

Business Continuity Plans Are Vital, Especially During a Crisis

The Disaster Recovery Institute International has spent decades training and certifying business continuity professionals. Here are its tips for coming back from a pandemic.

Janice Tober



Chloe Demrovsky
President & CEO,
Disaster
Recovery Institute
International (DRI)



John Yamniuk
President,
Disaster Recovery
Institute Canada
(DRI Canada)

In the era of the COVID-19 pandemic, one thing is clear: a worldwide disaster can happen at any time and businesses need to prepare for worst-case scenarios.

While many companies and governments employ risk specialists — those who work to avoid potential crises — on their teams, many also include resiliency experts. These forecasters play important roles in predicting potential disasters that can’t be avoided and in evaluating how to best manage these events. They focus on preparedness, disaster recovery, and business continuity when times are tough.

“Whether managing through COVID-19 or any other type of disaster, resilient organizations need to be prepared to adapt and respond in a complex and changing environment in order to continue to provide products and services and to survive. Business continuity, or continuity of operations, plans are a key component to have in place — particularly as we manage through COVID-19 and move into a new normal,” says John Yamniuk, President of the Disaster Recovery Institute Canada.

The key is planning

The Disaster Recovery Institute International (DRI) is the leading global non-profit organization that trains and certifies resilience professionals around the world in order to help businesses prepare for, and recover from, disasters. DRI Canada is the governing body that delivers training and oversees certification in Canada. Each year, the DRI consults with certified members before publishing its annual predictions report, which incorporates feedback from 15,000 thought leaders in over 100 countries.

“Our members are valuable resources for determining what keeps organizations up at night. The report highlights projected threats organizations could face, allowing them to identify areas of deficiency in preparedness,” says Chloe Demrovsky, President and CEO of DRI.

Although pandemics are difficult to predict, they’re not unprecedented and, by late

February of this year, most resilience experts already had a plan in place for the pandemic. “In the early days, we were thinking that this would be like SARS. We expected supply chain disruptions and we were looking at how companies could operate with 35 to 40 percent of their workforces out sick,” says Demrovsky.

As the virus spread, continuity plans had to evolve. As Demrovsky says, “The necessary public health response to controlling COVID-19 has impacted organizations by impeding their ability to operate.”

While some organizations — even entire cities — had good resiliency strategies in place, others are not faring as well. Demrovsky believes that every organization needs to have a business continuity plan in place. “The pandemic is affecting every organization in a different way, but resilience planning means looking at the risks that could affect you and the potential impact on your organizations, and then having a set of tools that you can apply when something happens. It gives you a head start because you’ve been thinking about it in advance. That’s what business continuity planning is all about.”

Tips to help companies reopen during the COVID-19 pandemic

As organizations look at reopening, Demrovsky has some advice on crisis recovery. “To get back up and running, organizations need to look at operational components and to figure out what their responsibilities are in terms of health and safety for employees and customers with regards to testing,

contact tracing, temperature checks, and personal protective equipment,” she says. “Next, organizations need to think about human resources issues, such as health care, worker anxiety, and childcare, particularly as schools will remain closed for the remainder of the school year.”

The final step is to communicate with all stakeholders. “People want to go back out into the world and re-engage, but they’re

nervous. Organizations need to actively tell stakeholders the safety measures they’ve put in place to reassure them that safety is a priority,” says Demrovsky. In addition to following requirements of federal, provincial, territorial, and local governing bodies, some safety measures might include shutting common spaces, enforcing social distancing, staggering shifts, limiting numbers of people on the premises, and having staff visibly

disinfecting surfaces.

“Ultimately, leaders need to be decisive,” says Demrovsky. “They have to be empathetic and make quick decisions in the beginning of a crisis. And then they have to communicate and over-communicate: ‘We understand. We see what’s happening. This is what we’re doing. This is what we know. This is what we don’t know. And I’m here. I’m here to help. I’m here to listen. Let me know what you need. And let’s talk about it.’”

