CIBC MELLON | BNY MELLON | CIBC

Preparing for the Unexpected: Business Continuity and Information Security Considerations

AUGUST 2021

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.

"Unprecedented" may have been one of the most-used words in 2020 as the COVID-19 pandemic impacted people, businesses and markets around the world. The rapid shift to remote working saw financial services market participants work to protect the health and safety of their teams, as well as respecting the evolving requirements of governments and health authorities. Amid this environment, business continuity and business resiliency took on even further importance and focus. Likewise, a new set of challenges faced organizations as they looked to secure the information under their control among a workforce suddenly dispersed into their home environments for an extended period of time.

CIBC Mellon has long invested in business continuity and resiliency, and our team is proud of its performance amid COVID-19. We worked to support clients, engage with market stakeholders and above all else, protect our teams. We were pleased to be named #1 in the world by Global Finance for treasury operations amid the COVID-19 pandemic. We remain nonetheless firmly committed to continuous improvement.

TECHNOLOGY AND RESILIENCY

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. CIBC Mellon has and will continue to take actions to sustain the high-quality service, stability and flexibility clients have come to expect of us. As a trusted safeguard of more than $2.4 trillion of assets held on behalf of banks, pension plans, investment 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.

PRACTICING A HIGH DEGREE OF DILIGENCE THROUGHOUT COVID-19

A significant contributor to CIBC Mellon's ability to serve its clients successfully is the robust control and risk governance we have in place. As we face this unprecedented environment, our commitment to practicing proper governance and adhering to our controls have not changed.

THIRD PARTY STANDARDS: ISO CERTIFICATION

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's ISO certification. Globally recognized, they help over 128,000 clients in 193 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.

Two standards that may be relevant to your business continuity and information security efforts are:

ISO 22301 | ISO 27001

ISO 22301: SECURITY AND RESILIENCE — BUSINESS CONTINUITY MANAGEMENT SYSTEMS

CIBC Mellon is ISO 22301 certified. This standard specifies requirements to implement, maintain and improve a management system to protect against, reduce the likelihood of, prepare for, respond to and recover from disruptions when they arise. ISO 22301 is not only a planning tool and a certification tool but it can also be used to assess an organization's ability to meet its own business continuity needs and obligations.

The below chart from the BCI Horizon Scan demonstrates that an increasing number of organizations are gaining ISO 22301 certification.

PERCENTAGE OF ORGANIZATIONS CERTIFIED OR ALIGNING TO ISO 22301

Year	Percentage of organizations certified to ISO 22301	Percentage of organizations certified to ISO 22301OR using it as a framework
2016	11.6%	67.7%
2017	9.6%	65.8%
2018	13.8%	69.2%
2019	20.5%	71.0%

ISO 22301 Update: To date, nearly three-quarters of organizations are either certified to ISO 22301 or using it as a framework 5% of organizations plan to move towards certification in 2021. From an information security perspective, there are multiple ways vendors can provide assurance that data under their control is sufficiently protected and that an organization has the necessary resilience. In engaging with vendors, consider seeking assurance of such factors as multiple redundant data centres, affirming that a detailed business continuity / disaster recovery plan is in place, and setting high standards for information security. In considering vendors, firms may wish to assess whether a vendor adheres to established third-party standards such as the ISO 22301:2012 Societal security — Business continuity management systems standard. It enables organizations to prepare for disruptive incidents and recover more quickly, minimizing the impact on employees, customers and suppliers.

ISO/IEC 27001 information security management

CIBC Mellon possesses the International Organization for Standardization's (ISO) 27001:2013 Certification, issued by the British Standards Institution. ISO/IEC 27001 is an internationally recognized management system for managing information security governance risk. The standard provides a best-practice framework, ongoing governance, and robust management of the system to:

Identify and minimize risks to the information under an organization's control

Improve reputation and stakeholder confidence

Increase in information security awareness

CIBC Mellon's ISO 27001 certification affirms our Leadership Team's commitment to maintain and evolve the framework that helps to protect financial data, intellectual property and sensitive client information. The scope of the certification includes but is not limited to process and technology that support the framework and verifies effectiveness of security measures. A continuous assessment of our risk landscape helps identify and mitigate external and internal risks, and is a vital part of ISO/IEC 27001.

