Preparing for the Unexpected: Business Continuity and Information Security Trends and Tactics

AUGUST 2018

By Kevin Kondo
Assistant Vice President,
Enterprise Security

Kevin Kondo is Assistant Vice President of Enterprise Security at CIBC Mellon. Kevin is responsible for overseeing the disaster recovery and business continuity program in addition to managing CIBC Mellon's information security programs. Kevin has more than 15 years of experience in the Canadian financial services industry.

Technology-related incidents impacting business operations are widely publicized in the media and are affecting businesses across Canada, and the globe, at a greater frequency in today's highly-connected, digital world. Institutional investors, regulators and stakeholders across financial services and other industry segments are seeking assurance from their suppliers and partners that they have the processes in place to mitigate the effects of unexpected incidents, disruptions and threats on critical services.

As a trusted safeguard of more than $2 trillion of assets held on behalf of banks, pension plans, mutual funds, corporations and other institutional investors, we recognize the importance of our resilience to our clients. That's why we continuously work to further reinforce our strong governance and control environment. We know we need to react to unplanned challenges in a prompt, organized and effective manner to continue to provide our services and solutions to our clients.

TRENDS IN BUSINESS CONTINUITY AND INFORMATION SECURITY

The Business Continuity Institute (BCI) is a leading international membership and certifying organization for business continuity professionals worldwide. The Business Continuity Institute produces an annual Horizon Scan Report designed to track risks and threats to organizations through assessing perceived threats as shown by practitioners' in-house analysis. In the most recent Horizon Scan, the Business Continuity Institute tracked the following top trends according to 657 responding organizations in 76 countries:

TOP 10 BUSINESS CONTINUITY THREATS: 2018 BCI INSTITUTE HORIZON SCAN

1. Cyber attack
2. Data breach
3. Unplanned IT and telecom outages
4. Interruption to utility supply
5. Adverse weather
6. Act of terrorism
7. Security incident
8. Fire
9. Supply chain disruption
10. Transport network disruption

Technology matters continue to lead with respondents. Recent events, such as, the Meltdown and Spectre vulnerabilities made public in January 2018, and the 'WannaCry' ransomware attack that occurred in May 2017, have placed cyber resilience and information security efforts at the forefront of organizations' minds across the globe.

CIBC MELLON

While we understand that the cyber attack and data breach threats are top-of-mind for organizations, those that organizations will tend to see on a more frequent basis are unplanned IT and telecom outages and interruptions to utility supply. In fact, unplanned IT and telecom outages are likely experienced by your organization in some capacity on a weekly basis.

Top Five Trends and Uncertainties, and CIBC Mellon's Responses

The following five trends and uncertainties were cited by more than half of respondents to the BCI survey, and will likely find broad resonance among institutional investors.

1. USE OF INTERNET FOR MALICIOUS ATTACKS

Sitting at the top of the list in 2016, 2017 and 2018 amongst BCI Horizon Scan survey respondents are cyber attacks and data breaches. As a key focus area for organizations, practitioners remain concerned about the potential for damage via cyber attacks and data breaches given the ever-increasing sophistication of hostile elements.

As organizations continue to move toward connection, digitization and technology, IT governance, security and preparation continue to be placed at the top of their considerations. From internal processes and employee education, to vendor management, businesses should look to remain vigilant and work to continuously improve the controls and security measures in place to protect themselves, their stakeholders and the information under their control.

An organization's planning, documentation and response to an issue will significantly depend on the ability of its teams to react quickly and effectively.

2. LOSS OF KEY EMPLOYEES

The "human factor", such as a skills shortage or loss of key employees, can impact business performance and requires a strategic response. Every business depends on key players to deliver strong results, deeming this a key focus area for business continuity management as a field.

From a business continuity perspective, we recognize the critical role that employees play. Every business unit at CIBC Mellon has a designated Business Recovery Planning Coordinator and Alternate who collaborate with the company's Business Continuity team to assess and document their individual continuity needs and plans. The plans cover a wide array of factors, for example, identifying business functions as time-sensitive and critical or more general activities that can take a lower priority during a business continuity issue. From working remotely to shifting to alternate offsite recovery locations to the specific technical and connectivity requirements of each employee's role and tasks, each team documents its needs, which in turn positions us to plan for, maintain and deploy critical capabilities during an incident.