Demrovsky continues, “The good news is that this can be planned and tested in advance. It’s important to always be planning for uncertainty. And those organizations that respond well will thrive and continue to provide products and services.” ■

The pandemic is affecting every organization in a different way, but resilience planning means looking at the risks that could affect you and the potential impact on your organization, and then having a set of tools that you can apply when something happens.

i

Being prepared is the key to mitigating the damage of — and recovering from — a crisis. For resources to help your business with disaster recovery planning and continuity management, visit drii.org and dri.ca.

This article was **sponsored by DRI Canada.**



DRI’s 5th Annual Predictions Report 2020: *Outlook for a Turbulent World*

The COVID-19 pandemic has emphasized the importance of preparedness within organizations. To aid in the process of preparedness, the DRI Future Vision Committee (FVC) has produced an annual set of predictions since 2015. Drawn from a wide range of subject areas and based on the research and opinions of the highly-experienced professionals that make up the FVC, this report can help ensure your organization is ready for any other surprises that 2020 may bring.

1 Technology Risks
Record number of ransomware attacks



2 Infrastructure
State-sponsored attack on a G8 institution



3 Extreme Weather
Several extreme weather events



4 Civil Unrest
Increasing global civil unrest



5 Geopolitics
Increased tension between US and traditional allies



6 Financial Crisis
Financial downturn similar to 2008



7 China’s Influence
Increasing Chinese influence in developing world



8 Social Media
Increasing social media activism



9 Resource Shortages
Electricity and water shortages globally



10 Transportation
Legal challenge to safety algorithms in transportation



To be prepared and for further information, analysis, and to see the full report, visit dri.ca.

Designing Your Reopening Infection Control Program

Brought to you by Environmental Consulting Occupational Health (ECOH) and the Disaster Recovery Information Exchange Toronto (DRIE)

With some of the COVID-19 pandemic restrictions starting to be lifted, many workplaces are faced with difficult decisions about how to re-start operations without jeopardizing the health of their employees, clients, or customers. This requires some systematic thinking about how to institute a workplace infection control program.

It's important to start by assessing the risks your operations pose to spreading infection. To conduct your risk assessment, think about all the processes in your workplace that could lead to infection through airborne droplets or aerosols (small particles) or contact with infected surfaces.

Then, develop a program to prevent those risks. Om Malik, CEO of Environmental Consulting Occupational Health (ECOH), an Ontario environmental and health and safety consulting firm, uses the acronym DOT — Design, Oversight, Test — to describe what's needed. The Design

process can involve re-arranging work to promote physical distancing and low-touch processes. For example, continue remote work where possible to reduce the number of people in the workplace. This will make it easier to space workstations and people in such a way so as to maintain a two-metre physical distance. Marking two-metre distances and designating corridors and stairways as one-way will help. Avoid shared equipment as much as possible. Plexiglass barriers, face shields, and masks will also help prevent infection spread. You will need special protocols for lunchrooms, elevators, and washrooms. Plan for emergencies like someone getting sick while at work. Train your staff in all requirements.

You'll need to screen visitors and staff and prevent entry to anyone who has COVID-19 symptoms or has travelled outside Canada in the last 14 days. If possible, inform visitors, customers, and clients about your procedures before they arrive to streamline entry.

You may want to use a visitor management system with COVID-19 screening.

Changes to ventilation systems and cleaning procedures may also be necessary. While infection control programs have typically been found in health care facilities, "With the onset of the novel coronavirus, infection control programs will now be the new normal for all commercial building environments," says Matt Johnson, President and CEO of Commercial Loss Experts and Member of the Board of Directors of the Disaster Recovery Information Exchange Toronto (DRIE). "It's important that you have a pre-established relationship with service providers that are equipped and skilled at decontamination and disinfection," he adds.

Finally, don't forget the Oversight and Test components of DOT. As Malik says, "You need to oversee your program to make sure it's done right, and test to make sure you got it right." ■



Om Malik
CEO,
Environmental
Consulting
Occupational Health
(ECOH)



Matt Johnson
President & CEO,
Commercial Loss
Experts, and Member
of the Board of
Directors, Disaster
Recovery Information
Exchange Toronto
(DRIE)

There's Light at the End of the Tunnel for Pandemic-Stricken Businesses

To find out how the pandemic has affected Canadian companies and how they can weather this storm, Mediaplanet spoke with Yohaán Thommy, Consulting Partner with MNP's Consulting Services team who leads the firm's performance improvement practice.



