes le champion d'une solution avec plusieurs fournisseurs qui ont l'habitude de travailler les uns avec les autres, et non les uns contre les autres. Pour survivre, il faut travailler en équipe, ce qui implique que les fournisseurs soient prêts à collaborer.

Les grandes entités qui ont le luxe (et le budget) de trouver des solutions en interne devront toujours collaborer avec des fournisseurs et éventuellement des auditeurs

- en fonction de leur secteur d'activité - pour évaluer cette capacité de survie.

Le fait de viser les étoiles avec un seul grand fournisseur, très respecté, qui propose une offre globale couvrant apparemment toutes les bases, donne l'impression d'un manque de supervision.

Il ne s'agit pas de dire qu'il ne faut confier ses précieuses données à personne, mais il est nécessaire d'avoir plus d'une solution à un problème qui n'a pas de fin. La périphérie du réseau et les appareils qui s'y connectent seront toujours les plus exposés aux attaques. Les appareils IoT vont encore compliquer les choses. Les utilisateurs disposant d'informations personnelles et d'un accès financier feront de ces appareils mobiles une cible encore plus juteuse pour les voleurs et les attaquants.

Les 7 étapes typiques des tests de pénétration, par exemple, peuvent et doivent être

## CONTINUITY & RESILIENCE TODAY

OCTOBER 22-23, 2024  
INTERNATIONAL CENTRE • TORONTO

Continuity & Resilience Today is Canada's premier business continuity event, providing global perspectives on current and emerging issues for continuity & resilience professionals

**12 CEAP POINTS/CPD HOURS**  
REGISTER TODAY  
WITH A 5% OFF DISCOUNT CODE  
**TRUENORTH24**

[CRTDEMCON.ca](http://CRTDEMCON.ca)

It's been said that managing devices is easier than managing the people using them. Accountability is responsibility and yet machines simply trust the software running on them – and that's an issue if a hacker has modified or code-injected that software.

People? Not so much. Trust and responsibility is learned and earned but distractions, life and the ever increasing mobility and personal usage of corporate devices mitigates this certainty. High value users especially, no matter their position, identity or role need to be aware that once identified will be a constant target. Anonymity cannot be guaranteed. Travel to foreign countries for example can escalate the potential of threat.

And while you can apply policy and attempt to educate users, there will always be those outliers. And if it's not the user, it very well could be the vendor.

The more eyes you have in the forest, the less dark it can appear. The more options you have to deflect a potential attack, the better your survivability. Build your relationships with as many vendors, open source communities and team members as you're able. And collaborate. Don't ignore those small anomalies, report them. Ω

---

### About the Author

#### **Randy Bucking**

*Working in various IT roles since 1995, for both large corporations and small businesses, I currently reside in the finance industry in the greater Toronto area designing, deploying and maintaining a global infrastructure for a broker-dealer / software firm.*



légèrement différentes d'un fournisseur à l'autre. Utilisez cette variabilité à votre avantage. Recherchez les valeurs aberrantes. Et posez des questions.

On dit qu'il est plus facile de gérer les appareils que les personnes qui les utilisent. L'obligation de rendre compte est synonyme de responsabilité et pourtant les machines font simplement confiance aux logiciels qui tournent sur elles - ce qui pose un problème si un pirate informatique a modifié ou injecté du code dans ces logiciels.

Les gens ? Pas tant que cela. La confiance et la responsabilité s'apprennent et se gagnent, mais les distractions, la vie et l'augmentation constante de la mobilité et de l'utilisation personnelle des appareils de l'entreprise atténuent cette certitude. Les utilisateurs de grande valeur en particulier, quels que soient leur position, leur identité ou leur rôle, doivent être conscients qu'une fois identifiés, ils seront une cible constante. L'anonymat ne peut être garanti. Les voyages à l'étranger, par exemple, peuvent accroître le potentiel de menace.

Et bien que vous puissiez appliquer une politique et tenter d'éduquer les utilisateurs, il y aura toujours des exceptions. Et si ce n'est pas l'utilisateur, cela peut très bien être le fournisseur.

Plus vous avez d'yeux dans la forêt, moins elle est sombre. Plus vous avez d'options pour détourner une attaque potentielle, meilleure est votre capacité de survie. Nouez des relations avec autant de fournisseurs, de communautés open source et de membres d'équipe que vous le pouvez. Et collaborez. N'ignorez pas les petites anomalies, signalez-les. Ω

---

### À propos de l'auteur

#### **Randy Bucking**

*Travaillant dans divers rôles informatiques depuis 1995, tant pour les grandes entreprises que pour les petites entreprises, je réside actuellement dans l'industrie financière dans la région du Grand Toronto en concevant, en déployant et en maintenant une infrastructure mondiale pour un courtier-négociant / société de logiciels.*

# Implementing the Professional Practices

# Mise en œuvre des pratiques professionnelles



**D**Ri's Professional Practices for Business Continuity Management are the foundation of an effective business continuity program. In this series of articles, we invited senior business continuity professionals to share their experiences in implementing the Professional Practices: the pitfalls and challenges they encountered, and how they managed them.

This series isn't intended to be the definitive word on implementing the Practices. Each article reflects the unique experiences of a business continuity professional. Take up their ideas, adapt them, disagree with them, but ultimately use them to deepen your understanding of the Professional Practices.

If you'd like to contribute a short article on implementing one of the Professional Practices, contact us at [editors@dri.ca](mailto:editors@dri.ca).

— Jeff Hortobagyi, CBCP, MBC

**L**es pratiques professionnelles de DRI en matière de gestion de la continuité des activités constituent la base d'un programme efficace de continuité des activités. Dans cette série d'articles, nous avons invité des professionnels chevronnés de la continuité d'activité à partager leur expérience de la mise en œuvre des pratiques professionnelles : les pièges et les défis qu'ils ont rencontrés, et la manière dont ils les ont gérés.

Cette série n'a pas pour but de faire autorité en matière de mise en œuvre des pratiques. Chaque article reflète l'expérience unique d'un professionnel de la continuité des affaires. Reprenez ses idées, adaptez-les, désapprouvez-les, mais en fin de compte utilisez-les pour approfondir votre compréhension des pratiques professionnelles.

Si vous souhaitez rédiger un article sur la mise en œuvre de l'une des pratiques professionnelles, contactez-nous à l'adresse [editors@dri.ca](mailto:editors@dri.ca).



# BUSINESS CONTINUITY PLAN



## From Confusion to Clarity: Four Tips to Building a Better Plan

## De la confusion à la clarté : quatre conseils pour bâtir un meilleur plan

*By/Par Jason Firlotte, MBCP, CBRM, MBCI, CSP, CBCV*

## From Confusion to Clarity: Four Tips to Building a Better Plan

Undertaking the development of a Business Continuity Plan can be a daunting journey, with many potential difficulties. By following a few key planning practices outlined below, you can avoid some of the pitfalls of planning.



### 1. It will take longer than you expect

Even the best project planning rarely survives first contact with the realities of business. When developing your timelines, ensure that you build in a sufficient buffer to accommodate the variables you cannot control.

It is important to be aware of peak or critical processing times for your business lines and the availability of staff. Just because it's a priority to you, doesn't mean it's the priority of the people you're interacting with. If a plan is going to have value, it is important to take the time to develop it correctly.

Be prepared, do your homework on the business line, and be available to answer questions and provide feedback. Managing expectations of your executive teams by factoring in sufficient buffer for unexpected delays will take pressure off both you and the service lines you are helping to create a plan with.



### 2. Always include IT

IT plays a crucial role in almost all critical business services today. It is important that they are a partner in the development of any Business Continuity Plan. Business lines are sometime unaware of the alternatives available to them should their primary systems become unavailable. The IT support team will help guide business on what IT can and cannot do to support them.

## De la confusion à la clarté : quatre conseils pour élaborer un meilleur plan

Entreprendre l'élaboration d'un plan de continuité des activités peut s'avérer une entreprise intimidante, qui comporte de nombreuses difficultés potentielles. En suivant quelques pratiques de planification clés décrites ci-dessous, vous pouvez éviter certains des pièges de la planification.



### 1. Cela prendra plus de temps que prévu

Même la meilleure planification de projet survit rarement au premier contact avec les réalités de l'entreprise. Lors de l'élaboration de vos calendriers, veillez à prévoir une marge suffisante pour tenir compte des variables que vous ne pouvez pas contrôler.

Il est important de connaître les périodes de pointe ou de traitement critique pour vos secteurs d'activité et la disponibilité du personnel. Ce n'est pas parce qu'il s'agit d'une priorité pour vous qu'il s'agit de la priorité de vos interlocuteurs. Pour qu'un plan ait de la valeur, il est important de prendre le temps de l'élaborer correctement.

Préparez-vous, faites vos devoirs sur le secteur d'activité et soyez disponible pour répondre aux questions et fournir un retour d'information. Gérer les attentes de vos équipes de direction en prévoyant une marge de manœuvre suffisante pour les retards imprévus vous soulagera, ainsi que les lignes de service avec lesquelles vous aidez à élaborer un plan.



### 2. Toujours inclure l'informatique

Aujourd'hui, les technologies de l'information jouent un rôle crucial dans presque tous les services essentiels des entreprises. Il est important qu'elles soient un partenaire dans l'élaboration de tout plan de continuité des activités. Les entreprises ignorent parfois les alternatives qui s'offrent à elles en cas d'indisponibilité de leurs systèmes principaux. L'équipe d'assistance informatique aidera à guider les entreprises sur ce que l'informatique peut et ne peut pas faire pour les aider.

En tant que planificateur, une bonne compréhension du processus de gestion des incidents informatiques,

As a planner, a good understanding of the IT incident management process, the methods in which systems outages can be reported, and how escalation and client interaction operate will allow you to better explain the process—as well as timelines to recover. Providing business lines with the broader picture of the processes IT follow to restore their key systems will result in fewer escalations and requests for status reports and updates. IT can then focus on system restoration instead of wasting time on extensive reporting.



### 3. Communication is crucial

Two areas of communication factor into the development of a good plan: the planning process and the content of the plan itself.

Presenting a clear understanding of the scope and objectives, as well as expectations of the service line, during the plan development phase will result in a better product and accelerate the development cycle. A BCM practitioner's role is to work closely with their clients to collect information, guide recovery strategies, and develop a useable plan for their clients. Frequent and ongoing collaboration throughout the process is necessary.

When examining plan content, ensure that management, support teams, suppliers, customers, and anyone else impacted by an outage are aware and clearly understand the issues being addressed. This will make it more likely that an organization retains

customers after the event. A plan should identify the decision-making internal teams, as well as the teams they need to work with, in order to ensure accurate information is being communicated to all stakeholders. A strong communication strategy will save time and customers.



### 4. Interviews are essential

Nothing can replace an interactive interview to gain insights into the inner working of a service and provide those vital bits of information that can help you guide your business lines in developing the most effective recovery strategies.

Plan development is a collaborative process between the practitioner and the client. Even if you leverage BCM software, or are part of a large organization, interviews should be included as a fundamental tool in your plan development.

This process must result in appropriate recovery strategies, communication and escalation process, and a clear understanding of the client's roles and responsibilities in response to a disaster. The interview process can act as both an information-gathering mechanism and a training opportunity. These interactions also serve a third, and very important purpose: they introduce the BCM teams to the organization, putting a face to the team and creating relationships with the clients you are supporting. Take every opportunity you can to interact with your clients. Ω

### ABOUT THE AUTHOR

#### Jason Firlotte

**MBCP, CBRM, MBCI, CSP, CBCV**

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.



des méthodes par lesquelles les pannes de systèmes peuvent être signalées et de la manière dont fonctionnent l'escalade et l'interaction avec les clients vous permettra de mieux expliquer le processus, ainsi que les délais de rétablissement. En donnant aux lignes d'affaires une vue d'ensemble des processus suivis par l'informatique pour restaurer leurs systèmes clés, vous réduirez le nombre d'escalades et de demandes de rapports d'état et de mises à jour. Le service informatique peut alors se concentrer sur la restauration des systèmes au lieu de perdre du temps à établir des rapports détaillés.



### 3. La communication est essentielle

Deux domaines de communication entrent en ligne de compte dans l'élaboration d'un bon plan : le processus de planification et le contenu du plan lui-même

Une bonne compréhension de la portée et des objectifs, ainsi que des attentes de la ligne de service, au cours de la phase d'élaboration du plan, permettra d'obtenir un meilleur produit et d'accélérer le cycle d'élaboration. Le rôle d'un praticien BCM est de travailler en étroite collaboration avec ses clients pour collecter des informations, guider les stratégies de récupération et développer un plan utilisable pour leurs clients. Une collaboration fréquente et continue tout au long du processus est nécessaire.

## À PROPOS DE L'AUTEUR

**Jason Firlotte**  
**MBCP, CBRM, MBCI, CSP, CBCV**

*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.*

Lors de l'examen du contenu du plan, il convient de s'assurer que la direction, les équipes d'assistance, les fournisseurs, les clients et toute autre personne touchée par une panne sont conscients des problèmes abordés et les comprennent clairement. Il est ainsi plus probable qu'une organisation conserve ses clients après l'événement. Un plan doit identifier les équipes internes qui prennent les décisions, ainsi que les équipes avec lesquelles elles doivent travailler, afin de s'assurer que des informations précises sont communiquées à toutes les parties prenantes. Une stratégie de communication solide permettra de gagner du temps et d'épargner des clients.

### 4. Les entretiens sont essentiels

Rien ne peut remplacer un entretien interactif pour comprendre le fonctionnement interne d'un service et fournir les éléments d'information essentiels qui vous aideront à guider vos secteurs d'activité dans l'élaboration des stratégies de recouvrement les plus efficaces.



L'élaboration d'un plan est un processus de collaboration entre le praticien et le client. Même si vous utilisez un logiciel de gestion de la continuité des activités ou si vous faites partie d'une grande organisation, les entretiens doivent être un outil fondamental dans l'élaboration de votre plan.

Ce processus doit aboutir à des stratégies de récupération appropriées, à un processus de communication et d'escalade, et à une compréhension claire des rôles et des responsabilités du client en cas de catastrophe. Le processus d'entretien peut servir à la fois de mécanisme de collecte d'informations et d'opportunité de formation. Ces interactions ont également un troisième objectif, très important : elles présentent les équipes BCM à l'organisation, en donnant un visage à l'équipe et en créant des relations avec les clients que vous soutenez. Saisissez toutes les occasions qui s'offrent à vous pour interagir avec vos clients.

Ω

# CRISIS COMMUNICATIONS

## COMMUNICATIONS DE CRISE

*By/Par Mark Hoffman, CBCP, MBCI*

### Why You Need to Care About Crisis Communications

**A**t first glance, the first eight DRI Professional Practices fit together like fingers on a glove. They are logical. They flow and build on one another. But the last two appear to be just...a little bit different. They're not completely outside the discipline of a strong Business Continuity Management Program, but they do stand out. Like a thumb. Still on the glove, but just a little bit different. They're so different that many in our profession, who excel at the first eight, don't always engage

### Pourquoi vous devez vous préoccuper de la communication de crise

**À** première vue, les huit premières pratiques professionnelles de la DRI s'emboîtent comme les doigts d'un gant. Elles sont logiques. Elles s'enchaînent et s'appuient les unes sur les autres. Mais les deux dernières semblent être... un peu différentes. Elles ne sont pas complètement en dehors de la discipline d'un

with the final two. We think of them as adjacent to our day-to-day role in ‘business continuity’. But they aren’t. Maybe we’ll address PPI0 – Coordination with External Agencies and Resources another time, but for now I want us to focus on PP9 – Crisis Communications.

The highlights of PP9 are pretty clear:

- Create and maintain a crisis communications plan
- Ensure that the plan provides for timely, effective communication with internal and external parties.

Simple, right? Well, let’s walk through what this communications plan looks like and what you should be covering in it.

I have been writing crisis communications plans (I call them “guidelines”, but hey, some say toMAYto, others say toMAHto) for several years. I will admit that I suffered a bit of “imposter syndrome” for a while, until one day, a client sent my plan off to a local public relations firm for a detailed review. Surely, I would be exposed for being in over my head, for writing outside of my scope of knowledge. But no! Not only had the PR firm accepted the premise of my document, but they also validated it AND agreed with the principles and the content. I no longer felt inferior in this area of work. Neither should you.

### Laying Out the Plan

I like to start my crisis communications plan with an Introduction section that establishes the goals, scope and rules of engagement. In short, it’s important to establish HOW the organization is going to communicate during a crisis, WHO is developing the statements, WHAT tools they are going to leverage and WHEN the statements will be delivered. I typically run a crisis management decisions workshop in conjunction with the communications plan writing, to understand the leadership team’s preferences in terms of timing and audience.

solide programme de gestion de la continuité des activités, mais elles se distinguent. Comme un pouce. Toujours sur le gant, mais juste un peu différent. Elles sont si différentes que de nombreux professionnels, qui excellent dans les huit premières, ne s’intéressent pas toujours aux deux dernières.