CIBC Mellon has long invested in business continuity and resiliency, and our team is proud of its performance amid COVID-19.

A significant contributor to CIBC Mellon's ability to serve its clients successfully is the robust control and risk governance we have in place.

Questions to Consider

1. Does your organization have an active and ongoing business continuity process?
2. What critical business or service commitments has your organization made to its clients and stakeholders?
3. How does your organization document its business continuity plans and needs?
4. How does your organization plan to communicate to its employees, clients and other stakeholders during an emergency or crisis?
5. How quickly can you reach employees outside regular business hours?
6. What are your organization's critical dependencies, technologies and systems?
7. Who are your essential employees?
8. 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?
9. What regulatory, board or stakeholder reporting requirements call for your organization to address business continuity preparations?

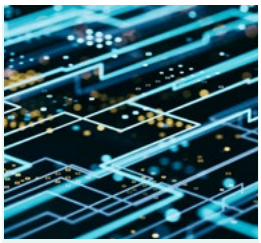
Top Ten Disruptions

Health incident

Unplanned IT and telecom outages

Safety incident (e.g. personal injury, fatality etc.)

Lack of talent/ key skills



Cyber attack & data breach

Non-occupational disease

Product safety recall

Extreme weather events (e.g. floods, storms, freeze etc.)

Interruption to utility supply

Exchange rate volatility

The disruption landscape has changed over the past year, while the lingering effects of the COVID-19 pandemic remain ever present. With Public Health authorities continuing to monitor the progression and spread of COVID-19, health incidents have replaced IT and telecom outages as the leading cause of disruption for organizations over the past twelve months.

Business continuity events span a variety of scenarios. Demonstrated by the BCI's research, as businesses, there is a focus on the technology-related events in today's digital environment. A technological scenario could include items such as: a critical system or network failure; a communication network failure; the loss of external service providers and suppliers (outsourcing) such as information providers; technical infrastructure failures such as a software or hardware failure, database loss, or online banking failure; or a power outage due to inclement weather.

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.

Cyber Security

Our approach and philosophy

At CIBC Mellon, we understand that our clients face increasing pressure from institutional investors, regulators and stakeholders to provide assurance that processes are in place to mitigate the effects of unexpected disruptions and threats on critical services such as breaches due to technology-related events. Information security is generally thought of as the risk of managing the confidentiality, integrity and availability of information assets. The goal is to prevent disclosure of data; unauthorized or accidental modification of data; or loss of information assets.

Information security breaches are usually due to technology-related incidents impacting business operations. These breaches are affecting businesses across Canada, and around 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 organizations continue to move toward connection, digitization and technology - IT governance, security and preparation have become increasingly important. From internal processes and employee education, to vendor management, businesses are expected 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.

Ensure you receive security information on potential threats from peers and the broader financial services industry, law enforcement and a variety of public and private sources. Many industries work together on cyber intelligence – a breach at one organization impacts the broader industry.

Cyber Security and Cyber Risk Mitigation

CIBC Mellon is well positioned with the support of leading global financial services organizations, CIBC and BNY Mellon – both of which place a high premium on risk culture. On an ongoing basis, 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.

Our risk and control assessments extend to our external service providers. We have established, mandatory requirements for our partners to protect clients' assets. We conduct scheduled due diligence reviews of our material outsourcing arrangements and critical technology and business service providers, including related subcontracting arrangements, to confirm that they meet our service level requirements and support our business and data protection commitments to our clients and regulators.