Yohaán Thommy
Consulting Partner,
MNP

What's the current state of Canada's business environment?

The pandemic has caused a lot of disruption. Many small- and medium-sized businesses don't have access to financial relief, so they'll have to plan to run their operations with less cash and more inventory as supply chains move from "just in time" to "just in case."

How should businesses react in general?

A lot of owners are worried about being resilient in the short term — they're focused on gross margins, but they would be better served by focusing on other issues, such as return on investment in terms of cost and time commitment.

What are a few of the specific steps a small business should take to adapt?

First, companies should get employees back to work. A majority of companies will experience a significant change, so they should look at ways to adjust their business models and sales channels. Some customers who were historically uncomfortable operating in a digital world may be changing their prefer-

ences. This is creating new business dynamics going forward.

Companies should prepare weekly cash flow forecasts for at least the next three to eight months to understand your cash flow needs and to determine how long your business can continue without burning through your working capital.

Small businesses should also identify all their critical accounts. Reach out to all the customers who represent critical accounts to understand how their needs have shifted and how to best meet those needs.

Another step is to manage your payables carefully. Prioritize important vendors when timing payments. For other vendors, discuss flexible or extended payment options.

Also, building many relationships and partnerships is a key aspect of resilience. If you're a business owner who's been relying on one supplier, change that.

What lies ahead?

We've yet to see the full economic impact of the pandemic. It will affect every aspect of industry, including supply chains. Compan-

This disruption is also creating new opportunities. Successful companies will adapt to the change.

ies will have to invest in risk management planning to identify the challenges and employ solutions to meet them. All this can prove costly, so smaller companies will go out of business unless their value propositions aren't based on price.

However, this disruption is also creating new opportunities. Successful companies will adapt to the change.

Small- and medium-sized businesses and entrepreneurs are encouraged to make MNP, a leading chartered accountancy and business advisory firm, their partner in business recovery. ■

Organizational Resilience Is Key to Successful Planning and Response

Christopher Horne

Globally, the COVID-19 pandemic may be the most significant disruption facing organizations of all sizes. In order to provide insight and guidance on potential incident responses, the Business Continuity Institute (BCI) has been gathering details on a regular basis about real actions taken by organizations across diverse industries through its international survey, Coronavirus: Organizational Preparedness, available online at thebci.org.

In its most recent report, the BCI highlighted the following trends, among others:

■ **Mental health is a key consideration.** 75 percent of organizations are now including mental health in their response plans.

■ **Organizations are expanding their supply chain reviews.** 60 percent have

reviewed the business continuity plans of tier one suppliers and beyond.

■ **Organizations are looking at the sustainability of their plans.** 61 percent have revised their business impact analysis to reflect changing priorities given the sustained impact of the pandemic. Additionally, 65 percent have evaluated their plans to ensure they can maintain the required level of support over the long haul.

■ **A majority of respondents are conducting scenario analyses, financial modelling, or both.** 55 percent have now undertaken scenario analysis to identify a range of potential outcomes and estimated impacts and 61 percent have undertaken financial modelling to determine how the organizations will be affected post-pandemic.

■ **Even so, planning for the next phase is limited.** Only 55 percent have considered their plans in the eventuality of a second or third wave.

In *Coronavirus — A Pandemic Response*, the BCI reports that 25 percent of organizations plan to return to the "old normal." To plan for the "new normal," progressive organizations are looking at investing in resilience, which is a more strategic and proactive focus on long-term viability.