Nous pensons qu’ils sont adjacents à notre rôle quotidien dans la “continuité des affaires”. Mais ce n’est pas le cas. Nous aborderons peut-être le PPI0 - Coordination avec les agences et ressources externes une autre fois, mais pour l’instant, je souhaite que nous nous concentrons sur le PP9 - Communication de crise.

Les points forts du PP9 sont assez clairs :

- Créer et maintenir un plan de communication de crise
- Veiller à ce que le plan prévoie une communication efficace et en temps utile avec les parties internes et externes.

C’est simple, non ? Voyons à quoi ressemble ce plan de communication et ce qu’il doit contenir.

Cela fait plusieurs années que je rédige des plans de communication de crise (que j’appelle des “lignes directrices”, mais bon, certains disent deMAYto, d’autres deMAHto). Je dois admettre que j’ai souffert un peu du “syndrome de l’imposteur” pendant un certain temps, jusqu’au jour où un client a envoyé mon plan à un cabinet de relations publiques local pour qu’il l’examine en détail. J’allais certainement être dénoncé pour avoir été dépassé par les événements, pour avoir écrit en dehors de mon champ de connaissances. Mais non ! Non seulement le cabinet de relations publiques avait accepté les prémisses de mon document, mais il l’avait également validé ET approuvé les principes et le contenu. Je ne me suis plus sentie inférieure dans ce domaine. Vous non plus, d’ailleurs.



## Implementing the Professional Practices

In the Introduction, I like to establish the principles that will be followed when communicating during a crisis. For example, it's important to establish certain pillars which our statements will be based on, including honesty, authenticity, responsiveness and the use of clear language.

I like to define the clear objectives of crisis communication: to effectively manage the crisis and protect the organization's reputation and public trust.

Then I move on to the rest of the document, which has seven main goals:

- To identify a communications strategy for the type of crisis at hand
- To establish a trigger point for its execution
- To define communication tactics during a crisis
- To establish core messaging
- To define the statement drafting and approval process
- To prepare communicators for questions from stakeholders
- To prepare drafted templates for key audiences

I'll walk you through each one:

### Strategy

Before I get to strategy definition, let me explain what I mean by "the type of crisis at hand". I will typically write ONE communication plan, but it will have multiple playbooks depending on the type of crisis I'm writing for. I would use a different strategy for a data breach than I would for a natural disaster. My tone might be different when employees are injured than in response to a labour disruption. Each type of crisis will need its own strategy. They should always be centred around our guiding principles, but things like timing and audience (for example) may differ.

I typically summarize the strategy with three or four bullet points that address timing of messaging, establish tone, define the audience, etc. In the event of a very public disaster, I always like to make sure that the leadership team is very visible.



## Mise en place du plan

J'aime commencer mon plan de communication de crise par une section Introduction qui définit les objectifs, la portée et les règles d'engagement. En bref, il est important d'établir COMMENT l'organisation va communiquer pendant une crise, QUI va élaborer les déclarations, QUELS outils elle va utiliser et QUAND les déclarations seront diffusées. J'organise généralement un atelier sur les décisions en matière de gestion de crise parallèlement à la rédaction du plan de communication, afin de comprendre les préférences de l'équipe dirigeante en termes de calendrier et d'audience.

Dans l'introduction, j'aime établir les principes qui seront suivis lors de la communication en temps de crise. Par exemple, il est important d'établir certains piliers sur lesquels nos déclarations seront basées, notamment l'honnêteté, l'authenticité, la réactivité et l'utilisation d'un langage clair.

J'aime définir les objectifs clairs de la communication de crise : gérer efficacement la crise et protéger la réputation de l'organisation et la confiance du public.

Je passe ensuite au reste du document, qui comporte sept objectifs principaux :

- Identifier une stratégie de communication pour le type de crise en question
- Établir un point de déclenchement pour son exécution
- Définir les tactiques de communication en cas de crise
- Établir un message de base
- Définir le processus de rédaction et d'approbation de la déclaration
- Préparer les communicateurs aux questions des parties prenantes
- Préparer des modèles de rédaction pour les publics clés

Je vais vous présenter chacun d'entre eux :

### Stratégie

Avant d'aborder la définition de la stratégie, permettez-moi d'expliquer ce que j'entends par "le type de crise en question". En règle générale, je

rédige UN plan de communication, mais ce plan comprendra plusieurs scénarios en fonction du type de crise pour lequel j'écris. Je n'utiliserai pas la même stratégie pour une violation de données que pour une catastrophe naturelle. Mon ton peut être différent selon que les employés sont blessés ou qu'il s'agit d'une interruption de travail. Chaque type de crise nécessite sa propre stratégie. Elles doivent toujours être axées sur nos principes directeurs, mais des éléments tels que le moment et le public (par exemple) peuvent différer.

Je résume généralement la stratégie en trois ou quatre points qui traitent du moment de la diffusion des messages, du ton, de la définition du public, etc. En cas de catastrophe très médiatisée, j'aime toujours m'assurer que l'équipe dirigeante est très visible.

### Déclencheur

Étant donné que mon document couvre généralement plusieurs types de crises, j'aime préciser ce que chaque manuel couvre. Par exemple, je propose deux manuels différents pour un incident de cybersécurité et une atteinte à la protection des données. Un incident au cours duquel des données personnelles ont été exfiltrées nécessite un tout autre niveau de communication. Alors qu'un cyberincident tel qu'une attaque par déni de service ou une attaque par ransomware, où les systèmes sont mis hors service, peut conduire à une interruption de service irritable, une violation de données peut entraîner des dommages importants. C'est pourquoi mon plan de communication de crise comporte deux sections. Je m'assure que le déclencheur définit quand utiliser chaque section.

### Tactique

Alors que la section sur la stratégie fait référence à la conception générale des communications, les tactiques établissent les actions et techniques spécifiques qui seront utilisées pour mettre en œuvre la stratégie. Toujours très axé sur les points, j'établis les choses spécifiques à faire pour communiquer efficacement en interne et en externe.





## Trigger

Since my document typically covers multiple crisis types, I like to make it clear what each playbook covers. For example, I typically provide two different playbooks for a cybersecurity incident and a data breach. An incident where personal data has been exfiltrated, requires a whole other level of communication. Where a cyber incident like a denial-of-service attack or ransomware attack where systems are taken down may lead to an irritable service interruption, a data breach can lead to significant harm. As a result, there are two sections in my crisis communications plan. I make sure the trigger defines when to use each section.

## Tactics

While the strategy section refers to the overall design of the communications, the tactics establish the specific actions and techniques that will be used to implement the strategy. Still very bullet driven, I establish specific things to be done to effectively communicate internally and externally. This is a good place to define who is responsible for delivering messages to various stakeholders. You may want to include specific language to use or avoid while using this plan. For example, I always include very clear instructions not to randomly throw around the word “breach” during a ransomware attack. “Breach” should only be used when data has been exposed.

## Core Messaging

Core messaging is used to keep the communicator on point. If they are asked a question that may trip them up, they should always refer to one of the core messages defined in this section. Core messages can include talking points specific to the crisis (“we are investigating a cybersecurity incident”), important things about your organization (“we are committed to the highest level of customer satisfaction, as has been our priority for the past 30 years”) and the fluid nature of the incident (“the situation is still evolving”). The trick

Il s'agit d'un bon endroit pour définir qui est responsable de la transmission des messages aux différentes parties prenantes. Vous pouvez inclure des termes spécifiques à utiliser ou à éviter dans le cadre de ce plan. Par exemple, je donne toujours des instructions très claires pour que le mot "violation" ne soit pas utilisé au hasard lors d'une attaque par ransomware. "Ce terme ne doit être utilisé que lorsque des données ont été exposées.

### Messagerie de base

Les messages clés sont utilisés pour que le communicateur ne s'écarte pas du sujet. Si on lui pose une question qui risque de le déconcerter, il doit toujours se référer à l'un des messages clés définis dans cette section. Les messages clés peuvent inclure des points de discussion spécifiques à la crise ("nous enquêtons sur un incident de cybersécurité"), des éléments importants concernant votre organisation ("nous nous engageons à satisfaire au mieux nos clients, comme c'est notre priorité depuis 30 ans") et la nature fluide de l'incident ("la situation évolue encore"). L'astuce avec les messages clés est qu'ils doivent être rédigés et prononcés de manière à ne pas donner l'impression d'être indifférents ou surutilisés. La dernière chose que vous voulez, c'est

que votre déclaration ressemble à cette voix agaçante à l'autre bout d'un appel téléphonique interminable ("votre appel est important pour nous, veuillez continuer à patienter"). Un message essentiel souvent négligé est une version plus professionnelle de "Je ne sais pas". Étant donné que la situation évolue encore, il est très probable que votre porte-parole ne sache pas tout ce qu'il y a à savoir. N'hésitez pas à l'intégrer dans votre message principal.

### Rédaction et approbation de la déclaration

Celui-ci est simple. Il s'agit de quelques lignes qui définissent qui est autorisé à rédiger des déclarations et à gérer les appels entrants pendant une crise. Avant tout, vous devez contrôler le message ! Établissez la règle de base selon laquelle seule votre équipe de communication peut rédiger des déclarations. Cela permettra à votre organisation de publier des déclarations cohérentes en termes de style et de contenu. Les déclarations devront peut-être être approuvées par l'équipe de gestion de crise ou par le service juridique. Établissez des règles pour la prise d'appels des parties prenantes et veillez à ce qu'il soit clairement établi qui est autorisé à répondre aux questions. Assurez-vous que



with core messages is that they need to be written and spoken in a way that doesn't come off as uncaring or overused. The last thing you want is for your statement to sound like that annoying voice on the other end of unending phone call; ("your call is important to us, please continue to hold"). One core message that is often overlooked is a more professional version of "I don't know". Since the situation is still evolving, it is very likely that your spokesperson may not know everything there is to know. Feel free to build that into your core message.

### Statement Drafting and Approval

This one is simple. It's a couple of lines that defines who is allowed to write statements and handle incoming calls during a crisis. Above all, you must control the message! Establish the ground rule that only your communications team can draft statements. This will enable your organization to issue statements that are consistent in terms of style and content. Statements may need to be approved by the crisis management team or Legal. Establish rules for taking calls from stakeholders and makes sure it's clear who is allowed to answer questions. Be sure that employees understand that questions from the press must go through the communications team.

### Prepare Your Communicators

This was the section that made me nervous when my client sent my plan to the PR firm for review. In the Q&A section, I build a list of likely / potential questions that our communicators may be asked, and then provide talking points or prompts for each one. The idea is that your communications team will need to work with your company spokesperson and other public facing employees to prepare them for tough questions. I would encourage you to think like a reporter and ask the most vicious questions you can think of. Watch the news and get a feel for how a reporter thinks. It's not often that a reporter asks

about what happened. They want to know what you're NOT telling them – who is to blame and how bad things really are. Make sure your spokesperson and all customer facing teams know how to answer these questions!

### Templates

One of the core principles of PP9 is that we are able to communicate effectively and in a timely manner. The best way to do that is to write the statement ahead of time. Build your statement according to your principles, strategies and tactics. Leave room for the specific details of the incident. Include a placeholder for a quote from the CEO or another member of the leadership team.

Give thought to the types of statements you'll need for each type of crisis. Consider a holding statement, updates, memos to employees, communication to the Board and statements to other key stakeholders.

### Conclusion

In summary, while crisis communications may feel a bit outside your comfort zone, the principles of creating a communications plan build on the information already established in your program. Don't be intimidated. Rely on subject matter experts and be willing to collaborate. Be open to feedback. In short – get writing. Ω

---

### About Mark Hoffman

*Mark is an award-winning Business Continuity and Crisis Management Consultant based just north of Toronto. He and his wife Cheryl run a boutique consulting firm with clients across North America, the Caribbean and Europe.*

*He has worked in the Business Continuity industry for nearly 25 years.*

*Mark is the host of The Resilient Journey podcast, which covers topics related to making organizations and people more resilient. The podcast is available across all major streaming services.*

*Mark is a Co-founder and Managing Partner of the Resilience Think Tank.*

les employés comprennent que les questions de la presse doivent passer par l'équipe de communication.

### Préparez vos communicateurs

C'est cette section qui m'a rendu nerveux lorsque mon client a envoyé mon plan à l'agence de relations publiques pour qu'elle le révise. Dans la section "Questions et réponses", je dresse une liste des questions probables ou potentielles qui pourraient être posées à nos communicateurs, puis je fournis des points de discussion ou des incitations pour chacune d'entre elles. L'idée est que votre équipe de communication devra travailler avec le porte-parole de votre entreprise et d'autres employés en contact avec le public pour les préparer à répondre à des questions difficiles. Je vous encourage à penser comme un journaliste et à poser les questions les plus vicieuses qui vous viennent à l'esprit. Regardez les journaux télévisés et faites-vous une idée de la façon dont un journaliste pense. Il est rare qu'un journaliste demande ce qui s'est passé. Il veut savoir ce que vous ne lui dites PAS - qui est à blâmer et quelle est la gravité de la situation. Assurez-vous que votre porte-parole et toutes les équipes en contact avec la clientèle savent comment répondre à ces questions !



### Modèles

L'un des principes fondamentaux de la PP9 est de pouvoir communiquer efficacement et en temps utile. Le meilleur moyen d'y parvenir est de rédiger la déclaration à l'avance. Construisez votre déclaration en fonction de vos principes, stratégies et tactiques. Laissez de la place pour les détails spécifiques de l'incident. Prévoyez un espace pour une citation du PDG ou d'un autre membre de l'équipe de direction.

Réfléchissez aux types de déclarations dont vous aurez besoin pour chaque type de crise. Envisagez une déclaration d'attente, des mises à jour, des notes de service aux employés, une communication au conseil d'administration et des déclarations à d'autres parties prenantes clés.

### Conclusion

En résumé, même si les communications de crise vous semblent un peu en dehors de votre zone de confort, les principes de la création d'un plan de communication s'appuient sur les informations déjà établies dans votre programme. Ne vous laissez pas intimider. Appuyez-vous sur des experts en la matière et soyez prêt à collaborer. Soyez ouvert au retour d'information. En bref – commencez à écrire. Ω

### À propos de Mark Hoffman

*Mark est un consultant primé en continuité des activités et en gestion de crise, basé au nord de Toronto. Avec sa femme Cheryl, il dirige un cabinet de conseil qui compte des clients en Amérique du Nord, dans les Caraïbes et en Europe.*

*Il travaille dans le secteur de la continuité des activités depuis près de 25 ans.*

*Mark est l'animateur du podcast The Resilient Journey, qui traite de sujets liés à l'amélioration de la résilience des organisations et des personnes. Le podcast est disponible sur tous les principaux services de streaming.*

*Mark est cofondateur et associé directeur du Resilience Think Tank.*

# The Vitality of Emergency Preparedness and Business Continuity Management in Healthcare Sectors

# La vitalité de la préparation aux situations d'urgence et de la gestion de la continuité des activités dans les secteurs des soins de santé

*By/Par Nix George, ABCP*

**A**S I work through solutions as a Regional Coordinator in a Healthcare environment under the discipline of Emergency Preparedness, Continuity Management and Security Services. I often run into situations where I am always explaining why Emergency planning and continuity management is important. A response that I get on a regular basis is “We have been through it before; we can manage that; we can do anything” even if it is last minute planning. However, if we can be proactive, we can mitigate those risks identified prior to an incident occurring rather than an incident occurring and then learning. Let me explain. Imagine your organization as a human body and consider as if:

## **Emergency planning as the Immune System**

The immune system handles protecting against harmful invaders. Similarly, emergency

**E**tant que coordonnateur régional dans un environnement de soins de santé, je travaille sur des solutions dans le domaine de la préparation aux situations d'urgence, de la gestion de la continuité et des services de sécurité. Je me retrouve souvent dans des situations où je dois expliquer pourquoi la planification des urgences et la gestion de la continuité sont importantes. La réponse que je reçois régulièrement est la suivante : “Nous sommes déjà passés par là ; nous pouvons gérer cela ; nous pouvons tout faire”, même s’il s’agit d’une planification de dernière minute. Cependant, si nous sommes proactifs, nous pouvons atténuer les risques identifiés avant qu’un incident ne se produise, plutôt que de subir un incident et d’en tirer des leçons. Je m’explique. Imaginez votre organisation comme un corps humain et considérez si -



preparedness in an organization involves measures and protocols that are put in place to protect against various threats such as natural disasters, cyberattacks, or pandemics. Just as the immune system employs different cells and mechanisms to respond to diverse types of threats, emergency preparedness plans include diverse strategies tailored to all types of emergencies.