3. INFLUENCE OF SOCIAL MEDIA

The growing influence of social media, especially in relation to company reputation, placed third in this year's report with 50 per cent of respondents noting this as a top threat. Beyond the concerns related to corporate and brand reputation, there are additional risks related to legal/regulatory compliance, security and privacy, and Human Resources-related issues.

Social media is not only a challenge, but also an opportunity, as monitoring can help an organization remain alert to potential threats and challenges and can provide a communication channel when an event occurs. CIBC Mellon also uses social media to raise the profile of its great workplace experience, helping us recruit talented professionals and maintain a strong pipeline of talent to address natural turnover experienced at every organization.

4. NEW REGULATIONS AND INCREASED REGULATORY SCRUTINY

Today's financial services market participants direct substantial attention to compliance with requirements from various industry and regulatory bodies in Canada. From the Canadian Securities Administrators (CSA)'s guidance on capital markets to the Financial Services Commission of Ontario (FSCO)'s records retention requirements, organizations face increased regulatory expectations to provide customers with confidence regarding business continuity risks and their ability to manage them well. CIBC Mellon provides its clients with detailed reporting on controls, practices and governance efforts, and makes available an overview of the steps CIBC Mellon takes with regard to business continuity efforts.

5. PREVALENCE AND HIGH ADOPTION OF INTERNET-DEPENDENT SERVICES

When responding to risks related to internet-enabled services, an integral step is to appropriately review service providers. While this is an important component of vendor selection and onboarding, it is imperative throughout the duration of the relationship as well. Vendors can provide assurance in many ways: multiple redundant data centres, detailed disaster recovery or service and high standards for information security.

CIBC Mellon leverages powerful and robust infrastructure from CIBC and BNY Mellon, together with extensive vendor management processes to support confidence around vendor services. We work to carefully assess vendors to confirm their alignment to our standards, and we leverage the expertise and scale of our two parent companies to help us monitor the IT environment. We provide all employees with detailed annual training related to information security, and work to monitor for emerging threats on an ongoing basis.

Business continuity management involves planning and preparation to support the continued operation of your business in the case of serious incidents and disasters, and the recovery to an operational state within a reasonably short period.

Considerations for robust and resilient business continuity management

CONSIDER SCENARIOS

Business continuity events span a variety of scenarios. Demonstrated by the BCI's research, as businesses, we are focused on the technological events in today's connected world. It is important, however, to consider a wide array of events to prepare you to react in a range of situations. We have outlined the top three buckets and sample scenarios for your consideration.

TECHNOLOGICAL

A technological scenario could include items such as:

- Critical system or network failures
- Communication network failures
- Loss of external service providers and suppliers (outsourcing) such as information providers
- Technical infrastructure failures such as software or hardware failure, database loss, or online banking failures
- Power outages due to inclement weather

Scenario example: Canada's harsh winter storms are known to cause power outages, supply disruptions, and safety hazards that may endanger lives and hinder access to key infrastructure. Planning for these naturally-occurring events can be achieved in advance so that readiness is in place. Such planning should include, but is not limited to the following:

- Conduct awareness training, including facility evacuation routes and procedures
- Coordinate activities with local and state response agencies
- Communicate recommended evacuation routes
- Procure emergency supplies
- Monitor radio and/or television reports
- Secure facility
- Secure and backup critical electronic files

FINANCIAL

Although business continuity events can have financial implications, a specific scenarios for which you could look to prepare your response include:

- Earnings shortfall
- Reinstatement of earnings
- Declining stock prices
- Loss of clientele
- Market turbulence
- Sociopolitical disruptions

Sample scenario: Starting in 2017 and continuing through to 2018, the NAFTA and other international trade agreement negotiations are resulting in rising tensions. The Dow and Nasdaq have seen the effects of the ongoing changes and imposition of tariffs between the U.S. and the EU, Canada, Mexico, China, and more. In fact, in a CNN Money article[1], it was reported that the Dow shed 400 points and the Nasdaq dropped two per cent with the news that President Trump planned to crack down on Chinese investment in major technologies within the U.S. While much is still uncertain here, this is a scenario that requires diligent preparation and thought to enable your business to react effectively.