Business continuity principles and practices are an essential contribution for an organization seeking to develop and enhance effective resilience capabilities to ensure that they can continue to support employees and meet customer public service expectations during the next inevitable incident. ■



Christopher Horne
Vice-Chair,
Business Continuity
Institute (BCI),
and Assistant
Vice President,
Business Continuity
Management,
Canada Life &
Great-West Lifeco



STRENGTHEN YOUR BUSINESS CONTINUITY AND RESILIENCE

- > WEB BASED BCM SOLUTION
- > CONSULTING SERVICES
- > CERTIFIED TRAINING

CONTACT US
1.877.761.6222
[premiercontinuum.com](https://www.premiercontinuum.com)

A LEADER IN
GARTNER MAGIC
QUADRANT



Create a Secure Network for Your Remote Employees

Companies dealing with a remote workforce in difficult circumstances have tools to make it easier and more secure for employees.

Ted Kritsonis

The COVID-19 pandemic forced a mass migration of the workforce from the office to the home, putting cybersecurity at the forefront for organizations managing employees remotely.

Statistics Canada reported that about 40 percent of Canadian employees began working from home because of the pandemic in late March, amounting to 6.7 million workers when you include the 1.8 million who were already working from home.

The cumulative number is a big chunk of the country's working population. With close to five million suddenly setting up shop at home because of shelter-in-place orders, IT personnel have had to ensure their corporate networks can maintain the same level of security with employees' personal devices.

"Visibility and control become factors with remote workforces, so having endpoint protection, cloud management for both public clouds and applications, and the right policies in place to protect data and users is important," says Ivan Orsanic, Regional Vice President and Country Manager at Palo Alto Networks.

Enabling access from anywhere

To adapt to a remote workforce and make the transition feel seamless for employees — and to have minimal impact on users — companies need to approach the issue from a few different angles. Orsanic points to Palo Alto Networks Prisma Access as a good start — a cloud-delivered secure access service edge (SASE) platform that allows users to securely access the internet from anywhere.

Such a tool works well with the company's GlobalProtect "Always On" virtual private network (VPN) connection to enable secure and direct access for mobile users connecting with their personal devices, Orsanic adds.

This way, an organization would be able to see and control all application traffic to ward off threats and protect all data.

This is done on a per-user basis, rather than only per IP address. A next-generation firewall can filter in good connections, though it would still look for anything out of the ordinary to prevent data loss.

"Organizations can still utilize their existing networking infrastructure, like public or private clouds, and virtual or physical firewalls, for instance," says Orsanic. "This flexibility doesn't restrict organizations to adhere to what we think is best but allows for them to utilize our products to optimize their network and security posture as they expand their remote workforces."

Maintaining visibility to ensure security

With access and expansion done, Orsanic points to Palo Alto Networks Cortex XSOAR product as a way to set up a virtual security operation centre, giving a company complete visibility into all key security metrics. "It empowers your team to virtually collaborate on

investigations in real-time and to automate and standardize any security processes to save time and reduce human error," he says.

Along with scouring for outside threats, it can also let IT personnel know if those within the organization are following best practices. Orsanic cites a hypothetical example of users who might disconnect from VPNs to improve bandwidth as one form of outright avoidance.

"If user activity is low and there's limited visibility on the activities, then chances are the user is finding ways around the processes that have been put in place," he says. "Endpoint management and security tools also shed light on user activities, while data loss prevention (DLP) services can inform and manage user behaviour around critical data." ■

“Visibility and control become factors with remote workforces, so having endpoint protection, cloud management for both public clouds and applications, and the right policies in place to protect data and users is important.”

Cybersecurity Tips in the Face of a Pandemic

As many companies adopt work-from-home policies in response to the COVID-19 pandemic, cybersecurity is a growing issue.

In this critical time, business leaders have a heightened responsibility to set clear expectations about how their organizations are managing security risk in the new work environments, leveraging new policies and technologies and empowering their employees.

Additionally, individual employees have critical roles in securing their organization and in ensuring that cyberattacks don't further compound the already-disrupted work environment.

Here are Palo Alto Networks' recommendations for business leaders and individuals.