### **Continuity management as your central nervous system**

The central nervous system (CNS) is made up of the brain and spinal cord, coordinates, and controls bodily functions. Similarly, business continuity management (BCM) serves as the core system that coordinates and ensures the continued functioning of an organization during disruptions. Like the CNS, which integrates signals from various parts of the body to keep homeostasis, BCM integrates

### **Les plans d'urgence comme le système immunitaire.**

Le système immunitaire assure la protection contre les envahisseurs nuisibles. De même, la préparation aux situations d'urgence dans une organisation implique des mesures et des protocoles mis en place pour se protéger contre diverses menaces telles que les catastrophes naturelles, les cyberattaques ou les pandémies. Tout comme le système immunitaire utilise différentes cellules et différents mécanismes pour répondre à divers types de menaces, les plans de préparation aux situations d'urgence comprennent diverses stratégies adaptées à tous les types de situations d'urgence.

La gestion de la continuité est votre système nerveux central. Le système nerveux central (SNC) est constitué du cerveau et de la moelle épinière, il coordonne et contrôle les



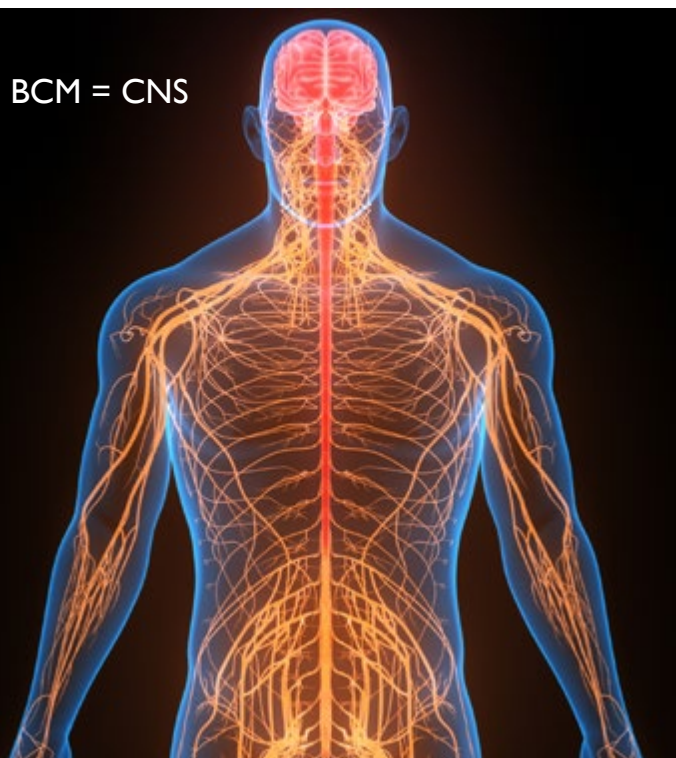
strategies, resources, and stakeholders to sustain critical operations and minimize downtime during crises.

### **Hazard risk assessment as your Sensory Input**

This is where the human body constantly receives sensory input to assess the environment and potential threats. Likewise, risk assessment in emergency preparedness and BCM involves evaluating potential hazards, vulnerabilities, and affects to decide initiative-taking measures. Like how the CNS processes sensory information to guide actions, risk assessment informs decision-making in emergency and continuity planning to prioritize resources and strategies.

### **And training, exercise, and drills as your Muscle Memory**

Practice and repetition help develop muscle memory in physical activities. Similarly, regular training, simulations, and drills in emergency preparedness and BCM instill familiarity and readiness among personnel, enabling them to respond effectively under stress. Just as muscle memory allows for quick and automatic responses in physical tasks, well-trained teams can execute predefined



protocols efficiently during crises, reducing errors and improving overall resilience.

In a complex web of healthcare provision, where every decision directly affects human lives, the significance of robust emergency planning and business continuity management cannot be overstated. Also, having a team or an assigned management group that can deliver this on a constant and consistent basis. Healthcare sectors worldwide face a myriad of challenges, from natural disasters to pandemics and cyberattacks, all of which can disrupt operations and compromise patient care. In this article, we delve into the relevance and necessity of emergency planning and business continuity management within healthcare sectors, emphasizing their pivotal role in ensuring resilience, safeguarding patient welfare, and keeping operational efficiency.

Emergency planning in healthcare involves the anticipation, preparation, response, and recovery from crises and disasters. Whether it is a sudden surge in patient volume, a cyber breach compromising sensitive data, or a natural calamity disrupting infrastructure, effective emergency planning lays the groundwork for prompt and coordinated responses. Primarily, emergency planning fosters initiative-taking risk assessment and mitigation strategies. By finding potential hazards and vulnerabilities prior to an incident occurring, healthcare organizations can implement preventive measures to minimize the impact of emergencies. This includes developing evacuation protocols, ensuring adequate medical supply reserves, and setting up communication channels for rapid response coordination. Moreover, emergency planning cultivates a culture of preparedness among healthcare professionals. Regular drills and training exercises familiarize staff with emergency procedures, empowering them to act decisively in high-pressure situations. Quick and informed decision-making during crises can significantly mitigate risks and save lives.

fonctions corporelles. De même, la gestion de la continuité des activités (BCM) est le système central qui coordonne et assure le fonctionnement continu d'une organisation en cas de perturbations. Comme le SNC, qui intègre les signaux provenant de différentes parties du corps pour maintenir l'homéostasie, la GCA intègre les stratégies, les ressources et les parties prenantes pour maintenir les opérations critiques et minimiser les temps d'arrêt en cas de crise.

### **L'évaluation des risques liés aux dangers est considérée comme un apport sensoriel.**

Le corps humain recevant en permanence des informations sensorielles pour évaluer l'environnement et les menaces potentielles. De même, l'évaluation des risques dans le cadre de la préparation aux situations d'urgence et de la gestion de la continuité implique l'évaluation des dangers potentiels, des vulnérabilités et des effets afin de décider des mesures à prendre. Tout comme le SNC traite les informations sensorielles pour guider les actions, l'évaluation des risques informe la prise de décision dans les plans d'urgence et de continuité afin de hiérarchiser les ressources et les stratégies.

### **Et la formation, les exercices et les entraînements comme mémoire musculaire.**

La pratique et la répétition aident à développer la mémoire musculaire dans les activités physiques. De même, une formation, des simulations et des exercices réguliers en matière de préparation aux situations d'urgence et de gestion de la continuité des activités permettent au personnel de se familiariser et d'être prêt, ce qui lui permet de réagir efficacement en cas de stress. Tout comme la mémoire musculaire permet des réponses rapides et automatiques dans les tâches physiques, des équipes bien formées peuvent exécuter efficacement des protocoles prédéfinis pendant les crises, réduisant ainsi les erreurs et améliorant la résilience globale.

Dans un réseau complexe de soins de santé, où chaque décision affecte directement des vies humaines, on ne saurait trop insister sur

l'importance d'une planification d'urgence solide et d'une gestion de la continuité des activités. Il est également important de disposer d'une équipe ou d'un groupe de gestion capable de fournir ces services de manière constante et cohérente. Les secteurs de la santé du monde entier sont confrontés à une myriade de défis, des catastrophes naturelles aux pandémies en passant par les cyberattaques, qui peuvent tous perturber les opérations et compromettre les soins aux patients. Dans cet article, nous examinons la pertinence et la nécessité des plans d'urgence et de la gestion de la continuité des activités dans les secteurs de la santé, en soulignant leur rôle essentiel dans la résilience, la protection du bien-être des patients et le maintien de l'efficacité opérationnelle.

La planification d'urgence dans le secteur des soins de santé implique l'anticipation, la préparation, la réponse et le rétablissement en cas de crise ou de catastrophe. Qu'il s'agisse d'une augmentation soudaine du nombre de patients, d'une cyber-faillie compromettant des données sensibles ou d'une catastrophe naturelle perturbant l'infrastructure, une planification d'urgence efficace jette les bases d'une réponse rapide et coordonnée. La planification des urgences favorise avant tout la prise d'initiatives en matière d'évaluation des risques et de stratégies d'atténuation. En identifiant les risques potentiels et les vulnérabilités avant qu'un incident ne se produise, les organismes de santé peuvent mettre en œuvre des mesures préventives pour minimiser l'impact des situations d'urgence. Il s'agit notamment d'élaborer des protocoles d'évacuation, de garantir des réserves de fournitures médicales adéquates et de mettre en place des canaux de communication pour une coordination rapide des interventions. En outre, la planification des urgences permet de cultiver une culture de la préparation parmi les professionnels de la santé. Des exercices réguliers et des formations familiarisent le personnel avec les procédures d'urgence, ce qui lui permet d'agir de manière décisive dans des situations de forte pression. Une prise de décision rapide et éclairée en cas de crise peut considérablement atténuer les risques et sauver des vies.




While emergency planning focuses on immediate responses to crises, business continuity management (BCM) encompasses broader strategies for keeping essential functions and services during disruptions. In the healthcare sector, where uninterrupted patient care is paramount, BCM plays a pivotal role in mitigating operational downtime and ensuring service continuity. A fundamental aspect of BCM is the development of comprehensive continuity plans tailored to healthcare-specific risks and dependencies. These plans outline alternative workflows, backup systems, and resource allocation strategies to sustain critical operations amidst disruptions. For example, setting up redundant IT systems and cloud-based data storage can mitigate the impact of cyberattacks or system failures on patient care delivery. Furthermore, BCM involves setting up robust supply chain resilience mechanisms to safeguard against shortages of vital medical supplies and pharmaceuticals. By diversifying suppliers, stockpiling essential resources, and setting up contingency agreements, healthcare organizations can mitigate the impact of supply chain disruptions on patient care.

Even though emergency planning and BCM are distinct disciplines, their constructive integration and collaboration is essential for comprehensive risk management in healthcare sectors. Integrating emergency planning into broader BCM frameworks ensures alignment of response strategies with overarching organizational goals. This integration eases seamless transitions from emergency response to recovery and enables healthcare organizations to adapt and evolve in the face of evolving threats. Likewise, effective emergency planning and BCM rely on interdisciplinary collaboration and stakeholder engagement. Healthcare providers, government agencies, community organizations, and private sector partners must collaborate to develop holistic and inclusive emergency

Alors que les plans d'urgence se concentrent sur les réponses immédiates aux crises, la gestion de la continuité des activités (BCM) englobe des stratégies plus larges visant à maintenir les fonctions et les services essentiels pendant les perturbations. Dans le secteur des soins de santé, où il est primordial de prodiguer des soins ininterrompus aux patients, la gestion de la continuité des activités joue un rôle essentiel pour atténuer les temps d'arrêt des opérations et garantir la continuité des services. L'un des aspects fondamentaux de la gestion de la continuité des opérations est l'élaboration de plans de continuité complets adaptés aux risques et aux dépendances propres au secteur des soins de santé. Ces plans décrivent des flux de travail alternatifs, des systèmes de sauvegarde et des stratégies d'allocation des ressources pour soutenir les opérations critiques en cas de perturbations. Par exemple, la mise en place de systèmes informatiques redondants et d'un stockage de données dans le nuage peut atténuer l'impact des cyberattaques ou des pannes de système sur la prestation des soins aux patients. En outre, la gestion de la continuité des soins implique la mise en place de solides mécanismes de résilience de la chaîne d'approvisionnement afin de se prémunir contre les pénuries de fournitures médicales et de produits pharmaceutiques vitaux. En diversifiant les fournisseurs, en stockant les ressources essentielles et en mettant en place des accords d'urgence, les organismes de santé peuvent atténuer l'impact des perturbations de la chaîne d'approvisionnement sur les soins aux patients.

Bien que les plans d'urgence et la gestion des crises soient des disciplines distinctes, leur intégration et leur collaboration constructives sont essentielles pour une gestion globale des risques dans le secteur des soins de santé. L'intégration des plans d'urgence dans des cadres plus larges de gestion des crises garantit l'alignement des stratégies de réponse sur les objectifs généraux de l'organisation. Cette intégration facilite les transitions entre l'intervention d'urgence et le rétablissement et permet aux organismes de santé de s'adapter et d'évoluer face à des menaces en constante évolution. De même, l'efficacité de la planification des urgences et de la gestion des crises repose sur la collaboration interdisciplinaire et l'engagement des parties prenantes. Les prestataires de soins de santé, les agences gouvernementales, les organisations communautaires et les partenaires du secteur privé doivent collaborer

preparedness initiatives. By sharing resources, ability, and best practices, stakeholders can enhance collective resilience and foster a unified response to emergencies.

In conclusion, emergency Preparedness and Business Continuity Management can be related to the immune system and central nervous system, respectively, in how they predict, respond to, and recover from disruptions, safeguarding the well-being and continuity of your organizations. In an era defined by unprecedented challenges and uncertainties, the relevance of emergency planning and business continuity management in healthcare sectors cannot be overstated, especially with a resolute team and resources that includes a financial budget. By fostering a culture of preparedness, enhancing operational resilience, and promoting collaboration across stakeholders, emergency planning and BCM are indispensable tools for safeguarding patient welfare and ensuring continuity of care in the face of adversity. As healthcare sectors continue to evolve, investing in robust emergency planning and BCM capabilities will remain a cornerstone of sustainable and patient-centric healthcare delivery. 


---

### ABOUT THE AUTHOR

**Nix George** is a seasoned professional with over a decade of combined experience in these fields, Nix has proven a strong commitment to enhancing organizational resilience and safeguarding assets in the face of diverse threats and challenges. Nix's journey in emergency management began with a passion for ensuring public safety and disaster preparedness. He is ABCP certified from DRI, currently working as a Regional Coordinator for Health Emergency Management, Business Continuity Management (BCM) and Security Services with Newfoundland and Labrador Health Services (NLHS), Canada.



pour développer des initiatives holistiques et inclusives de préparation aux situations d'urgence. En partageant les ressources, les capacités et les meilleures pratiques, les parties prenantes peuvent améliorer la résilience collective et favoriser une réponse unifiée aux situations d'urgence.

En conclusion, la préparation aux situations d'urgence et la gestion de la continuité des activités peuvent être assimilées respectivement au système immunitaire et au système nerveux central, dans la manière dont ils prévoient les perturbations, y répondent et s'en remettent, sauvegardant ainsi le bien-être et la continuité de vos organisations. À une époque définie par des défis et des incertitudes sans précédent, la pertinence de la planification d'urgence et de la gestion de la continuité des activités dans les secteurs de la santé ne peut être surestimée, en particulier avec une équipe résolue et des ressources qui incluent un budget financier. En favorisant une culture de la préparation, en améliorant la résilience opérationnelle et en promouvant la collaboration entre les parties prenantes, la planification d'urgence et la gestion de la continuité des activités sont des outils indispensables pour préserver le bien-être des patients et assurer la continuité des soins face à l'adversité. Alors que les secteurs de la santé continuent d'évoluer, l'investissement dans de solides capacités de planification d'urgence et de gestion des crises restera la pierre angulaire d'une prestation de soins de santé durable et centrée sur le patient. 

---

### À PROPOS DE L'AUTEUR

Nix George est un professionnel chevronné qui possède des années d'expérience combinée dans ces domaines. Nix a fait preuve d'un engagement fort en faveur du renforcement de la résilience des organisations et de la protection des actifs face à des menaces et des défis divers. Le parcours de Nix dans la gestion des urgences a commencé par une passion pour la sécurité publique et la préparation aux catastrophes. Il est certifié ABCP par DRI et poursuit son programme de maîtrise en gestion des catastrophes et des urgences. Il est actuellement responsable provincial de la gestion des urgences sanitaires et de la continuité des activités (BCM) pour les services de santé de Terre-Neuve-et-Labrador (NLHS), au Canada.

# Comprehensive Risk Assessment- A Dual Approach for Organizational Resilience

# Évaluation globale des risques - Une double approche pour la résilience organisationnelle

By/Par Ray Unrau

**I**n today's dynamic business environment, uncertainty reigns supreme. Organizations grapple with diverse challenges. These challenges can be born from from the complex impacts of simultaneously occurring low level emergencies, to cyber threats to natural calamities. Complex events like these, or others, are poised to disrupt operations without warning. This unpredictable landscape underscores the necessity of robust business continuity planning. Central to this planning is a meticulous **operational risk assessment**, bolstered by a **hazard risk vulnerability assessment**—two foundational elements that fortify the structure of organizational resilience.

Recognizing that risk management is an applied management science, not an exact pure science, is crucial. As such, it eludes precise definition, compelling planning experts to exercise judgment regarding the scope and intricacy of the risk assessment process.

Management decisions within an organization are made daily, drawing on a complex interplay of expertise, judgment, logic,

**D**ans l'environnement commercial dynamique d'aujourd'hui, l'incertitude règne en maître. Les organisations sont confrontées à divers défis. Ces défis peuvent résulter de l'impact complexe d'urgences de faible niveau se produisant simultanément, de cybermenaces ou de catastrophes naturelles. Des événements complexes comme ceux-ci, ou d'autres, sont susceptibles de perturber les opérations sans avertissement. Ce paysage imprévisible souligne la nécessité d'une planification solide de la continuité des activités. Au cœur de cette planification se trouve une évaluation méticuleuse des risques opérationnels, renforcée par une évaluation de la vulnérabilité aux dangers - deux éléments fondamentaux qui fortifient la structure de la résilience organisationnelle.