REPUTATIONAL

Reputational is reportedly frequently ignored by organizations, but can often result in lost revenue, increased operating or regulatory costs, decreased shareholder value, or even a potential criminal event even when the company is not found guilty. Reputation is also at risk in the event that a scenario from either of the above categories is not managed effectively. Some examples of reputational business continuity events, include:

- Illegal Activity
  - Extortion
  - Bribery
  - Fraud
  - Criminal investigation
- Employee Misconduct

Reputational damage can be minimized through an organization's response to disruption. According to the Business Continuity Institute[2], honesty is the best first step. Honesty with stakeholders builds trust, and confidence that your organization has the ability to resume operations and return to normal following an event.

An organization's planning, documentation and response to an issue will significantly depend on the ability of its teams to react quickly and effectively.

CHAMPION EFFORTS AND MEASURE

In order for the business to prepare adequately for any incident, it is important to have a leader championing the significance of business continuity events to business operations, the employee and client experience, and potentially the bottom line. Ongoing monitoring of incidents, minor and major, helps demonstrate the frequency of these incidents and the benefits of being prepared.

THIRD-PARTY VERIFICATION

Further to considering scenarios, third-party leaders in business continuity can help your business uncover opportunities, further enhance your plans and certify your preparedness to leadership, clients or prospects and other key industry stakeholders. An example of this is the British Standards Institution (BSI)'s ISO 22301 certification. Globally recognized, BSI helps more than 80,000 clients in 182 countries understand, assess and develop new standards to perform better in a variety of situations. They offer a variety of certifications ranging from energy management requirements to occupational health and safety. The two of relevance to your business continuity and information security efforts are ISO 22301 and ISO 27001 respectively.

CIBC Mellon is ISO 22301 and ISO 27001 certified. The below chart from the BCI Horizon Scan demonstrates that an increasing number of organizations are gaining ISO 22301 certification.

Year	ISO 22301 uptake
2016	51%
2017	63%
2018	70%

INCLUDE PARTNERS, SUPPLIERS AND THIRD PARTIES

As you look to develop business continuity plans and efforts surrounding information security, it is important to consider your partners, suppliers and any third parties that are part of your wider business. These are often extensions of your operations and in an event, it is equally important that they have the ability to respond and return to business as usual as soon as possible. Read the vendor management section that follows, which includes some key questions to consider when evaluating vendor readiness.

INTERNAL MANAGEMENT

Your employees are your first line of defence. Not only can they help identify potential serious situations through their daily activities, but they are also one of your highest-risk groups for penetrating your organization. Ongoing education, involving in-depth training and regular knowledge sharing is key to keeping your employees armed with the information required to protect the integrity of your daily operations. We covered key considerations from a business continuity perspective in the Trends and Uncertainties section above.

CYBER SECURITY AND DATA MANAGEMENT

CIBC Mellon is well positioned with the support of two leading global financial services organizations – CIBC and BNY Mellon – both of which place a high premium on cyber security. CIBC Mellon, CIBC, and BNY Mellon monitor the IT environment for potential threats and concerns, and work to further strengthen security and governance measures.