How Businesses Can Respond

- Understand the threats to your organization
- Provide clear guidance and encourage communication
- Provide the right security capabilities

How Individuals Can Respond

- Users must be empowered to follow the guidance provided to them by organizations and take preventative measures
- Maintain good password hygiene
- Update systems and software
- Secure your WiFi access point
- Use a VPN
- Be wary of COVID-19 scams
- Don't mix personal and work



Ivan Orsanic
Regional Vice President & Country Manager (Canada), Palo Alto Networks

This article was **sponsored by Palo Alto Networks.**



HOW TO SECURE YOUR MOBILE WORKFORCE

There's a shift happening in mobile workforce remote access. Before, mobile users would connect to the internal data centre using a remote access VPN, which acted as a gateway. This allowed users located beyond the perimeter firewall to access resources within the data centre. Now that applications have shifted to the cloud, remote access VPN no longer makes sense for network optimization.



Traditional Approach to Remote Access VPN Has Challenges

- Usability:** Connectivity can be confusing and challenging.
- Performance:** Distance degrades performance and mobile users can potentially be very far from their organization's headquarters. When the application is in the cloud, this distance increases even more.
- Security:** You can't be sure how mobile workforces are connected — and protected — at any given time.



A Better Solution: It's All in the Cloud

- Core Capabilities:**
 - Accommodates global scope and scale
 - Provides access to all applications
 - Connects users from any device
 - Provides consistent security
 - Improves user experience



PHOTO COURTESY OF THE CANADIAN CENTRE FOR CYBER SECURITY

Staying Cyber-Healthy During the COVID-19 Pandemic

Scott Jones



Scott Jones
Head,
Canadian Centre
for Cyber Security

This is a challenging time for Canadians and Canadian businesses. For many people, the phrase “work from home” has become synonymous with the COVID-19 pandemic. Unfortunately, new COVID-19 work arrangements combined with online threats related to the crisis are increasing the need to practise good cybersecurity.

When you work in an office setting, you benefit from the security measures that your organization has in place to protect its networks, systems, devices, and information from cyber threats. Working remotely generally provides employees with flexibility and convenience. However, remote work can raise risks if employees are using personal laptops, tablets, and phones that aren’t subject to the same good security measures.

The good news is that even basic cyber hygiene can be effective in mitigating some of today’s nastiest cyber threats. Canadians should feel secure working from home,

without compromising information technology security. As we continue working in an unpredictable environment, there are important tips we must follow.

A few key actions can make a big difference:

- Practise good password etiquette
- Accept updates to your mobile devices, computers, and applications
- Secure your social media and email accounts
- Be on guard for phishing (and spear-phishing) messages
- Store your data securely and know your back-up procedures

The Canadian Centre for Cyber Security is Canada’s authority on cybersecurity. It publishes advice and guidance, including about the importance of security awareness training for employees, and how to create robust incident response plans for organizations.

“

Basic cyber hygiene can be effective in mitigating some of today’s nastiest cyber threats. Canadians should feel secure working from home, without compromising information technology security.

Before you determine if you would like to set up a virtual private network (VPN), host video teleconferences, or allow your employees to work remotely, you should understand the threats and set yourself up for success. Visit cyber.gc.ca for a list of alerts and advisories, including those regarding critical vulnerability patches.

The Canadian Centre for Cyber Security is here to help protect you and your organization from cyber threats. Canadians need to be on top of their cybersecurity. ■

This article was **sponsored by the Canadian Centre for Cyber Security.**



Construction Firm Hands Out Tech and Culture to Employees

The construction industry is sometimes viewed as archaic, but the COVID-19 pandemic may have spurred lasting cultural change.

Ted Kritsonis



The COVID-19 pandemic has had a profound effect on construction projects in Canada, casting a spotlight on the culture that helps keep workers employed.

In responding to the crisis, provinces were mixed on whether or not to deem construction sites as essential. Statistics Canada found the total value of building permits issued by Canadian municipalities fell by 13.2 percent in March, driven largely by British Columbia, Ontario, and Quebec. With unemployment rates also reaching highs unseen for decades, firms were forced to act.

Montreal-based company Pomerleau chose to keep its staff on the job during the pandemic by first sending employees to work from home.