Il est essentiel de reconnaître que la gestion des risques est une science appliquée de la gestion, et non une science pure exacte. En tant que telle, elle échappe à toute définition précise, obligeant les experts en planification à faire preuve de discernement quant à la portée et à la complexité du processus d'évaluation des risques.

unspoken knowledge, and intuitive forecasting. This amalgamation of skills is particularly pivotal during disruptive events. Thus, it is imperative for continuity planners to equip their management teams with risk assessments that are both realistic and all-encompassing, addressing every facet of the business. These assessments must be useable, enabling decision-makers to swiftly arrive at well-informed decisions when urgency prevails.

I think the classic 80/20 rule is pertinent here. Decision-makers constrained to intuitive choices with insufficient information or context risk ill-informed decisions, akin to a gunslinger's hasty draw. Conversely, managers who delay action while waiting for excessive detail may be perceived as indecisive.

In a world where business landscapes are in constant flux, the most effective risk assessment(s) take in the larger landscape of hazards while focusing on risks that, while not precisely predictable, provide sufficient insight to guide organizations through significant complex disruptions. This article will briefly review both the traditional operational risk assessments, then the Hazard Risk Vulnerability Assessments, to conclude with highlighting the beneficial synergies each assessment will provide to organizational continuity planners, as well as the managers responsible for decision making during these disruptive events.

### Operational Risk Assessment

The operational risk assessment is a systematic endeavor crucial to an organization's business continuity plan, and ultimately its continuity program. It entails the identification of potential events that could adversely affect operations and the assessment of their likelihood and impact. **The Disaster Recovery Institute (DRI)** advocates for principles that emphasize the identification, response, and recovery from such disruptions. The RMLE 2000 training program enhances this approach, presenting a structured method for evaluating risks within an organization.

Les décisions de gestion au sein d'une organisation sont prises quotidiennement, en s'appuyant sur une interaction complexe d'expertise, de jugement, de logique, de connaissances tacites et de prévisions intuitives. Cet amalgame de compétences est particulièrement crucial lors d'événements perturbateurs. Il est donc impératif que les planificateurs de la continuité dotent leurs équipes de gestion d'évaluations des risques qui soient à la fois réalistes et exhaustives, et qui abordent toutes les facettes de l'entreprise. Ces évaluations doivent être utilisables, afin de permettre aux décideurs de prendre rapidement des décisions éclairées lorsque l'urgence prévaut.

Je pense que la règle classique des 80/20 est pertinente ici. Les décideurs contraints de faire des choix intuitifs en l'absence d'informations ou de contexte suffisants risquent de prendre des décisions mal informées, à l'instar d'un tireur d'élite qui tire à la hâte. Inversement, les gestionnaires qui retardent l'action en attendant trop de détails peuvent être perçus comme indécis.

Dans un monde où le paysage des entreprises est en constante évolution, les évaluations des risques les plus efficaces prennent en compte l'ensemble des dangers tout en se concentrant sur les risques qui, bien qu'ils ne soient pas précisément prévisibles, fournissent suffisamment d'informations pour guider les organisations à travers des perturbations complexes et significatives. Cet article passe brièvement en revue les évaluations traditionnelles des risques opérationnels, puis les évaluations de la vulnérabilité aux risques liés aux aléas, pour conclure en soulignant les synergies bénéfiques que chaque évaluation apportera aux planificateurs de la continuité organisationnelle, ainsi qu'aux gestionnaires responsables de la prise de décision lors de ces événements perturbateurs.

### Évaluation du risque opérationnel

L'évaluation des risques opérationnels est une activité systématique essentielle au plan de continuité des activités d'une organisation et, en



My experience in emergency management involved collaboration with various organizations, from mid-sized enterprises to large-scale corporations across private and public sectors. These partnerships were sometimes proactive, with organizations seeking integration into a broader emergency planning framework. More often, my involvement was reactive, stemming from post-event analyses to assess the impact of unexpected events beyond their planning scope. Organizations with established continuity programs impressed me with their detailed and practical plans.

Post-event reviews yielded insights, especially concerning unforeseen challenges from external factors—the ‘unknown unknowns.’ These reviews revealed that while organizations might have robust continuity programs, limitations often existed up to the immediate environment’s periphery—a concept I describe as ‘planning from the C suite to the curb.’

It became clear that many lessons were linked to internal risk assessments that did not fully consider the broader operational context. This highlights the need for comprehensive organizational planning that extends beyond internal factors to include external dynamics and influences.

### **Hazard Risk Vulnerability Assessment**

Planning for disruptive events that affect multiple sectors, regions, or have prolonged impacts is challenging for individual organizations. A valuable tool in the continuity risk assessment process is the emergency management Hazard Risk Vulnerability Assessment (**HRVA**). The HRVA offers a detailed overview of potential hazards and their consequences, guiding decision-making, hazard mitigation, and preparation for response and recovery from regional risks.

I advocate for organizational risk assessments to utilize the HRVA, aiding organizations in aligning their plans with regional responses when resource and service demands exceed regional capacities. Integrating operational risk assessments with the HRVA provides decision-makers with essential information from ‘beyond the curb,’ aiding optimal decision-making in critical moments.

The HRVA’s value extends from response to planning. It equips community leaders and organizational decision-makers with the necessary details to make risk-based decisions addressing vulnerabilities. It serves as a foundation for local planners, politicians, and responders to update emergency plans, allocate resources for risk mitigation, bolster community preparedness, and budget for cost-effective, ongoing emergency planning.

**Emergency Management British Columbia** highlights the HRVA’s role in understanding community risk and resilience, aiding in hazard selection, vulnerability identification, and consideration of disaster risk drivers.

**Public Safety Canada** champions the integration of a mandate-specific all-hazards risk assessment. Their All-Hazards Risk Assessment (AHRA) identifies, analyzes, and prioritizes a comprehensive range of threats, assessing vulnerabilities and potential consequences, and exploring risk mitigation strategies.

In summary, the HRVA is an indispensable asset in emergency management. It facilitates the identification and comprehension of potential risks and informs the development of mitigation strategies. Consequently, it contributes to a safer, more prosperous, and resilient community, embodying the principle that proactive planning is superior to reactive measures.



**Public Safety  
Canada**

**Sécurité publique  
Canada**

fin de compte, à son programme de continuité. Elle implique l'identification d'événements potentiels susceptibles de nuire aux opérations et l'évaluation de leur probabilité et de leur impact. Le **Disaster Recovery Institute (DRI)** préconise des principes qui mettent l'accent sur l'identification, la réponse et la reprise après de telles perturbations. Le programme de formation RMLE 2000 renforce cette approche en présentant une méthode structurée d'évaluation des risques au sein d'une organisation.

Mon expérience en matière de gestion des urgences m'a amené à collaborer avec diverses organisations, des entreprises de taille moyenne aux grandes sociétés des secteurs privé et public. Ces partenariats étaient parfois proactifs, les organisations cherchant à s'intégrer dans un cadre plus large de planification des urgences. Le plus souvent, mon implication a été réactive, découlant d'analyses post-événement visant à évaluer l'impact d'événements inattendus dépassant le cadre de leur planification. Les organisations dotées de programmes de continuité bien établis m'ont impressionné par leurs plans détaillés et pratiques.

Les analyses effectuées après l'événement ont permis d'obtenir des informations, en particulier sur les défis imprévus liés à des facteurs externes - les "inconnus inconnus". Ces analyses ont révélé que même si les organisations disposaient de solides programmes de continuité, des limites existaient souvent à la périphérie de l'environnement immédiat - un concept que je décris comme "la planification de la suite C à la bordure du trottoir".

Il est apparu clairement que de nombreux enseignements étaient liés à des évaluations internes des risques qui ne tenaient pas pleinement compte du contexte opérationnel plus large. Cela souligne la nécessité d'une planification organisationnelle globale qui dépasse les facteurs internes pour inclure les dynamiques et les influences externes.

## Évaluation des risques et de la vulnérabilité

La planification d'événements perturbateurs qui affectent plusieurs secteurs ou régions, ou qui ont des effets prolongés, est un défi pour les organisations individuelles. Un outil précieux dans le processus d'évaluation des risques de continuité est l'évaluation des risques et de la vulnérabilité (**ÉRV**) en matière de gestion des urgences. Cette évaluation offre une vue d'ensemble détaillée des risques potentiels et de leurs conséquences, guidant la prise de décision, l'atténuation des risques et la préparation à la réponse et au rétablissement en cas de risques régionaux. Je préconise que les évaluations des risques organisationnels utilisent l'ÉVRH, afin d'aider les organisations à aligner leurs plans sur les réponses régionales lorsque les demandes de ressources et de services dépassent les capacités régionales. L'intégration de l'évaluation des risques opérationnels à l'HRVA permet aux décideurs de disposer d'informations essentielles "au-delà du trottoir", ce qui les aide à prendre des décisions optimales dans les moments critiques.

La valeur de l'HRVA s'étend de la réponse à la planification. Elle fournit aux dirigeants des communautés et aux décideurs des organisations les informations nécessaires pour prendre des décisions fondées sur les risques et les vulnérabilités. Elle sert de base aux planificateurs locaux, aux politiciens et aux intervenants pour mettre à jour les plans d'urgence, allouer des ressources à l'atténuation des risques, renforcer la préparation de la communauté et établir un budget pour une planification d'urgence rentable et continue.

**Emergency Management British Columbia** souligne le rôle de l'ÉVRH dans la compréhension des risques et de la résilience des communautés, en aidant à la sélection des aléas, à l'identification des vulnérabilités et à la prise en compte des facteurs de risque de catastrophe.

---

# Emergency Management British Columbia



## Integrating Both Assessments

While organizational risk assessment concentrates on internal threats, the HRVA encompasses a broader spectrum, including external threats and environmental factors. This expansive view is essential for comprehending the full array of risks a business may encounter. It is instrumental in creating a comprehensive risk profile, vital for informed decision-making and strategic planning. Municipal or provincial emergency management organizations offer invaluable resources for medium to large organizations, ensuring their internal operational assessments are effective during complex disruptive events that impact large geographic areas or multiple community sectors.

The simultaneous execution of both organizational risk assessments and hazard risk vulnerability assessments provides a multifaceted perspective on an organization's risk environment. This dual approach allows for a comprehensive integration of findings into a unified business continuity strategy, bolstering defenses against a wide array of internal and external threats. The effectiveness of this strategy is evidenced by case studies, which recount the experiences of numerous organizations that have adeptly managed crises through this holistic approach.

## Conclusion

Experts in business continuity are well-versed in the necessity of a systematic approach to implementing these assessments. A structured, step-by-step guide that incorporates established best practices and utilizes modern tools and resources can greatly aid in this process. It is essential for the scope of the operational risk assessment methodology to extend its vision beyond immediate

organizational boundaries and to be subject to regular updates.

Such proactive maintenance ensures that an organization's risk management strategy remains aligned with the ever-evolving landscape of risks in which they operate.

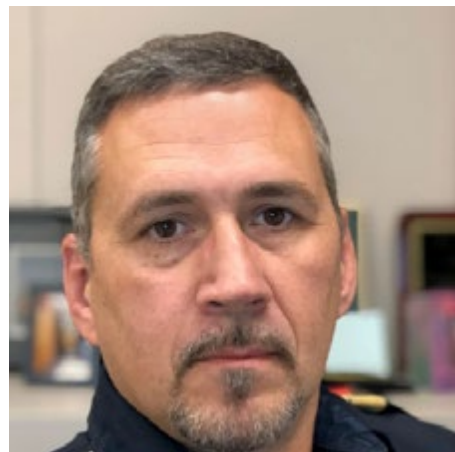
This article has offered a high-level overview of the field of risk assessment, underscoring the pivotal role that thorough risk evaluations play in the development of effective business continuity plans. Employing a strategy that

encompasses both types of assessments yields a more comprehensive understanding of potential risks, thereby enhancing organizational resilience. Business continuity professionals are urged to adopt these concepts, integrating them into their operational frameworks to protect their organizations from unpredictable events. Ω



## ABOUT THE AUTHOR

*Ray Unrau has been very involved in the EM world, started as a firefighter, transitioned to EMT, then into Emergency Management. He was the Director of EM for the City of Saskatoon, and then finished his career running the SK Provincial EM program and was instrumental in bringing BC to the Regional Municipalities in SK. He had DRIC come and run the 2000 course for key folks and they then went out and helped the smaller RMs bridge the gap between EM and BC.*



**Sécurité publique Canada** préconise l'intégration d'une évaluation des risques tous azimuts spécifique au mandat. L'évaluation des risques tous azimuts (ERA) identifie, analyse et hiérarchise une gamme complète de menaces, en évaluant les vulnérabilités et les conséquences potentielles, et en explorant les stratégies d'atténuation des risques.

En résumé, l'HRVA est un atout indispensable pour la gestion des situations d'urgence. Elle facilite l'identification et la compréhension des risques potentiels et contribue à l'élaboration de stratégies d'atténuation. Elle contribue ainsi à rendre la communauté plus sûre, plus prospère et plus résiliente, en incarnant le principe selon lequel la planification proactive est supérieure aux mesures réactives.

### Intégration des deux évaluations

Alors que l'évaluation des risques organisationnels se concentre sur les menaces internes, l'HRVA englobe un spectre plus large, y compris les menaces externes et les facteurs environnementaux. Cette vision élargie est essentielle pour comprendre l'ensemble des risques auxquels une entreprise peut être confrontée. Elle permet de créer un profil de risque complet, indispensable à une prise de décision éclairée et à la planification stratégique. Les organismes municipaux ou provinciaux de gestion des urgences constituent des ressources inestimables pour les moyennes et grandes entreprises, en veillant à ce que leurs évaluations opérationnelles internes soient efficaces lors d'événements perturbateurs complexes ayant un impact sur de vastes zones géographiques ou de multiples secteurs de la communauté.

L'exécution simultanée d'une évaluation des risques organisationnels et d'une évaluation de la vulnérabilité aux dangers offre une perspective à multiples facettes de l'environnement de risque d'une organisation. Cette double approche permet une intégration complète des résultats dans une stratégie unifiée de continuité des activités, renforçant ainsi les défenses contre un large éventail

de menaces internes et externes. L'efficacité de cette stratégie est démontrée par des études de cas, qui relatent les expériences de nombreuses organisations qui ont su gérer les crises grâce à cette approche holistique.

### Conclusion

Les experts en continuité des affaires connaissent bien la nécessité d'une approche systématique pour la mise en œuvre de ces évaluations. Un guide structuré, étape par étape, qui intègre les meilleures pratiques établies et utilise des outils et des ressources modernes, peut grandement faciliter ce processus. Il est essentiel que le champ d'application de la méthodologie d'évaluation des risques opérationnels dépasse les frontières immédiates de l'organisation et fasse l'objet de mises à jour régulières. Cette mise à jour proactive garantit que la stratégie de gestion des risques d'une organisation reste alignée sur le paysage des risques en constante évolution dans lequel elle opère.

Cet article propose une vue d'ensemble du domaine de l'évaluation des risques, soulignant le rôle essentiel que jouent les évaluations de risque approfondies dans l'élaboration de plans de continuité des activités efficaces. L'utilisation d'une stratégie englobant les deux types d'évaluation permet d'obtenir une compréhension plus complète des risques potentiels et d'améliorer ainsi la résilience de l'organisation. Les professionnels de la continuité des activités sont invités à adopter ces concepts et à les intégrer dans leurs cadres opérationnels afin de protéger leurs organisations contre les événements imprévisibles. Ω

---

### À PROPOS DE L'AUTEUR

*Ray Unrau a été très impliqué dans le monde de la SE, a commencé comme pompier, est passé à EMT, puis à la gestion des urgences. Il a été directeur de la GU pour la Ville de Saskatoon, puis a terminé sa carrière en dirigeant le programme provincial de GU de la Saskatchewan et a joué un rôle déterminant dans l'introduction de la Colombie-Britannique dans les municipalités régionales de la Saskatchewan. Il a demandé à DRIC de venir diriger le cours de 2000 pour les gens clés, puis ils sont allés aider les plus petits MR à combler le fossé entre EM et BC.*

# Interim Report on Resilience and Preparedness – Canadian Journal of Emergency Management MINDS Initiative

## Introduction

**O**n July 23rd, 2024, the Canadian Journal of Emergency Management (CJEM) hosted a webinar entitled “From Lights & Sirens to Resilience” in collaboration with Disaster Recovery Institute Canada (DRIC) as part of the MINDS initiative. This webinar addressed the critical implications of emergency and disaster response, focusing on the intersections of resilience from the perspective of emergency management and disaster recovery. The aim was to bring together experts from the fields of business continuity and emergency management to share their ideas, experiences, and strategies in a cross-functional basis to improve collective understanding and preparedness.

### Panel Participants and Moderator

The webinar was structured in two distinct panels, one in each of Canada’s official languages to ensure accessibility to a wider audience.