WHAT CYBER SECURITY QUESTIONS SHOULD CLIENTS BE ASKING THEMSELVES?

- How do you document, understand and capture the scope of data under your control?
- What measures do you have in place to protect data? What policies?
- Do you encrypt data, if so when?
- How do you secure the transmission of data?
- How do you keep employees informed and prepared of updated, cyber security procedures, and similar matters?
- How do you make sure that employees – from the newest entrant to the most senior leaders – are well prepared?
- What are your organization's critical dependencies, technologies and systems?
- What are some of the potential risk events, and how would you react if you were breached?
- For example, would you pay a ransom or under which circumstances would you consider it?
- What can and can't my employees do with the data in their care? How is that access to the data controlled?
- What safeguards do you have in place to prevent data loss events, data breaches, denial of service attacks? How do you detect and defend against against malware and spear phishing attacks?
- What confidence do you have in the fundamentals of your organization? For example, ability to monitor the evolving threat landscape, patching, vulnerability management and access management programs?

Risks that extend beyond technology risks in the event of a cyber-attack:

Transaction Processing - which could result in a risk of loss resulting from failures in processing or performance of a task if you cannot access and systems and process transactions.

Business Continuity Risk - resulting from an cyber events can obviously adversely impact the ongoing continuation of a firm's operational processes.

Legal Risk - a firm could be at risk of being negligent in protecting its data which could result in potential litigation with clients, vendors or other affiliates.

Regulatory and Compliance Risk - from potential violations of or non-conformance with laws, rules, policies, regulations, prescribed practices or ethical standards with respect to information security.

Reputational Risk - which results in the loss of business due to a diminution of your organization's public image with customers, employees, regulators, underlying stakeholders such as plan members or investors, and other stakeholders in the markets or communities where you operate. Reputational risk impacts the organization's ability to establish new relationships or services, or to continue servicing existing clients. A reputational risk issue can often result in lost revenue, increased operating or regulatory costs, decreased shareholder value. Reputation is also at risk in the event that a scenario is not managed effectively.

Reputational damage can be minimized through an organization's response to disruption. The Business Continuity Institute states that a business' best practice is to be transparent. Honesty with stakeholders builds trust, and confidence that your organization has the ability to resume operations and return to normal following an event.