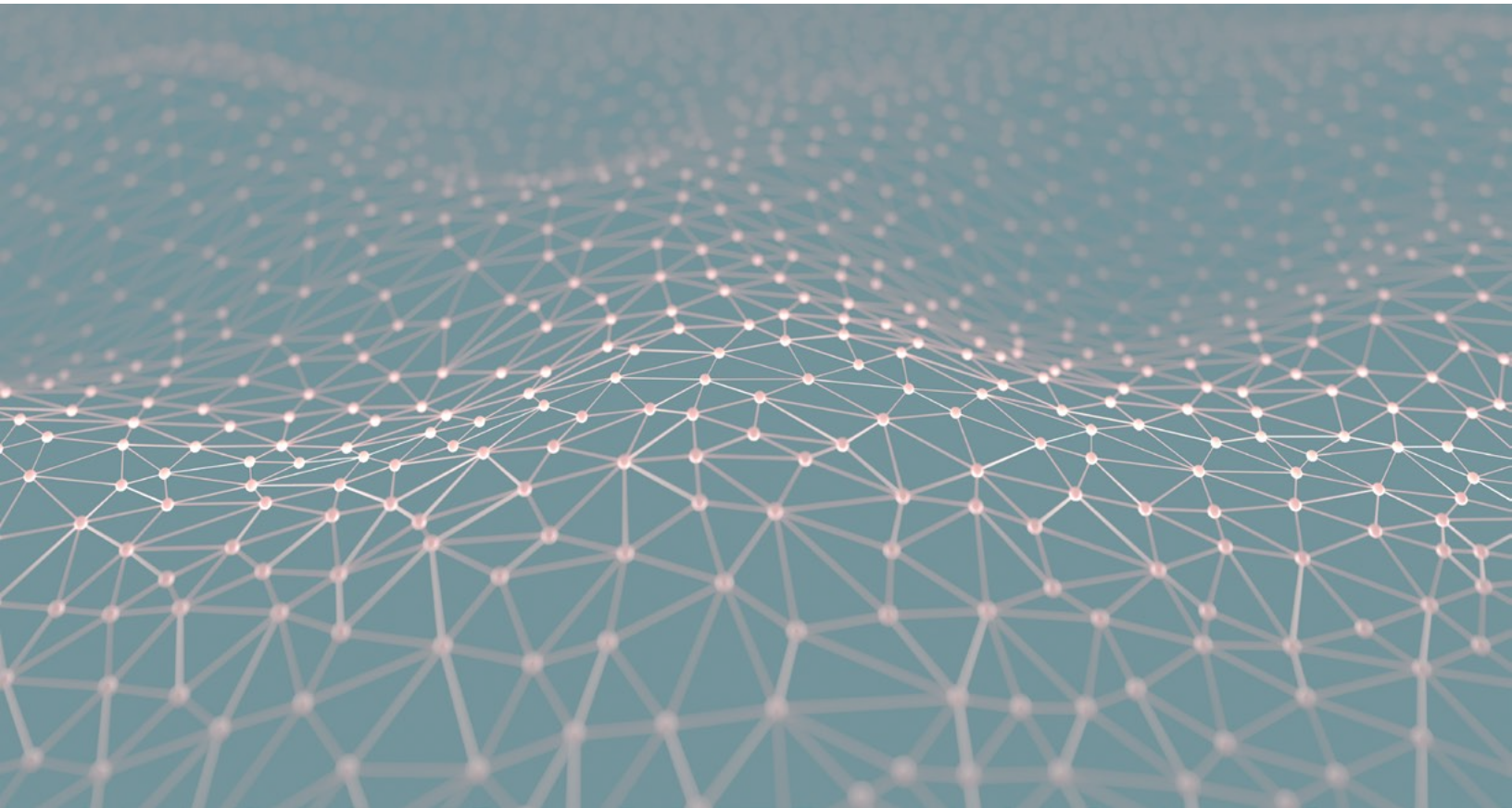
CIBC Mellon and its parent companies have multiple levels of IT-related threat protection, and have implemented – and seek to continuously improve – a wide array of security measures designed to protect our company, clients, employees and the information under our control. We regularly receive security information on potential threats from our peers and the broader financial services industry, as well as from our clients, law enforcement and a variety of public and private sources. CIBC Mellon and its parent companies monitor and assess our IT environments for potential vulnerabilities and threats, and we continue to invest in and implement protections as deemed necessary.

At CIBC Mellon, we also work at the individual employee level. We work regularly with employees to raise awareness of the specific steps that they can take to help protect the company, its clients and the information under its control; from reporting phishing attempts to reinforcing controls around information handling, we know that employees' diligence and awareness of good practices are critical elements in our efforts to maintain strong controls.