The first panel, held conducted in English, featured the following experts:

**Dr Michel C. Doré**, an Associate Professor at l’Université de Québec à Montréal, also

# Rapport Intermédiaire sur la Résilience et la Préparation – Initiative MINDS de la Revue canadienne de la Gestion des Urgences

## Introduction

**L**e 23 juillet 2024, la Revue canadienne de la gestion des urgences (RCGU) a organisé un webinaire intitulé “Des lumières et des sirènes à la résilience” en collaboration avec l’Institut canadien de la continuité des affaires (DRIC) dans le cadre de l’initiative MINDS. Ce webinaire a abordé les implications critiques de la réponse aux urgences et aux catastrophes, en mettant l’accent sur les intersections de la résilience du point de vue de la gestion des urgences et de la reprise après sinistre. L’objectif était de réunir des experts des domaines de la continuité des affaires et de la gestion des urgences pour partager leurs idées, expériences et stratégies sur une base transversale afin d’améliorer la compréhension collective et la préparation.

### Participants du Panel et Modérateur

Le webinaire était structuré en deux panels distincts, l’un dans chacune des langues officielles du Canada pour assurer l’accessibilité à un public plus large.

Le premier panel, en anglais, comprenait les experts suivants :

represented St John Ambulance Canada as its National Emergency Management Advisor.

**Dr Jeff Donaldson**, a distinguished veteran of the Canadian Armed Forces and current Principal Researcher for Preparedness Labs Inc.

**Ernie Polsom**, a former fire chief at both municipal and provincial levels, now CEO of FireWise Consulting.

**Pascal Rodier**, a Senior Emergency Management, Response, and Continuity Leader in Nova Scotia & throughout the Atlantic Region.

The second panel, conducted in French, featured the following experts:

**Jean-François Couture-Poulin**, Public Safety Advisor for the City of Lévis, Québec.

**Guy Lapointe**, President of the Quebec Association of Volunteer Search & Rescue, as well as Vice- President of the Search and Rescue Volunteer Association of Canada.

**Eric Martel**, Resilience, Risk, and Disaster Manager for the Municipality of Pincourt, Québec.

**Christian Legault**, Director of Fire Services for the Municipality of Sainte-Thérèse, Québec.

Notably, the webinar event began with keynote remarks from **Nancy Holloway-White**, President of Disaster Recovery Institute Canada and a Senior Business Continuity Consultant in Canada. Both panels were moderated by **Alexander Landry**, Senior Manager for Strategic Implementation with the Canadian Journal of Emergency Management and a member of the Disaster Recovery Institute of Canada Board of Directors.

### Key Themes

In continuing follow up from previous CJEM events, this webinar sought to address certain themes that were residual from discussions with experts held on February 24th and June 6th. Among them, specific items that were brought forward are as follows:

**Dr Michel C. Doré**, professeur associé à l'Université du Québec à Montréal, également conseiller national en gestion des urgences pour Saint-Jean Ambulance Canada.

**Dr Jeff Donaldson**, vétéran distingué des Forces armées canadiennes et chercheur principal actuel pour Preparedness Labs Inc.

**Ernie Polsom**, ancien chef des pompiers aux niveaux municipal et provincial, maintenant PDG de FireWise Consulting.

**Pascal Rodier**, leader senior en gestion des urgences, réponse et continuité en Nouvelle-Écosse et dans toute la région de l'Atlantique.

Le deuxième panel, en français, comprenait les experts suivants :

**Jean-François Couture-Poulin**, conseiller en sécurité publique pour la ville de Lévis, Québec.

**Guy Lapointe**, président de l'Association québécoise des bénévoles en recherche et sauvetage, ainsi que vice-président de l'Association des bénévoles en recherche et sauvetage du Canada.

**Eric Martel**, gestionnaire de la résilience, des risques et des catastrophes pour la municipalité de Pincourt, Québec.

**Christian Legault**, directeur des services d'incendie de la municipalité de Sainte-Thérèse, Québec.

Notamment, le webinaire a débuté par des remarques liminaires de **Nancy Holloway-White**, présidente de DRIC et consultante senior en continuité des affaires au Canada. Les deux panels ont été modérés par **Alexander Landry**, directeur principal de la mise en œuvre stratégique la RCGU et membre du conseil d'administration de DRIC.

### Thèmes clés

En poursuivant le suivi des événements précédents du CJEM, ce webinaire a cherché à aborder certains thèmes résiduels des discussions avec des experts tenues les 24 février et 6 juin. Parmi eux, les points spécifiques qui ont été soulevés sont les suivants :

### *Whole of Government Approach and Community Resilience*

The webinar emphasized a holistic, integrated approach to emergency management. It highlighted the importance of clearly defining disaster frameworks and understanding what constitutes a disaster. There was a debate over the effectiveness of standardization versus tailored, community-specific disaster response plans. The necessity of identifying specific needs and resources from the Canadian Armed Forces (CAF) and the federal government during emergencies, such as surge capabilities, wildland firefighters, or helicopters, was underscored.

### *Provincial and Territorial Capacity Building*

Discussions revolved around the need for provinces and territories to build local capacities and cooperation strategies to mobilize resources effectively before seeking federal assistance. There was recognition by our firefighting experts of a significant shortfall in volunteer firefighters, with 37,000 fewer than needed (CTIF:International Association of Rescue and Fire Services, 2024). The influence of the US National Guard and FEMA on Canadian emergency management perceptions was noted.

### *Incentivizing Community and Private Sector Involvement*

Clear incentives are needed to encourage communities and businesses to invest in resilience and business continuity efforts. Suggestions included integrating business continuity into audit processes, providing funding through provincial channels, and

making grants available. The role of NGOs and private organizations in daily life and emergencies was highlighted, including the notion that volunteers during incidents tend to stem from local communities. This emphasized the importance of partnerships with large corporations considering their reach and integration into communities already.

To this effect, stronger partnerships with private sector entities were deemed essential for enhancing emergency preparedness and response. Examples from other jurisdictions, such as pre-positioning of supplies by companies like Walmart in the United States, were provided. Formalizing partnerships, sharing knowledge and resources, and recognizing the critical role of private organizations in supporting public efforts were recommended.

### *Education and Training for Emergency Management*

The panel advocated for incorporating emergency preparedness and resilience education into school curriculums, potentially beginning at the elementary school level. This approach has historical precedent, similar to the “Duck and Cover” videos, which aimed to educate children on how to protect themselves during emergencies (J. Mauer, 1951). Emphasis was placed on practical, scenario-based training for emergency managers, especially in smaller communities. Specifically, Dr. Jeff Donaldson remarked, “Preparedness is where the response fight is won,” alluding to the need for adequate preparation to ensure emergencies are appropriately addressed when they occur.

One participant incorrectly suggested that communities don’t have a mandate to be emergency prepared. The assertion itself is incorrect - all Provinces and Territories require their municipalities to have some type of emergency management plans - but it also highlighted a need for stronger practical and programmatic training and education in emergency management. Simple knowledge gaps like this indicate that more specific knowledge about emergency management capabilities and response / aid mechanisms (RFAs) aren’t being shared or learned.



### *Approche Pangouvernementale et Résilience Communautaire*

Le webinaire a mis en avant une approche holistique et intégrée de la gestion des urgences. Il a souligné l'importance de définir clairement les cadres de catastrophe et de comprendre ce qui constitue une catastrophe. Un débat a eu lieu sur l'efficacité de la standardisation par rapport aux plans de réponse aux catastrophes adaptés aux communautés spécifiques. La nécessité d'identifier les besoins spécifiques et les ressources des Forces armées canadiennes (FAC) et du gouvernement fédéral pendant les urgences, comme les capacités de renfort, les pompiers forestiers ou les hélicoptères, a été soulignée.

### *Renforcement des Capacités Provinciales et Territoriales*

Les discussions ont tourné autour de la nécessité pour les provinces et les territoires de renforcer les capacités locales et les stratégies de coopération pour mobiliser efficacement les ressources avant de demander une assistance fédérale. Nos experts en lutte contre les incendies ont reconnu un déficit significatif de pompiers volontaires, avec 37 000 de moins que nécessaire (CTIF : Association internationale des services de secours et d'incendie, 2024). L'influence de la Garde nationale américaine et de la FEMA sur les perceptions canadiennes de la gestion des urgences a été notée.

### *Incitations à l'Implication des Communautés et des Entreprises*

Des incitations claires sont nécessaires pour encourager les communautés et les entreprises à investir dans les efforts de résilience et de continuité des affaires. Les suggestions incluaient l'intégration de la continuité des affaires dans les processus d'audit, la fourniture de financements par le biais de canaux provinciaux et la mise à disposition de subventions. Le rôle des ONG et des organisations privées dans la vie quotidienne et les urgences a été souligné,

notamment l'idée que les volontaires lors d'incidents proviennent généralement des communautés locales. Cela a mis en avant l'importance des partenariats avec les grandes entreprises, compte tenu de leur portée et de leur intégration déjà existante dans les communautés.

À cet effet, des partenariats plus solides avec les entités du secteur privé ont été jugés essentiels pour renforcer la préparation et la réponse aux urgences. Des exemples d'autres juridictions, telles que le pré-positionnement des fournitures par des entreprises comme Walmart aux États-Unis, ont été fournis. La formalisation des partenariats, le partage des connaissances et des ressources, et la reconnaissance du rôle crucial des organisations privées dans le soutien des efforts publics ont été recommandés.

### *Éducation et Formation à la Gestion des Urgences*

Le panel a plaidé pour l'intégration de l'éducation à la préparation aux urgences et à la résilience dans les programmes scolaires, potentiellement dès le niveau de l'école primaire. Cette approche a un précédent historique, similaire aux vidéos "Duck and Cover" de l'époque de la guerre froide, qui visaient à éduquer les enfants sur la manière de se protéger en cas d'urgence (J. Mauer, 1951). L'accent a été mis sur la formation pratique et basée sur des scénarios pour les gestionnaires d'urgence, en particulier dans les petites communautés. Plus précisément, le Dr Jeff Donaldson a déclaré : "La préparation est là où se gagne le combat de la réponse", faisant allusion à la nécessité d'une préparation adéquate pour garantir que les urgences soient correctement gérées lorsqu'elles se produisent.

Un participant a incorrectement suggéré que les communautés n'ont pas de mandat pour être prêtes en cas d'urgence. Cette affirmation est incorrecte - toutes les provinces et territoires exigent que leurs municipalités disposent de plans de gestion des urgences - mais cela met également en évidence la nécessité



### *Leveraging Civilian Resources & Volunteer Interest*

The significant role of community involvement and volunteerism in disaster response was acknowledged. Harnessing and building upon the natural, spontaneous response of people during disasters was suggested. The integration of skilled volunteers, including physicians, nurses, paramedics, and first responders, into emergency response plans was also highlighted.

Further, the exploration of existing provincial and territorial resources that can be shared easily between jurisdictions was discussed. Challenges and barriers to effective collaboration between agencies were highlighted, along with the use of technology to facilitate better communication and information sharing. The National Risk Profile has identified the use of technology as a crucial capacity to address moving forward on a national basis (Public Safety Canada, 2024). This profile uses the All-Hazards Risk Assessment and Emergency Management Capability Assessment methodologies to assess Canada's current risk levels and inform our collective ability to mitigate impacts. The importance of social capital and community relationships in disaster response was emphasized, alongside the need to develop a culture of preparedness and codify the transition from passion and commitment to actionable volunteer efforts.

### *Business Continuity and Resilience*

The lack of mandated continuity of operations plans for government offices in Canada was noted. Investment in preparedness, mitigation, and resilience was deemed essential for effective recovery. Financial assistance programs like the Disaster Financial Assistance Arrangements (Public Safety Canada, 2024) can sometimes disincentivize local investment in emergency management.

Accordingly, there was a call to define what a resilient individual and community look like. Assessing current community standards to design effective education and preparedness programs was suggested. Investments in preparedness, mitigation, and resilience were seen as having long-term benefits for community safety and disaster recovery.

### *Interoperability and Collaboration*

Interoperability was discussed as involving people and relationships, not just technology. The inclusion of private sector and volunteer groups in planning and exercises to ensure coordinated efforts during disasters was recommended.

Ultimately, the finite nature of emergency management resources and the competition with other essential services were highlighted. Regional collaboration among communities to pool resources for targeted education and preparedness campaigns was suggested.

### *Unique Aspects of Québec's Approach*

One of the distinctive features of the July 23rd event was the inclusion of a French panel with experts stemming from the Province of Québec, thus providing insight to both English and French communities into the unique aspects of Québec's approach to both emergency management and business continuity.

Of primordial importance, the recent Quebec Civil Protection Act (Public Safety Canada, 2018) emphasizes individual responsibility for safety and property during emergencies. The law mandates local authorities to engage citizens in risk management efforts, consulting, and informing them about measures to reduce risks and consequences of disasters.

The discussion highlighted the importance of moving from mitigation to true adaptation. This shift involves not only reducing the immediate impacts of disasters (mitigation) but also making long-term changes to how communities interact with their environment to minimize future risks (adaptation). Revising the relationship with the territory means adopting strategies that integrate the natural characteristics and vulnerabilities of the area into planning and development. This territorial adaptation includes prioritizing systemic vulnerabilities and implementing nature-based solutions, such as restoring ecosystems and using natural barriers, to enhance resilience and reduce disaster risks.

d'une formation et d'une éducation plus pratiques et programmatiques en gestion des urgences. De simples lacunes dans les connaissances comme celle-ci indiquent que des connaissances plus spécifiques sur les capacités de gestion des urgences et les mécanismes de réponse/assistance (RFA) ne sont pas partagées ou apprises.

### *Exploitation des Ressources Civiles et l'intérêt des bénévoles*

Le rôle significatif de l'implication communautaire et du bénévolat dans la réponse aux catastrophes a été reconnu. Il a été suggéré de tirer parti de la réponse naturelle et spontanée des gens lors des catastrophes. L'intégration de bénévoles qualifiés, y compris des médecins, des infirmières, des ambulanciers paramédicaux et des premiers intervenants, dans les plans de réponse aux urgences a également été soulignée.

De plus, l'exploration des ressources provinciales et territoriales existantes qui peuvent être facilement partagées entre les juridictions a été discutée. Les défis et les obstacles à une collaboration efficace entre les agences ont été mis en évidence, ainsi que l'utilisation de la technologie pour faciliter une meilleure communication et un meilleur partage de l'information. Le Profil national des risques a identifié l'utilisation de la technologie comme une capacité cruciale à aborder à l'avenir au niveau national (Sécurité publique Canada, 2024). Ce profil utilise les méthodologies d'évaluation des risques tous risques et d'évaluation des capacités de gestion des urgences pour évaluer les niveaux de risque actuels du Canada et informer notre capacité collective à atténuer les impacts. L'importance du capital social et des relations communautaires dans la réponse aux catastrophes a été soulignée, ainsi que la nécessité de développer une culture de préparation et de codifier la transition de la passion et de l'engagement vers des efforts bénévoles concrets.

### *Continuité des Affaires et Résilience*

L'absence de plans de continuité des opérations obligatoires pour les bureaux gouvernementaux au Canada a été notée. L'investissement dans la préparation, l'atténuation et la résilience a été jugé essentiel pour une récupération efficace. Les programmes d'aide financière en cas de catastrophe, comme les arrangements de financement des secours en cas de catastrophe (Sécurité publique Canada, 2024), peuvent parfois dissuader les investissements locaux dans la gestion des urgences.

En conséquence, il a été demandé de définir à quoi ressemble un individu et une communauté résilients. Il a été suggéré d'évaluer les normes communautaires actuelles pour concevoir des programmes d'éducation et de préparation efficaces. Les investissements dans la préparation, l'atténuation et la résilience ont été considérés comme ayant des avantages à long terme pour la sécurité communautaire et la reprise après une catastrophe.

### *Interopérabilité et Collaboration*

L'interopérabilité a été discutée comme impliquant des personnes et des relations, pas seulement la technologie. L'inclusion de groupes du secteur privé et de bénévoles dans la planification et les exercices pour assurer des efforts coordonnés lors des catastrophes a été recommandée.

En fin de compte, la nature limitée des ressources de gestion des urgences et la concurrence avec d'autres services essentiels ont été soulignées. Une collaboration régionale entre les communautés pour mettre en commun les ressources pour des campagnes ciblées d'éducation et de préparation a été suggérée.

### **Aspects Uniques de l'Approche du Québec (Panel Français)**

L'un des aspects distinctifs de l'événement du 23 juillet était l'inclusion d'un panel en français avec des experts de la province de Québec, fournissant ainsi des informations aux



There was a call for clearer communication and understanding between federal, provincial, and local levels regarding emergency management. The language used for risk communication should be adapted for better comprehension by the general public, and efforts should be made to enhance community and corporate resilience. This inter-provincial cooperation should extend to other weather-related disasters and public health emergencies.

The importance of civilian involvement as first responders in emergencies was stressed, focusing on collective self-reliance and making informed choices, supported by local authorities and humanitarian organizations. As an example, the idea of mobilizing and training urban firefighters to assist in forest fire situations, while also enhancing volunteer organizations with proper training and equipment was proposed.