“We had a plan to start with 40 people working from home on a trial basis only two months before we sent 1,500 people home for their safety,” says Pierre Pomerleau, the company’s President and CEO. “It accelerated everything, from our business plan to the change in the mindset of the client. The new way to build with the technology available is to have more collaboration and cooperation that involves the stakeholders talking together.”

Giving back

Pomerleau and his brother Francis, who runs the firm’s talent, culture, and leadership policies, have redoubled efforts to assuage workers’ fears and improve efficiency at building sites. That included a philanthropic approach through the company’s Love is an essential service initiative by donating \$600,000 to organizations serving communities affected by the pandemic.

Above all, the brothers sought to deliver on the culture they believe makes the construction firm what it is — and can become.

Despite being a large company with 30,000 total workers on sites nationwide, they describe their namesake firm as “like a family business” and strove to affirm employees “were important and necessary for the continuation of our business.”

“Their resilience, effort, and adaptability have us looking at the future in a very favourable way, especially when it wasn’t that clear at the beginning, but we now see that construction will rebound,” says Francis. “It’s not just a bulldozer that will change the world, it’s people with great ideas that make the difference on a project at all levels, so the more respect and training you have, the more your investment in them pays off.

Building consensus

Technology is also building consistency for off-site construction, they add. Along with maintaining work-from-home options in a post-COVID-19 scenario, there’s what they call “industrialization.” The information modelling and surveying technologies, among others done off-site, contribute to faster and less wasteful building practices on job sites, they say. As an example, Pomerleau is constructing eight specialty health clinics ranging between \$10 to \$30 million apiece in four months.

“The only way to achieve that is with a great team of architects, engineers, and clients, and us making sure we have prefabricated or off-site communication builders,” says Pierre. “Everything will be collaborative in the future, and it wasn’t the industry pushing back before, it was the clients. Now, they’re getting on board. We need to bring the whole industry to where everything will be mobilized and digitized within the next 5 to 10 years.” ■



Pierre Pomerleau
President & CEO,
Pomerleau



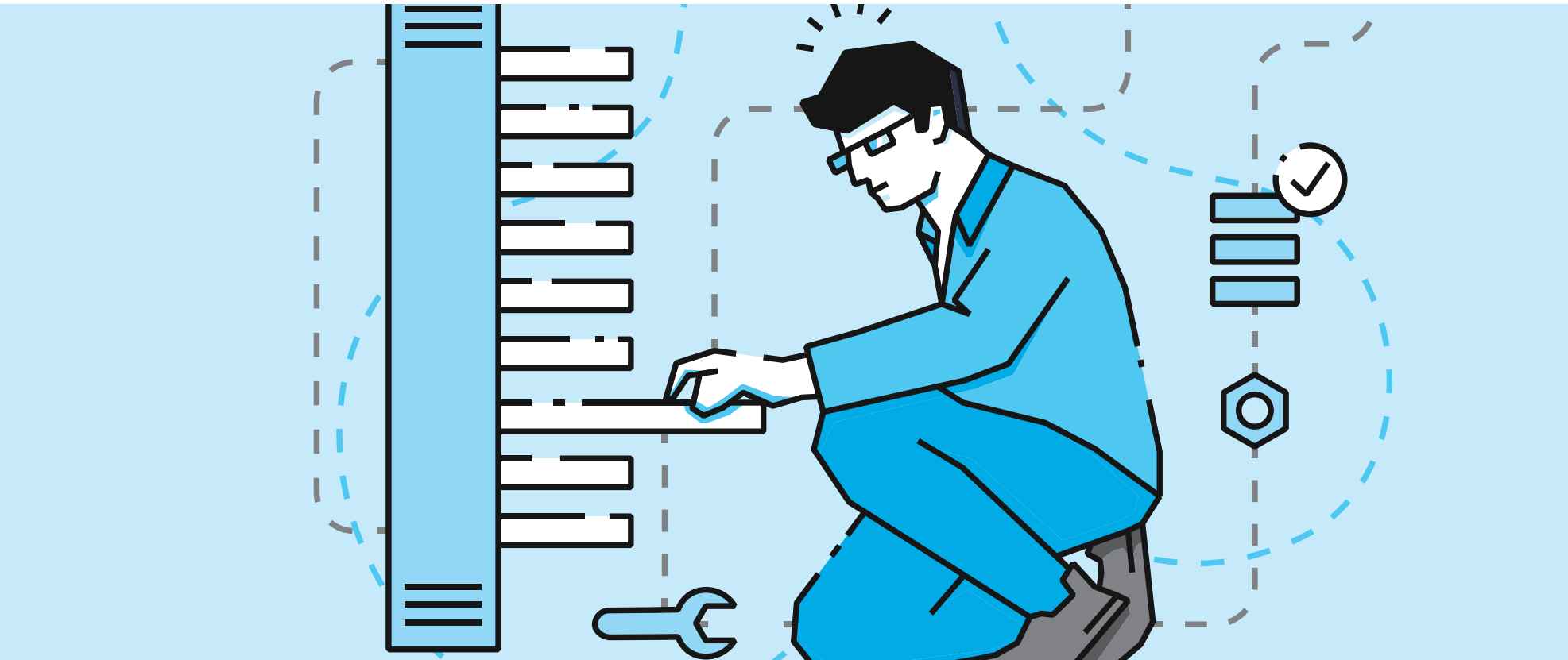
Francis Pomerleau
Chief Executive,
Talent, Culture &
Leadership,
Pomerleau