VENDOR GOVERNANCE

CIBC Mellon has an established vendor governance program through which we exercise oversight of our third-party vendors. Through this program, we document and hold vendors accountable to standards for performance with regular due diligence reviews and appropriate reporting requirements. For vendors whose services are deemed critical to CIBC Mellon, including technology-related vendors, we implement additional controls and monitoring to provide further assurance that risks related to our vendors and supply chain are being managed in accordance with CIBC Mellon's requirements. This is all part of our goal to carry on our business with governance and operational excellence.

CIBC Mellon and its parent companies have multiple levels of IT-related threat protection, and have implemented – and seek to continuously improve – a wide array of security measures designed to protect our company, clients, employees and the information under our control.



QUESTIONS TO CONSIDER

Business Continuity Questions to Consider

- Does your organization have an active and ongoing business continuity process?
- What critical business or service commitments has your organization made to its clients and stakeholders?
- How does your organization document its business continuity plans and needs?
- How does your organization plan to communicate to its employees, clients and other stakeholders during an emergency or crisis?
- How quickly can you reach employees outside regular business hours?
- What are your organization's critical dependencies, technologies and systems?
- Who are your essential employees?
- Who are your critical vendors, and how have you worked to satisfy yourself and your own stakeholders that those vendors are prepared for a disruption?
- What regulatory, Board or stakeholder reporting requirements call for your organization to address business continuity preparations?

Vendor Questions to Consider

- Do you have an active and ongoing business continuity process?
  - If so, what is it?
- What measures do you have in place to protect my data?
- Do you encrypt your data?
- How do you secure the transmission of data?
- How and when will I be notified as a client of any incidents?
- Who are the essential employees on my account and what is their contact information?
- Who are your critical vendors, and how have you worked to satisfy yourself and your own stakeholders that those vendors are prepared?
- What certifications, regulations, and/or measures do you use to measure your incident preparedness?
- How do you keep employees informed and prepared of updated business continuity processes, cyber security procedures, and similar matters? What policies do you have in place?

CIBC Mellon's business continuity and information security efforts are designed to provide our clients with confidence and assurance that risks related to the continuity of our business and the data under our control are appropriately assessed, monitored, managed and mitigated.

For More Information

We are committed to working in collaboration with clients to take steps to protect the information under CIBC Mellon's control. If you require additional information from CIBC Mellon, including comment from our company related to a specific IT security matter (e.g., virus, malware that has been identified in the media), an update on your technology measures and needs which may impact CIBC Mellon, or a more general discussion about the cyber security measures CIBC Mellon, CIBC and BNY Mellon have in place, please contact your service director or relationship manager.

Notes:

1 http://money.cnn.com/2018/06/25/investing/dow-jones-stock-market-trade-war/index.html

2 https://www.thebci.org/news/what-are-the-effects-of-reputational-damage.html

About CIBC Mellon

CIBC Mellon is a Canadian company exclusively focused on the investment servicing needs of Canadian institutional investors and international institutional investors into Canada. Founded in 1996, CIBC Mellon is 50-50 jointly owned by The Bank of New York Mellon (BNY Mellon) and Canadian Imperial Bank of Commerce (CIBC). CIBC Mellon's investment servicing solutions for institutions and corporations are provided in close collaboration with our parent companies, and include custody, multicurrency accounting, fund administration, recordkeeping, exchange-traded fund services, pension services, securities lending services, foreign exchange processing and settlement, and treasury services. As at June 30, 2018, CIBC Mellon had more than C$2 trillion of assets under administration on behalf of banks, pension funds, investment funds, corporations, governments, insurance companies, foreign insurance trusts, foundations and global financial institutions whose clients invest in Canada. CIBC Mellon is part of the BNY Mellon network, which as at June 30, 2018 had US$33.6 trillion in assets under custody and/or administration.

For more information visit www.cibcmellon.com.

CIBC MELLON

A BNY MELLON AND CIBC JOINT VENTURE COMPANY℠

000 - KL29 - 07 - 18