Private sector participation in risk communication and disaster preparedness was encouraged. The Quebec Civil Security Act supports the alignment of business continuity plans with regional and local authority standards to enhance overall community resilience.

As an example, the municipalities of Pincourt, Pointe-Fortune, and Très-Saint-Rédempteur have joined forces for a multi-municipal civil security approach, led by the Municipality of Pincourt (Neo-Media, 2024).

This initiative includes a structure compliant with provincial requirements, alert mechanisms, mobilization strategies, and partnerships with external actors. A vulnerability profile initiative involving community organizations is also being developed. This collaborative approach could serve as a model for other municipalities moving forward.

Finally, the panel explored how technology can improve communication and information sharing between civil agencies, provincial/territorial bodies, and the federal government. Enhanced processes and agreements are needed to facilitate the use of civilian resources

during emergencies. The National Risk Profile has identified the use of technology as a critical capacity to address these challenges on a national basis, leveraging methodologies like the All-Hazards Risk Assessment and Emergency Management Capability Assessment to enhance overall preparedness and response capabilities across Canada's diverse hazardscape.

## Interim Recommendations

From the discussions and insights shared during the webinar, several interim recommendations emerged:

### 1. Development of a National Knowledge-Sharing Platform:

The panel proposed the development of a national knowledge-sharing platform to allow emergency management professionals to share best practices, lessons learned, and innovative strategies. This platform aims to enhance collective knowledge and improve response efforts. By utilizing advanced situational awareness tools from the Government of Canada (GoC) and the Canadian Armed Forces (CAF), communities can gain more lead-time in preparation for potential disasters. These tools can help identify probable threats early, enabling communities to prepare and respond more effectively using available resources. This proactive approach can reduce the frequency and urgency of Requests for Assistance (RFAs), allowing for more efficient disaster management and response.

### 2. Conduct of Regular Inter-Agency Drills:

The panel recommended conducting regular inter-agency drills to improve coordination and communication. Specifically, agencies should carry out ground-level drills that simulate actual emergency response scenarios. These drills should also include Tabletop Exercises (TTXs) with the potential to escalate into full-scale dry deployments. This approach ensures that all stakeholders are fully aware of their roles and responsibilities during emergencies and holds each agency accountable for their part in the response efforts. Ideally, these drills need to be spearheaded by federal, provincial, and municipal authorities, yet also include private sector and volunteer participation.

communautés anglophones et francophones sur les aspects uniques de l'approche du Québec en matière de gestion des urgences et de continuité des affaires.

De prime importance, la récente Loi sur la protection civile du Québec (Sécurité publique Canada, 2018) met l'accent sur la responsabilité individuelle en matière de sécurité et de biens en cas d'urgence. La loi oblige les autorités locales à engager les citoyens dans les efforts de gestion des risques, en les consultant et en les informant des mesures à prendre pour réduire les risques et les conséquences des catastrophes.

La discussion a souligné l'importance de passer de l'atténuation à la véritable adaptation. Ce changement implique non seulement de réduire les impacts immédiats des catastrophes (atténuation), mais aussi de faire des changements à long terme sur la façon dont les communautés interagissent avec leur environnement pour minimiser les risques futurs (adaptation). Revoir la relation avec le territoire signifie adopter des stratégies qui intègrent les caractéristiques naturelles et les vulnérabilités de la région dans la planification et le développement. Cette adaptation territoriale comprend la priorisation des vulnérabilités systémiques et la mise en œuvre de solutions basées sur la nature, telles que la restauration des écosystèmes et l'utilisation de barrières naturelles, pour renforcer la résilience et réduire les risques de catastrophes.

Il a été demandé d'améliorer la communication et la compréhension entre les niveaux fédéral, provincial et local concernant la gestion des urgences. Le langage utilisé pour la communication des risques devrait être adapté pour une meilleure compréhension par le grand public, et des efforts devraient être faits pour renforcer la résilience communautaire et corporative. Cette coopération interprovinciale devrait s'étendre à d'autres catastrophes liées aux conditions météorologiques et aux urgences de santé publique.

L'importance de l'implication des civils en tant que premiers intervenants en cas d'urgence a été soulignée, en mettant l'accent sur l'autosuffisance collective et la prise de décisions éclairées, soutenues par les autorités locales et les organisations humanitaires. Par exemple, l'idée de mobiliser et de former les pompiers urbains pour aider dans les situations d'incendies de forêt, tout en renforçant les organisations de bénévoles avec une formation et un équipement adéquat, a été proposée.

La participation du secteur privé à la communication des risques et à la préparation aux catastrophes a été encouragée. La Loi sur la sécurité civile du Québec soutient l'alignement des plans de continuité des affaires avec les normes des autorités régionales et locales pour renforcer la résilience communautaire globale.

Par exemple, les municipalités de Pincourt, Pointe-Fortune et Très-Saint-Rédempteur se sont associées pour une approche de sécurité civile multi-municipale, dirigée par la municipalité de Pincourt (Neo-Media, 2024). Cette initiative comprend une structure conforme aux exigences provinciales, des mécanismes d'alerte, des stratégies de mobilisation et des partenariats avec des acteurs externes. Une initiative de profil de vulnérabilité impliquant des organisations communautaires est également en cours de développement. Cette approche collaborative pourrait servir de modèle pour d'autres municipalités à l'avenir.

Enfin, le panel a exploré comment la technologie peut améliorer la communication et le partage d'informations entre les agences civiles, les organismes provinciaux/territoriaux et le gouvernement fédéral. Des processus et des accords améliorés sont nécessaires pour faciliter l'utilisation des ressources civiles en

### 3. Inclusion of Mitigation and Preparedness in After-

**Action Reports:** The panel suggested that organizations include mitigation and preparedness measures in their after-action reports to promote continuous improvement and readiness for future incidents. Encouraging an open culture for sharing information, experiences, and best practices beyond organizational boundaries is crucial for fostering collective improvement and innovation.

### Conclusion

Overall, the CJEM-DRIC collaborative webinar provided a comprehensive discussion on the critical implications of emergency and disaster response, focusing on the intersections of resilience from the perspective of emergency management and disaster recovery. Key themes such as community resilience, pan-governmental approaches, provincial and territorial capacity building, civilian involvement, and the role of public-private partnerships were thoroughly explored, offering valuable insights and strategies for improving collective understanding and preparedness. The discussion ultimately led to the recommendations provided above, supporting previously explored items from the events of February 24th and June 6th.

Future focus areas include developing community-based training programs, enhancing funding mechanisms for local resilience initiatives, and integrating technological innovations to support disaster management efforts. Through these efforts, communities can reduce dependency on external aid and ensure a more effective and coordinated response to emergencies. Ω

### References:

Public Safety Canada. "Get Prepared: Quebec." Last modified February 21, 2018. <https://www.getprepared.gc.ca/cnt/hzd/rgnl/qc-en.aspx>.

Neo-Media. "Civil Protection: Pincourt, Très-Saint-Rédempteur and Pointe-Fortune Join Forces." Last modified January 23, 2024. <https://www.neomedia.com/vaudreuil-soulanges/actualites/my-english-news/602483/civil-protection-pincourt-tres-saint-redempteur-and-pointe-fortune-join-forces>.

Public Safety Canada. "Disaster Financial Assistance Arrangements (DFAA)." Last modified April 3, 2024. <https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/rcvr-dsstrs/dsstr-fnncl-ssstnc-rrngmnts/index-en.aspx>.

cas d'urgence. Le Profil national des risques a identifié l'utilisation de la technologie comme une capacité critique pour relever ces défis à l'échelle nationale, en s'appuyant sur des méthodologies telles que l'évaluation des risques tous risques et l'évaluation des capacités de gestion des urgences pour améliorer la préparation et les capacités de réponse globales à travers le paysage diversifié des risques du Canada.

### Recommandations Intermédiaires

À partir des discussions et des idées partagées lors du webinaire, plusieurs recommandations intérimaires ont émergé :

**I. Développement d'une plateforme nationale de partage des connaissances :** Le panel a proposé le développement d'une plateforme nationale de partage des connaissances permettant aux professionnels de la gestion des urgences de partager les meilleures pratiques, les leçons apprises et les stratégies innovantes. Cette plateforme vise à améliorer les connaissances collectives et à renforcer les efforts de réponse. En utilisant des outils de connaissance avancée de la situation du gouvernement du Canada (GoC) et des Forces armées canadiennes (FAC), les communautés peuvent bénéficier d'un délai de préparation plus long pour les catastrophes potentielles. Ces outils peuvent aider à identifier les menaces probables tôt, permettant aux communautés de se préparer et de répondre plus efficacement en utilisant les ressources disponibles. Cette approche proactive peut réduire

la fréquence et l'urgence des demandes d'assistance (RFA), permettant une gestion et une réponse aux catastrophes plus efficaces.

**2. Conduite d'exercices inter-agences réguliers :** Le panel a recommandé de mener des exercices inter-agences réguliers pour améliorer la coordination et la communication. Plus précisément, les agences devraient réaliser des exercices sur le terrain simulant des scénarios réels de réponse aux urgences. Ces exercices devraient également inclure des exercices sur table (TTX) pouvant se transformer en déploiements à sec à grande échelle. Cette approche garantit que toutes les parties prenantes sont pleinement conscientes de leurs rôles et responsabilités en cas d'urgence et tient chaque agence responsable de sa part dans les efforts de réponse. Idéalement, ces exercices doivent être dirigés par les autorités fédérales, provinciales et municipales, mais inclure également la participation du secteur privé et des bénévoles.

**3. Inclusion des mesures d'atténuation et de préparation dans les rapports après action :** Le panel a suggéré que les organisations incluent des mesures d'atténuation et de préparation dans leurs rapports après action pour promouvoir l'amélioration continue et la préparation aux incidents futurs. Encourager une culture ouverte de partage d'informations, d'expériences et de meilleures pratiques au-delà des frontières organisationnelles est crucial pour favoriser l'amélioration collective et l'innovation.

## Conclusion

Dans l'ensemble, le webinaire collaboratif CJEM-DRIC a offert une discussion approfondie sur les implications critiques de la réponse aux urgences et aux catastrophes, en se concentrant sur les intersections de la résilience du point de vue de la gestion des urgences et de la reprise après sinistre. Les thèmes clés tels que la résilience communautaire, les approches pangouvernementales, le renforcement

des capacités provinciales et territoriales, l'implication des civils et le rôle des partenariats public-privé ont été explorés en profondeur, offrant des idées et des stratégies précieuses pour améliorer la compréhension collective et la préparation. La discussion a finalement conduit aux recommandations fournies ci-dessus, soutenant les éléments précédemment explorés lors des événements des 24 février et 6 juin.

Les domaines de concentration futurs incluent le développement de programmes de formation communautaires, l'amélioration des mécanismes de financement pour les initiatives locales de résilience et l'intégration des innovations technologiques pour soutenir les efforts de gestion des catastrophes. Grâce à ces efforts, les communautés peuvent réduire leur dépendance à l'aide extérieure et garantir une réponse plus efficace et coordonnée aux urgences. Ω

---

## Références

Sécurité publique Canada. "Préparez-vous : Québec." Dernière modification le 21 février 2018. <https://www.getprepared.gc.ca/cnt/hzd/rgnl/qc-en.aspx>.

Neo-Media. "Protection civile : Pincourt, Très-Saint-Rédempteur et Pointe-Fortune unissent leurs forces." Dernière modification le 23 janvier 2024. <https://www.neomedia.com/valdreuil-soulanges/actualites/my-english-news/60248/civil-protection-pincourt-tres-saint-redempteur-and-pointe-fortune-join-forces>.

Sécurité publique Canada. "Arrangements de financement des secours en cas de catastrophe (DFAA)." Dernière modification le 3 avril 2024. <https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/rcvr-dsstrs/dsstr-fnncl-ssstnc-rrngmnts/index-en.aspx>.

Sécurité publique Canada. "Profil national des risques." Dernière modification le 16 février 2024. <https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/ntnl-rsk-prfl/index-en.aspx>.



Public Safety Canada. "National Risk Profile." Last modified February 16, 2024. <https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/ntnl-rsk-prfl/index-en.aspx>.

Mauer, Raymond J. "Duck and Cover (1951) Bert the Turtle." YouTube video, 9:15. Posted July 12, 2009. <https://www.youtube.com/watch?v=IKqXu-5jw60>.

CTIF: International Association of Fire and Rescue Services. "Difficult Shortages of Volunteer Firefighters in the US and Canada." Last modified February 2024. <https://www.ctif.org/news/difficult-shortages-volunteer-firefighters-us-and-canada-recruitment-crucial-wildfire-fighting#:~:text=In%202016%2C%20when%20he%20became,alone%20as%20a%20Volunteer%20Firefighter.>

### Contributors

Author:

**Sara Kallas**, Lead Research Assistant, MINDS Initiative (CJEM)


Editors:

**Connor Hunerfauth**, Strategic Project Officer (CJEM) **Alexander Landry**, Senior Manager - Strategic Implementation (CJEM)

Reviewer:

**Simon Wells**, Principal and Director (CJEM)

### \*Editorial Note

*Of important note is that this webinar along with others for the Canadian Journal of Emergency Management in 2024 have been a part of a Government of Canada-funded initiative with the Department of National Defence. The "Mobilizing Insights in Defense and Security" Targeted Engagement Grant program aims to drive innovation in defence policy thinking and to foster the next generation of defence and security experts.* 

Mauer, Raymond J. "Duck and Cover (1951) Bert the Turtle." Vidéo YouTube, 9:15. Publié le 12 juillet 2009. <https://www.youtube.com/watch?v=IKqXu-5jw60>.

CTIF : Association internationale des services de secours et d'incendie. "Pénuries difficiles de pompiers volontaires aux États-Unis et au Canada." Dernière modification en février 2024. <https://www.ctif.org/news/difficult-shortages-volunteer-firefighters-us-and-canada-recruitment-crucial-wildfire-fighting#:~:text=In%202016%2C%20when%20he%20became,alone%20as%20a>

### Contributeurs

Auteure :

**Sara Kallas**, adjointe de recherche principale, Initiative MINDS (CJEM)

Rédacteurs :


**Connor Hunerfauth**, agent de projet stratégique (CJEM)

**Alexander Landry**, gestionnaire principal - Mise en œuvre stratégique (CJEM)

Réviseur :

**Simon Wells**, directeur principal et directeur (CJEM)

### \*Note éditoriale

*Il est important de noter que ce webinaire ainsi que d'autres pour la Revue canadienne de gestion des urgences en 2024 ont fait partie d'une initiative financée par le gouvernement du Canada avec le ministère de la Défense nationale. Le programme de subventions d'engagement ciblé « Mobiliser les connaissances en matière de défense et de sécurité » vise à stimuler l'innovation dans la réflexion sur les politiques de défense et à favoriser la prochaine génération d'experts en défense et en sécurité.* 



# The Role of the OHS Professional in Business Continuity

## Le rôle du professionnel de la santé dans la continuité des activités

By/Par V J McNeilly, MRSC, CFIOSH

**T**hroughout my career, I sought to ask a simple yet compelling question: “What if?” At times, I was met with a wall of delusional skepticism, believing that what I had asked was so far-fetched it could never happen.

Throughout our industrial history, numerous events have not been adequately assessed, and as a result, the loss of life and the loss of businesses, litter our history. Almost all events were preventable. How do we ensure we have done everything possible to prevent the event and the damage it could inflict on the business and its most valuable asset – its people?

**Occupational Health and Safety (OHS)** plays a crucial role in business continuity by ensuring that a company’s operations can continue smoothly, even in the face of potential disruptions.

We need to use our tools and valuable assets, including our people, to make the business robust and resilient. Business continuity and OHS each have well-established frameworks to address different organizational resilience aspects. The integration of these two frameworks ensures comprehensive risk management across all aspects of the business. We need to develop a system that embodies the Business Continuity process, its procedures, and activities to ensure the business continues to function with maximum operational impact while focusing on employee safety and operational continuity.

**T**out au long de ma carrière, j’ai cherché à poser une question simple mais convaincante : “Et si ?” Parfois, je me suis heurtée à un mur de scepticisme délirant, persuadée que ce que j’avais demandé était tellement farfelu qu’il ne pourrait jamais se produire.

Tout au long de notre histoire industrielle, de nombreux événements n’ont pas été évalués de manière adéquate et, par conséquent, des pertes humaines et des pertes d’entreprises ont émaillé notre histoire. Presque tous les événements auraient pu être évités. Comment s’assurer que l’on a fait tout ce qui était possible pour prévenir l’événement et les dommages qu’il pourrait infliger à l’entreprise et à son actif le plus précieux - son personnel ?

**La santé et la sécurité au travail (SST)** jouent un rôle crucial dans la continuité des activités en garantissant que les opérations d’une entreprise peuvent se poursuivre sans heurts, même en cas de perturbations potentielles.