i

To discover more on how your talent can shape Pomerleau’s story and how you can push your limits in an environment fuelled by adaptability, innovation, and love, visit talent-pomerleau.ca/welcome.



Headshot photos copyright of Andr anne Gauthier



Cyber Resilience — Changing the Face of the Business Continuity Profession

Joe Ozorio



Joe Ozorio
President,
Disaster Recovery
Information
Exchange (DRIE)
Toronto

There are two types of organizations when it comes to cyber breaches: those that have been hacked, and those that don't know yet they've been hacked." Of all the cute quotes by cybersecurity evangelists, I like this one best, because to me it reflects the all-pervasive nature of cyber breaches today. I truly doubt that there's any commercial, private, or public organization where a hacking attempt hasn't been made, whether successful or not. Today's cyber criminals have too many resources, technologies, motives, incentives, and insidious purposes for us to be able to avoid.

At the Disaster Recovery Information Exchange (DRIE), we've seen the rapid evolution of cyber attacks that now impact every facet of our profession. The Business Continuity Institute's (BCI) 2019 *Horizon Scan Report*, drawing input from 569 global professionals, shows that "cyber attack and data breach" is considered to be the primary global threat over the next year. And justifiably so, as you've likely read in this special issue. It's for this reason that cyber resiliency has been a recurring theme at DRIE Toronto's regular symposiums in recent years. We believe business continuity management (BCM) and organizations resiliency profession-

als must be vigilant in understanding the threat and incorporating appropriate planning and response to meet the ever-changing nature of cyber attacks.

At our Sept. 12, 2019 symposium, the theme "Testing and Exercises — Why You Should Be Including Cyber in Your Exercises" brought to the forefront compelling issues centered around cyber resiliency. Two of our presenters came from the cybersecurity departments of two of Canada's major banks. You might imagine they have a tall order in protecting the bank's assets from the claws of cyber criminals around the world! They spoke about the current cyber threat landscape including cyber fraud, supply chain attacks, phishing, and insider threats; and risks to businesses ranging from loss of customer, client, or employee information to electronic channel fraud. They demonstrated how the advantage is clearly and deeply on the side of the cyber attacker. These attackers consider what they do simply as a business. They have patience, great skill, and no rules of engagement. Their funding is unlimited because they steal what they need.

Above all, both banks agreed that cyber attacks are not solely an IT problem. To think

so is extremely short-sighted and places the organization at huge risk. Cybersecurity is a business problem, and everyone needs to be a cyber risk manager.

From a BCM professional's perspective, regular business continuity exercises must incorporate cyber attacks in their scenarios, or craft entire scenarios around cyber attacks. To not do this is to ignore what is now considered to be the foremost global threat.

If you're a BCM or resiliency professional, whether at the practitioner or management level, you're in a unique and pivotal position to bring together many different parts of your organization together to plan, prepare, and practice responses to what's now inevitable.