Nous devons utiliser nos outils et nos actifs précieux, y compris notre personnel, pour rendre l’entreprise robuste et résiliente. La continuité des activités et la santé et la sécurité au travail disposent chacune de cadres bien établis pour traiter les différents aspects de la résilience organisationnelle. L’intégration de ces deux cadres garantit une gestion complète des risques dans tous les aspects de l’entreprise. Nous devons développer un système qui incarne le processus de

Throughout industry and across many sectors within our global village of work, there are events that are waiting for the opportunity to occur. The consequences often damage the organization in more ways than just the initial impact on disruption of business, the event has the potential of seriously damaging and destroying the very lifeblood of any business... it's people. We don't have to wait for the cyber-attack or Mother Nature; the workplace incident is a willing player in this game. We need to ensure controls are in place to prevent and protect people, processes and our planet.

The Business Continuity team consists of educated, qualified, and experienced people that are capable to assess and determine the risk from the potential harm that could result in significant business loss. In our world of work, the Health and Safety Professional, offers the team a unique insight into the potential for harm at the coal face of the business. They hold a body of knowledge that enables the team to take advantage of expertise in determining the consequences to ensuring business continuity by helping to establish preventive and protective measures, creating the Business Continuity Plan.

The **Health and Safety Plan (HSP)** is key to supporting and maintaining the command-and-control process developed, implemented and delivered in a business, by assisting in training senior executives through tabletop exercises on and off site. They enable scenarios to be played out in real time, ensuring the players understand their roles and what is needed to establish a control structure that has rigor and clarity from 'C'-suite to the seat of the incident and beyond the site perimeter to neighbours, the media and families.

continuité des activités, ses procédures et ses activités afin de garantir que l'entreprise continue à fonctionner avec un impact opérationnel maximal tout en se concentrant sur la sécurité des employés et la continuité des activités.

Dans l'ensemble de l'industrie et dans de nombreux secteurs de notre village mondial du travail, il y a des événements qui n'attendent que l'occasion de se produire. Les conséquences portent souvent atteinte à l'organisation de bien d'autres manières que l'impact initial sur l'interruption des activités, car l'événement a le potentiel d'endommager gravement et de détruire l'élément vital de toute entreprise... son personnel. Il ne faut pas attendre la cyber-attaque ou Dame Nature ; l'incident sur le lieu de travail est un acteur volontaire dans ce jeu. Nous devons veiller à ce que des contrôles soient mis en place pour prévenir et protéger les personnes, les processus et notre planète.

L'équipe chargée de la continuité des activités est composée de personnes instruites, qualifiées et expérimentées, capables d'évaluer et de déterminer les risques de dommages potentiels susceptibles d'entraîner des pertes importantes pour l'entreprise. Dans notre monde du travail, le professionnel de la santé et de la sécurité offre à l'équipe un point de vue unique sur les risques potentiels au sein de l'entreprise. Il possède un ensemble de connaissances qui permet à l'équipe de tirer parti de son expertise pour déterminer les conséquences et assurer la continuité des activités en aidant à mettre en place des mesures de prévention et de protection, en créant le plan de continuité des activités.

**Le plan de santé et de sécurité (PSS)** est essentiel pour soutenir et maintenir le processus de commandement et de contrôle élaboré, mis en œuvre et appliqué dans une entreprise, en contribuant à la formation des cadres supérieurs par le biais d'exercices sur table sur site et hors site. Ces exercices permettent de jouer des scénarios en temps réel, en veillant à ce que les acteurs comprennent leur rôle et ce qui est nécessaire pour établir une structure de contrôle rigoureuse et claire, de la suite "C" au siège de l'incident et, au-delà du périmètre du site, aux voisins, aux médias et aux familles.

Mise en place de la prévention et de la protection sur le lieu de travail Le PSH est à nouveau un membre clé de l'équipe chargée de mettre en place les contrôles qui permettront d'atténuer les effets de l'événement anormal. Il forme les acteurs de première ligne de l'entreprise, en

Establishing prevention and protection in the workplace the HSP is again a key member of the team in establishing the controls that will mitigate the abnormal event. The HSP trains the players on the front line of the business, ensuring everyone who has a role to play in the abnormal incident understands what is needed and the part they play in controlling the emergency.

The HSP is crucial in implementing effective occupational health and safety practices that safeguard employees and play a pivotal role in managing business risks. By systematically identifying hazards, assessing risks, and instituting control measures, the HSP ensures a safer work environment, which helps in reducing workplace incidents and related disruptions. Its integration into the Business Continuity Plan (BCP) is essential, as it aligns safety practices with broader operational strategies. This integration ensures that the procedures for handling safety issues are harmonized with those for maintaining business operations during events of disruption.

Consequently, the HSP and BCP together help minimize the impact of emergencies on business continuity, ensuring that the organization can continue to operate effectively even when faced with significant disruptions. This coordinated approach enhances organizational resilience and supports a seamless response to emergencies, safeguarding both employee well-being and business operations. They bring their competency and capability to the business team to establish and nurture an environment of ZERO HARM. Ω

veillant à ce que tous ceux qui ont un rôle à jouer dans l'incident anormal comprennent ce qui est nécessaire et le rôle qu'ils jouent dans la maîtrise de la situation d'urgence.

Le PSS est essentiel à la mise en œuvre de pratiques efficaces en matière de santé et de sécurité au travail, qui protègent les employés et jouent un rôle central dans la gestion des risques de l'entreprise. En identifiant systématiquement les dangers, en évaluant les risques et en instaurant des mesures de contrôle, le PSS garantit un environnement de travail plus sûr, ce qui contribue à réduire les incidents sur le lieu de travail et les perturbations qui y sont liées. Son intégration dans le plan de continuité des activités (PCA) est essentielle, car elle permet d'aligner les pratiques de sécurité sur des stratégies opérationnelles plus larges. Cette intégration garantit que les procédures de gestion des problèmes de sécurité sont harmonisées avec celles visant à maintenir les activités de l'entreprise en cas de perturbation.

Par conséquent, le HSP et le BCP contribuent ensemble à minimiser l'impact des urgences sur la continuité des activités, en garantissant que l'organisation peut continuer à fonctionner efficacement même lorsqu'elle est confrontée à des perturbations importantes. Cette approche coordonnée renforce la résilience de l'organisation et favorise une réponse transparente aux situations d'urgence, en préservant à la fois le bien-être des employés et les activités de l'entreprise. Ils apportent leurs compétences et leurs capacités à l'équipe de l'entreprise afin d'établir et d'entretenir un environnement ZERO HARM. Ω

### ABOUT THE AUTHOR

*Vince McNeilly is a seasoned professional in occupational health and safety with over 35 years of experience. He has managed and directed health and safety (HSE) in international organizations and operated globally to improve HSE, successfully around the globe. He has served as President of the International Network of Safety and Health Professional Organizations (INSHPO), a global alliance of professional safety organizations. Today, he operated a successful consulting firm in Europe, working with organizations worldwide.*



### À PROPOS DE L'AUTEUR

*Vince McNeilly est un professionnel chevronné de la santé et de la sécurité au travail, avec plus de 35 ans d'expérience. Il a géré et dirigé des services de santé et de sécurité (SST) dans des organisations internationales et a travaillé à l'échelle mondiale pour améliorer la SST, avec succès dans le monde entier. Il a été président de l'International Network of Safety and Health Professional Organizations (INSHPO), une alliance mondiale d'organisations professionnelles de sécurité. Aujourd'hui, il dirige un cabinet de conseil prospère en Europe, qui travaille avec des organisations du monde entier.*

# Implications of a Cyber Breach

## Implications d'une cyber-fraude



*By/Par Garth Tucker, CBCP, CORP*

# Implications of a Cyber Breach

**In** 2000/2001, I was in Moscow teaching people how to use Linux for a world-wide business machine organization that shall remain nameless (they walk softly and carry a big lawyer.)

There were some extremely talented people in the course, I felt like they should be teaching me at times. Think Chief Software Engineers with the former Soviet space agency...

Rocket scientists.  
Great.  
No pressure.

I got to know these folks well and they were very friendly and open once they got to know me, and we had some great conversations around the future of Linux and MS, etc. The one that stuck out most to me however was regarding what happened when the Soviet Union disintegrated (yay Capitalism 😊). As they said, up to that point, everyone worked for the State, then suddenly there was no state. What now? They kept going to work because at least the coffee was free.

Then out of the blue, several scary looking guys walked in and told many of the staff that they work for them now. The Russian Mafia saw the opportunity to steal from the sitting ducks in the West without having to risk being shot by police, and Cyber Theft was born.

## Think about this.

For years, some seriously smart, well-educated computer scientists / engineers were poking holes in our security before we even knew they were attempting to gain access. Honestly, until 5 or so years ago, most people couldn't spell Cybersecurity, let alone build a program to combat it. We lost battles before we even knew we were in them, and we aren't even touching on State Sponsored attacks.

# Implications d'une cyber-fraude

**En** 2000/2001, j'étais à Moscou pour enseigner aux gens comment utiliser Linux pour une organisation mondiale de machines commerciales qui restera anonyme (ils marchent doucement et portent un grand avocat).

Il y avait des gens extrêmement talentueux dans le cours, j'avais l'impression que c'était eux qui devaient m'enseigner à certains moments. Pensez aux ingénieurs logiciels en chef de l'ancienne agence spatiale soviétique...

Les scientifiques des fusées.  
Très bien.  
Pas de pression.

J'ai appris à bien connaître ces gens et ils ont été très amicaux et ouverts une fois qu'ils m'ont connu, et nous avons eu d'excellentes conversations sur l'avenir de Linux et de MS, etc. La conversation qui m'a le plus marqué concerne ce qui s'est passé lorsque l'Union soviétique s'est désintégrée (yay Capitalism 😊). Comme ils l'ont dit, jusqu'à ce moment-là, tout le monde travaillait pour l'État, et soudain, il n'y a plus d'État. Et maintenant ? Ils ont continué à aller travailler parce qu'au moins le café était gratuit.

Puis, tout à coup, plusieurs types à l'air effrayant sont entrés et ont dit à de nombreux membres du personnel qu'ils travaillaient désormais pour eux. La mafia russe a vu là l'occasion de voler les cibles faciles de l'Occident sans risquer de se faire tirer dessus par la police, et le cybervol est né.

## Pensez-y.

Pendant des années, des informaticiens/ingénieurs très intelligents et bien formés ont percé des trous dans notre sécurité avant même que nous sachions qu'ils tentaient d'y accéder. Honnêtement, jusqu'à



## Where does this leave us?

While we were starting from way behind in this war and lost the initial battles, there are some very smart people in the West as well and we've rallied and they are fighting the good fight to protect us, but we're still fighting from low ground. In the meantime, we are tasked with finding solutions to mitigate, thwart, blunt, or marginally disrupt the impact of cyber breaches.

### Let's discuss the implications of a cyber breach.

#### *Reputational harm*

No question, once your customer data has been compromised, they're going to blame you and your reputation is going to take a hit.

Your Enterprise Risk Management (ERM) Team will undoubtedly have this as a line in their risk registers, and your DRI Certified Business Continuity Professional will have looked at this in their Risk Assessment (RA)

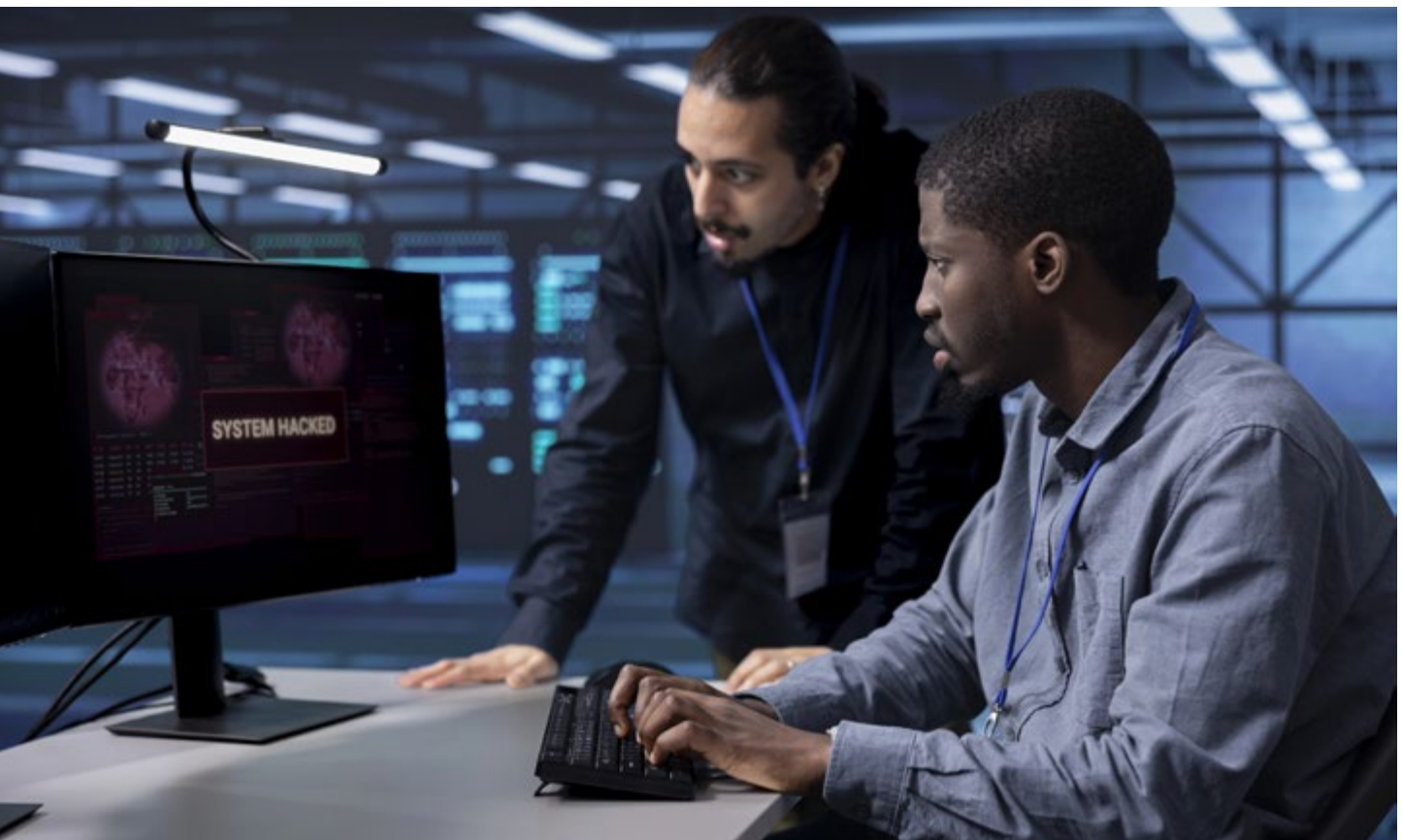
– **DRI Professional Practice 2** –

so it's up to the business how much effort and financial support they are willing to provide to offset this damage based on the output of these processes.

Honestly, at this point, many people have become so used to the idea of their data being sold on the Dark Web, it's almost become blasé. They aren't happy about it, but it's a fact of life in today's world. Every day I see stories about another well-known organization being a victim. So, your reputational impact may not be as severe as it was 5 or 10 years ago, but do you really want to test the theory? Personally, I pay both Equifax and Trans Union to monitor my data and inform me of any issues, just another life cost, like auto or home insurance.

#### *Breaches of contract*

This is becoming a part of many contracts / SLAs when dealing with public sector, the banking industry, or other financial organizations. You must indemnify them against losses resulting from cyber breaches



il y a environ 5 ans, la plupart des gens ne savaient pas épeler cybersécurité, et encore moins construire un programme pour la combattre. Nous avons perdu des batailles avant même de savoir que nous y étions engagés, et nous ne parlons même pas des attaques parrainées par les États.

### Où cela nous mène-t-il ?

Bien que nous soyons partis de loin dans cette guerre et que nous ayons perdu les premières batailles, il y a aussi des gens très intelligents à l'Ouest et nous nous sommes ralliés et ils mènent le bon combat pour nous protéger, mais nous nous battons toujours à partir d'un terrain bas. En attendant, nous sommes chargés de trouver des solutions pour atténuer, contrecarrer, éteindre ou perturber marginalement l'impact des cyber-attaques.

### Examinons les conséquences d'une cyber-fraude.

#### Atteinte à la réputation

Il ne fait aucun doute qu'une fois que les données de vos clients auront été compromises, ils vous blâmeront et votre réputation en pâtira.

Votre équipe de gestion des risques d'entreprise (ERM) aura sans aucun doute inscrit ce point dans son registre des risques, et votre professionnel certifié en continuité des activités (DRI) l'aura examiné dans son évaluation des risques (RA) - pratique professionnelle 2 de DRI - il appartient donc à l'entreprise de déterminer les efforts et le soutien financier qu'elle est disposée à fournir pour compenser ces dommages sur la base des résultats de ces processus.

Honnêtement, à ce stade, de nombreuses personnes se sont tellement habituées à l'idée que leurs données soient vendues sur le Dark Web qu'elles en sont presque devenues blasées. Ils n'en sont pas heureux, mais c'est une réalité dans le monde d'aujourd'hui. Chaque jour, je vois des histoires sur une autre organisation bien

connue qui a été victime. L'impact sur votre réputation n'est peut-être pas aussi grave qu'il y a 5 ou 10 ans, mais avez-vous vraiment envie de tester la théorie ? Personnellement, je paie Equifax et Trans Union pour qu'ils surveillent mes données et m'informent de tout problème, ce qui représente un coût supplémentaire dans la vie, comme l'assurance automobile ou l'assurance habitation.

#### Rupture de contrat

Cette disposition fait de plus en plus partie de nombreux contrats ou accords de niveau de service (SLA) avec le secteur public, l'industrie bancaire ou d'autres organisations financières. Vous devez les indemniser en cas de pertes résultant de violations cybernétiques et des contrats, car ils invoqueront probablement une rupture de contrat, ce que les tribunaux canadiens ont confirmé.

*Owsianik c. Equifax Canada Co,*  
2022 ONCA 813,

*Obodo c. Trans Union of Canada, Inc.*  
2022 ONCA 814, et

*Winder c. Marriott International, Inc,*  
2022 ONCA 815.

Ces trois décisions concernaient des propositions d'actions collectives dans le cadre desquelles

- Le groupe proposé est composé de personnes dont les informations personnelles ont été (ou sont supposées avoir été) compromises dans le cadre d'une violation de données.
- Le défendeur est l'entreprise qui a traité et stocké les informations personnelles ; et
- La violation de données a été perpétrée par des pirates informatiques tiers non identifiés.

(al, 2022) <https://www.torlys.com/en/our-latest-thinking/publications/2022/11/liability-for-cyber-attacks-clarified-by-ontario-court-of-appeal>



and the contracts as they will likely claim a breach of contract and Canadian courts have upheld this.

*Owsianik v. Equifax Canada Co.*,  
2022 ONCA 813,

*Obodo v. Trans Union of Canada, Inc.*,  
2022 ONCA 814, and

*Winder v. Marriott International, Inc.*,  
2022 ONCA 815.

All three decisions involved proposed class actions where:

- The proposed class are individuals whose personal information was (or is alleged to have been) compromised in a data breach
- The defendant is the company that handled and stored the personal information; and
- The data breach was perpetrated by unidentified third-party hackers.

(al, 2022) <https://www.torys.com/en/our-latest-thinking/publications/2022/11/liability-for-cyber-attacks-clarified-by-ontario-court-of-appeal>

Reach out to corporate counsel and have them assess your legal vulnerability and use this assessment to help drive your response posture and program goals.

#### *Financial loss*

This is probably where most people's thoughts go when you mention cyber breach and there's a good reason for that, because the criminals who attack organizations are doing this for the money. Not high-minded, freedom fighting reasons, strictly financial gain.

The immediate thought is payouts to affected users through class action suits, remuneration for missing funds, paying for credit monitoring, etc. These are all very real costs but are one-time expenses.

The bigger costs are things such as increased (if you're fortunate enough to keep it) insurance premiums and deductibles, loss of business / revenue, higher expenditures on prevention (more staff and software), legal costs – your payouts to law firms are going

Demandez aux conseillers juridiques de l'entreprise d'évaluer votre vulnérabilité juridique et utilisez cette évaluation pour vous aider à définir votre position de réponse et les objectifs de votre programme.

### *Perte financière*

C'est probablement ce qui vient à l'esprit de la plupart des gens lorsque l'on évoque les cyberattaques, et il y a une bonne raison à cela : les criminels qui s'attaquent aux organisations le font pour l'argent. Il ne s'agit pas de raisons nobles de lutte pour la liberté, mais strictement de gains financiers.

L'idée qui vient immédiatement à l'esprit est celle des indemnités versées aux utilisateurs concernés dans le cadre de recours collectifs, de la rémunération des fonds manquants, du paiement de la surveillance du crédit, etc. Tous ces coûts sont bien réels, mais il s'agit de dépenses ponctuelles.

Les coûts les plus importants sont les suivants : augmentation des primes d'assurance et des franchises (si vous avez la chance de les conserver), perte d'activité/ de revenus, augmentation des dépenses de prévention (personnel et logiciels supplémentaires), frais juridiques - les sommes versées aux cabinets d'avocats seront astronomiques si vous choisissez de combattre votre responsabilité ou si vous ne souscrivez pas d'assurance cybernétique, et enfin, la campagne de relations publiques que vous devrez peut-être mettre en place pour rétablir votre réputation.

Ces problèmes peuvent s'éterniser pendant des mois, voire des années, et les coûts qui en découlent ont de graves répercussions sur l'ensemble de l'organisation.

Vous devrez consacrer des ressources pour vous assurer que votre personnel connaît les techniques d'hameçonnage, d'ingénierie sociale, etc., car c'est par là que la plupart des cyberattaques commencent et accèdent à votre organisation. Envisagez

de retirer des cycles de productivité au personnel pour vous assurer qu'il n'est pas responsable d'une violation au lieu de générer des revenus. Il n'y a pas de question, la cyberpréparation est un centre de coûts, mais vous ne pouvez pas choisir de le négliger (contrairement à ceux qui se mettent la tête dans le sable avec la reprise après sinistre et la continuité des activités).

### **Quelle est la réponse ?**

J'aimerais avoir de meilleures nouvelles pour vous, mais il n'y a pas qu'une seule réponse pour résoudre votre dilemme en matière de cyber-réponse, et il faut se rabattre sur un dicton éculé : "Une once de prévention vaut une livre de remède".

Voici quelques éléments qui me paraissent importants,

- **Embaucher les meilleurs talents en matière de cybersécurité.** Investissez dans leur formation et veillez à ce qu'ils aient accès aux outils dont ils ont besoin. J'ai la chance de travailler avec des personnes très expérimentées qui me facilitent grandement la tâche en se chargeant de la planification et de l'organisation de la réponse. Je l'intègre simplement dans la posture de résilience globale.
- **Travaillez en étroite collaboration avec votre assureur et son service d'intervention.** Identifiez et intégrez les étapes qu'ils proposent dans vos processus et veillez à ce que toutes les personnes de votre organisation qui participent à la surveillance et à l'intervention les connaissent aussi bien que leur date d'anniversaire et leur adresse.
- **Recherchez en dehors de votre environnement des experts en matière de préparation et de réaction.** Surtout en matière d'intervention. D'après ce que l'on m'a raconté, les organisations de lutte contre le cyber-vol ne sont pas à la portée des personnes inexpérimentées, n'essayez pas de vous en occuper vous-même. Les



to be astronomical if you choose to fight your liability or don't carry cyber insurance, and finally, the public relations campaign you may have to mount in order to recover your reputation.

These things can drag on for months or years and the costs will have a serious knock-on effect on the entire organization.

Another financial implication will be in staff training. You will be dedicating resources to ensuring your staff are aware of phishing, social engineering, etc. as this is where most cyber attacks typically begin and gain access to your organization. Consider taking productivity cycles away from staff to ensure they're not responsible for a breach instead of driving revenue. There's no question, cyber prep is a cost center, but one you cannot choose to overlook (unlike those who put their heads in the sand with disaster recovery and business continuity.)

### **What's the answer?**

Wish I had better news for you, but there isn't just one answer to solve your Cyber response dilemma, but to fall back on a hackneyed saying, "An ounce of prevention is worth a pound of cure."

Here are a few things that come to my mind as important,

- **Hire top Cyber Security talent.** Invest in their training and ensure they have access to the tools they require. I'm fortunate to work with some very experienced folks who make my job far easier by taking on the response planning and organization. I simply integrate it into the overall resilience posture.
- **Work closely with your insurance provider and their response resource.** Identify and incorporate the steps they provide into your processes and ensure all those within your organization who are part of monitoring and response know them as well as they know their birthdays and addresses.

- **Look outside your environment for experts in preparation and response.** Especially response. From stories I've been made privy to, dealing with cyber theft organizations is not something for the inexperienced, don't try and run this yourself. They, the villains, are very professional and organized. To steal a quote, "They had a better help desk process than Microsoft" including a guided process to obtain bitcoin and how to transfer the keys. You cannot be lulled into thinking they're your friends, leave this to the professional responders from organizations that specialize in cyber breach response, such as Booz Allen.

- **Work with your government agencies and/or law enforcement.** Follow their guidelines and advice. Here in Canada, Public Safety Canada, the RCMP, and CSIS provide guidance and standards for cyber. Use them. In the past, I was involved in a program that provided advice on critical infrastructure for a Canadian province that included the organizations mentioned, as well as others including public utilities, local law enforcement, other municipal and provincial emergency management groups, and large private enterprise organizations. We all benefitted from these groups' knowledge and experience in security.

- **Treat Cyber as you do any other business unit.** Develop a program, implement policies, and hire top people to manage that program. Ensure there is adequate budget for training, both cyber staff and for all other staff, buy the right tools and consulting (penetration testing is critical), and have your program audited by outside experts on a regular basis.
- **Exercises.** If you aren't prepared to react in seconds to a breach, you're adding to the impact. Running through



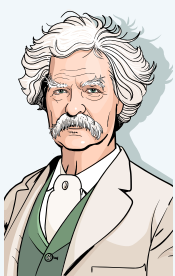
malfructeurs sont très professionnels et organisés. Pour reprendre une citation, “ils avaient un meilleur service d’assistance que Microsoft”, y compris une procédure guidée pour obtenir des bitcoins et comment transférer les clés. Ne vous laissez pas bercer par l’idée qu’ils sont vos amis, laissez cela aux professionnels d’organisations spécialisées dans la réponse aux cyberattaques, telles que Booz Allen.

• **Travaillez avec vos agences gouvernementales et/ou les forces de l’ordre.** Suivez leurs lignes directrices et leurs conseils. Au Canada, Sécurité publique Canada, la GRC et le SCRS fournissent des conseils et des normes en matière de cybercriminalité. Consultez et . Dans le passé, j’ai participé à un programme de conseil sur les infrastructures critiques pour une province canadienne qui comprenait les organisations mentionnées, ainsi que d’autres, notamment les services publics, les forces de l’ordre locales, d’autres groupes

de gestion des urgences municipaux et provinciaux, et de grandes entreprises privées. Nous avons tous bénéficié des connaissances et de l’expérience de ces groupes en matière de sécurité.

• **Traitez le cyberspace comme n’importe quelle autre unité commerciale.** Élaborez un programme, mettez en œuvre des politiques et engagez des personnes de haut niveau pour gérer ce programme. Veillez à ce qu’un budget suffisant soit consacré à la formation du personnel cybernétique et de tous les autres employés, achetez les outils et les services de conseil adéquats (les tests de pénétration sont essentiels) et faites régulièrement auditer votre programme par des experts externes.

• **Exercices.** Si vous n’êtes pas prêt à réagir en quelques secondes à une violation, vous en aggravez l’impact. En passant en revue les processus et en veillant à ce que toutes les personnes concernées connaissent leur



**Mark Twain Quote:**

“Good decisions come from experience. Experience comes from making bad decisions.”

**Citation de Mark Twain :**

« Les bonnes décisions viennent de l’expérience. L’expérience vient de la prise de mauvaises décisions. »



the processes and ensuring all involved knows their roles reduces your time required to react and makes your reaction(s) more efficient. This is not a polite suggestion, if you haven't exercised your cyber breach response, you're playing with a loaded gun that has a hair trigger.

The response to these impacts, both financial and reputational, should be driven by the output calculations from the RA and Business Impact Analysis (BIA) – **DRI Professional Practice 3**. These numbers don't lie, they're based in factual data, not feelings or opinions, and the same holds true for other aspects of the corporate resilience posture. Things such as your Recovery Time and Point Objectives (RTO & RPO) come out of the process as well, and it should be what drives your backup and recovery approach and how much you should invest.

Hope this very brief overview into some of the implications of a Cyber attack will help you get moving towards making your environment more secure.  
Keep your head up! Ω

---

### ABOUT THE AUTHOR

**Garth Tucker** *a seasoned resilience management professional with more than 20 years of experience. Garth has responded to many crisis events over the years; from the "Lights Out" of 2003 in Ontario, Canada, to the 2018 tragedy in Humboldt, SK as a Planning Section Chief, and has quarterbacked corporate responses to climate crisis events such as wildfires in Alberta and Nova Scotia, and hurricanes in Texas, Florida, and Eastern Canada. Two term member of the board of directors for the Disaster Recovery Institute Canada (DRIC), and currently, editor-in-chief of True North Resilience magazine. A frequent contributor to industry magazines and speaker at conferences, he was the winner of the 2023 DRI Canada Builder of the Year Award. He also develops Business Continuity type stuff as Director of BC for a multinational SaaS organization.*



rôle, vous réduisez le temps nécessaire pour réagir et vous rendez votre (vos) réaction(s) plus efficace(s). Il ne s'agit pas d'une suggestion polie : si vous ne vous êtes pas exercé à réagir en cas de cyberintrusion, vous jouez avec un pistolet chargé dont la gâchette est en forme de cheveu.

La réponse à ces impacts, à la fois financiers et réputationnels, devrait être guidée par les calculs des résultats de l'AR et de l'analyse d'impact sur les activités (BIA) - Pratique professionnelle 3 de la DRI. Ces chiffres ne mentent pas, ils sont basés sur des données factuelles, et non sur des sentiments ou des opinions, et il en va de même pour d'autres aspects de la posture de résilience de l'entreprise. Des éléments tels que vos objectifs de temps et de point de récupération (RTO & RPO) sont également issus du processus, et c'est ce qui devrait déterminer votre approche en matière de sauvegarde et de récupération, ainsi que le montant de vos investissements.

J'espère que ce très bref aperçu des implications d'une cyberattaque vous aidera à rendre votre environnement plus sûr.  
Gardez la tête haute ! Ω

---

### À PROPOS DE L'AUTEUR

**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.*



VIRTUAL / VIRTUEL  
NOVEMBER 21, 2024



VANCOUVER  
MARCH 25, 2025

### Virtual Symposium on Business Continuity, Cyber Resilience, and Disaster Management

Join us for an immersive one-day virtual symposium designed specifically for professionals in business continuity, cyber resilience, disaster management, and crisis communications. This event promises to be an engaging and thought-provoking experience, bringing together experts and thought leaders from across the industry to share insights, strategies, and the latest developments in the field.

#### Event Highlights

**Thought-Provoking Discussions:** Engage with industry experts in deep, insightful discussions on the most pressing issues and emerging trends in business continuity and disaster management.

**Expert Panels:** Hear from seasoned professionals and thought leaders in cyber resilience and crisis communications, offering diverse perspectives and actionable advice.

**Interactive Sessions:** Participate in interactive workshops and Q&A sessions designed to foster collaboration and knowledge sharing.

**Networking Opportunities:** Connect with fellow professionals, share experiences, and build valuable relationships within the business continuity community.

### Symposium virtuel sur la continuité des activités, la cyberrésilience et la gestion des catastrophes

Joignez-vous à nous pour un symposium virtuel immersif d'une journée conçu spécifiquement pour les professionnels de la continuité des activités, de la cyberrésilience, de la gestion des catastrophes et des communications de crise. Cet événement promet d'être une expérience engageante et stimulante, réunissant des experts et des leaders d'opinion de l'industrie pour partager des idées, des stratégies et les derniers développements dans le domaine.

#### Faits saillants de l'événement

**Discussions stimulantes :** Engager avec des experts de l'industrie dans des discussions approfondies et perspicaces sur les questions les plus urgentes et les tendances émergentes en matière de continuité des activités et de gestion des catastrophes.

**Groupes d'experts :** Écoutez des professionnels chevronnés et des leaders d'opinion en matière de cyberrésilience et de communications de crise, offrant divers points de vue et des conseils pratiques.

**Séances interactives :** Participer à des ateliers interactifs et à des séances de questions-réponses conçus pour favoriser la collaboration et le partage des connaissances.

**Occasions de réseautage :** Connectez-vous avec d'autres professionnels, partagez des expériences et établissez des relations précieuses au sein de la communauté de la continuité des activités.

---

# DRI CANADA

2024-2025 BOARD OF DIRECTORS



## REGIONAL DIRECTORS

TROY MCQUINN, atlantic  
PATRICK LEDUC, quebec  
JASON FIRLOTTE, ontario  
BROCK HOLOWACHUK, central  
JEFF HORTOBAGYI, pacific

---

## COMMISSION CHAIRS

REJEAN PESANT  
STEVE PALUBISKI

---

## DIRECTORS AT LARGE

ANDREA BUCHHOLZ  
BRENDA ESCRIBANO  
NANCY HOLLOWAY-WHITE  
ALEXANDER LANDRY  
SCOTT LEAVITT  
LISA MADDOCK  
JEREMY PAULUS  
GREG SOLECKI

[Return to TOC](#)

[Retour au sommaire](#)