Cyber attacks have changed the very fabric of organizational resiliency. So too, we as BCM professionals must change with it, or be left in the cyber dust. ■

The Disaster Recovery Information Exchange is a non-profit, member-funded association of BCM and resiliency professionals dedicated to the exchange of information on all aspects of BCM, from emergency response to the resumption of business as normal. DRIE has chapters and affiliates across Canada and in the Caribbean.

Please visit [drie.org](#) for more information.

Invest in Your Reputation: Disinfection in the Post-Pandemic World

Nicole Kenny



Nicole Kenny
Vice President,
Virox
Technologies

The COVID-19 pandemic caught many of us off guard. There's been panic, uncertainty, and fear. The pandemic has meant a crash course on the subjects of germs, their transmission, and how to deal with an outbreak. As we begin the slow journey of opening up once more, businesses need to focus on doing their part to protect their staff and clients. As a society, we have a heightened sense of social vigilance with our newfound knowledge of zoonotic diseases, hand hygiene, physical distancing, and keeping our environment safe via disinfection.

Must be wet to disinfect

Many of today's disinfectants evaporate before they have a chance to completely kill pathogens. It's essential that businesses and the general public understand that disinfectants must reach the wet dwell time (the length of time the surface needs to stay wet) as listed on the product label in order to achieve disinfection. If the label indicates a contact time of 10 minutes, the surface needs to stay wet for 10 minutes. For this reason, the best disinfectant products must be capable of staying wet throughout the length of the contact time listed on the label.

Avoid poison control

Many of today's disinfectant chemicals are a threat to human and animal health. Accidental poisonings associated with disinfectants have more than doubled due to the COVID-19 pandemic. The safety profile and the potential health risks of a disinfectant must be assessed. Some disinfectants can cause permanent eye, skin, and mucous membrane damage, some are potentially carcinogenic, and some have been shown to induce asthma.

Business owners are required to provide a safe work environment. When providing disinfectants for staff to use, training and access to personal protective equipment also need to be considered.

Whether at work or at home, focus on the areas that are most frequently touched: this might include doorknobs, faucets, light switches, TV remotes, cell phones, and keyboards. These surfaces are often highly contaminated with pathogens and we may not think to wash our hands after touching them.

Good, but not good enough

In the post-pandemic era, people are going to question the things they had previously taken for granted. Companies that communicate what they're doing to make a positive impact on the world will attract people, providing a sense of community that staff and clients can be proud to stand behind. The pandemic provides a unique opportunity for businesses to show how responsible they are.


In cases of emerging viral pathogens like SARS-CoV-2 (the virus causing COVID-19), Health Canada uses the broad-spectrum virucide concept to determine whether a disinfectant is expected to kill it.

Strategic businesses plan for the future. Choosing to use a hospital-grade disinfectant that kills more than 99.9 percent of bacteria and carries a broad-spectrum virucidal claim shows you're thinking about future outbreaks and investing in the long-term health of its staff and clients.

The war against pathogens

As disinfection is one of the key tenets for breaking the chain of infection, at Virox® Technologies our focus is on educating and developing disinfectant technologies to combat the shortcomings of legacy disinfectants currently used around the globe.

Accelerated Hydrogen Peroxide® (AHP®) provides the perfect balance between safety and efficacy. The patented technology uses the power of oxidation to clean and disinfect surfaces as it dries slowly to ensure disinfection has occurred. From SARS and norovirus to pandemic influenza and now COVID-19, AHP® has been on the front lines, fighting outbreaks and helping to save lives. ■




Dwell Time Disease

Many disinfectants evaporate before achieving disinfection. Using disinfectants that stay wet for required contact time will increase product effectiveness.



Label Deficit Disorder

Some disinfectants have labels that are ambiguous. Due diligence is required to effectively select disinfectants to meet regulatory compliance.



Safety Indifference Syndrome

Some disinfectants may pose a health risk to users, patients, clients, and the environment. Using a disinfectant with a preferred safety profile will increase user safety.