Evolving threat landscape amid sustained remote operation

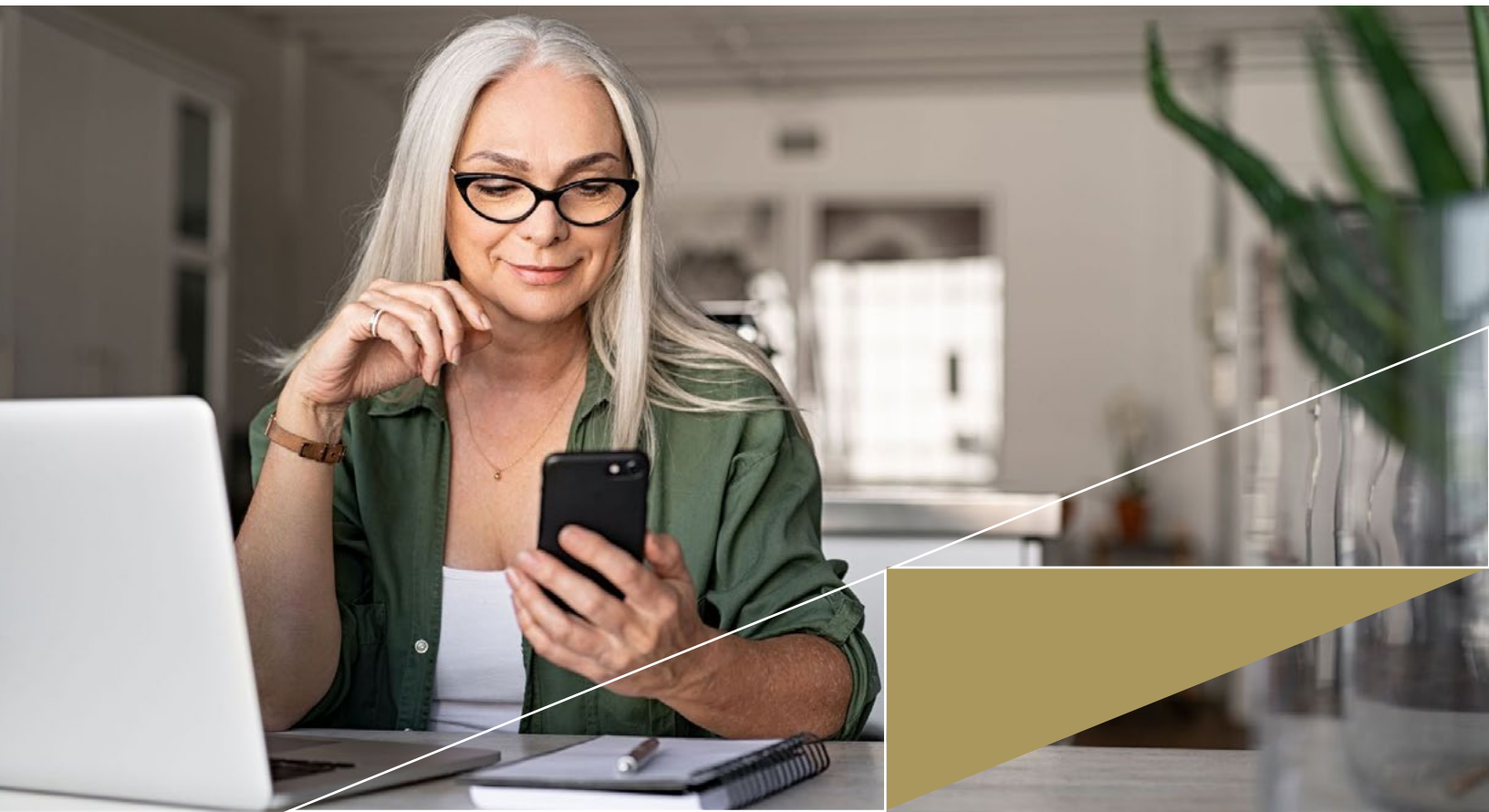
Especially amid a move where the majority of employees are working remotely, employees' diligence and awareness of good practices are critical elements in a corporations' efforts to maintain strong controls. Working from home for extended periods of time can result in changes to the threat landscape and can create new risks and opportunities.

THE FUTURE OF WORK IS AT LEAST PARTIALLY REMOTE

Even as organizations contemplate their operational stance for a post-pandemic environment, in many cases this stance includes a portion of the workforce working remotely at least some of the time. CIBC Mellon continues to progress its "Future Ways of Work" strategic efforts, which recognize that remote operation has produced sustained and, in some cases, beneficial outcomes for our clients, employees and organization. To learn more, contact your relationship manager.

A constantly evolving threat landscape requires a constantly evolving employee program. Strengthening employees to detect and respond to threats is a prevalent theme in the financial industry. Unprotected technology vulnerabilities can lead to disastrous consequences such as unpatched systems, back doors and unrevoked access. Staff need to understand the criticality of data. This can be done through making data classifications available, such as internal or confidential handling, so employees know what standard of care is required related to each set of information. Key areas to train employees on include: how to handle data, move the data, how to identify phishing emails, and how to know if a desktop has been hacked. It's not enough to teach an employee to identify if they have been hacked or to notice a bad link – your people also need to know what to do about it, and where to report the incident.

An area where the industry can continue to mature is the movement of secure information to external parties outside our organizations such as clients and vendors.



ALWAYS CONSIDER THE FOLLOWING TWO QUESTIONS:

Is my company carrying out its activities using consistent approaches to diligence – across functions and over time?

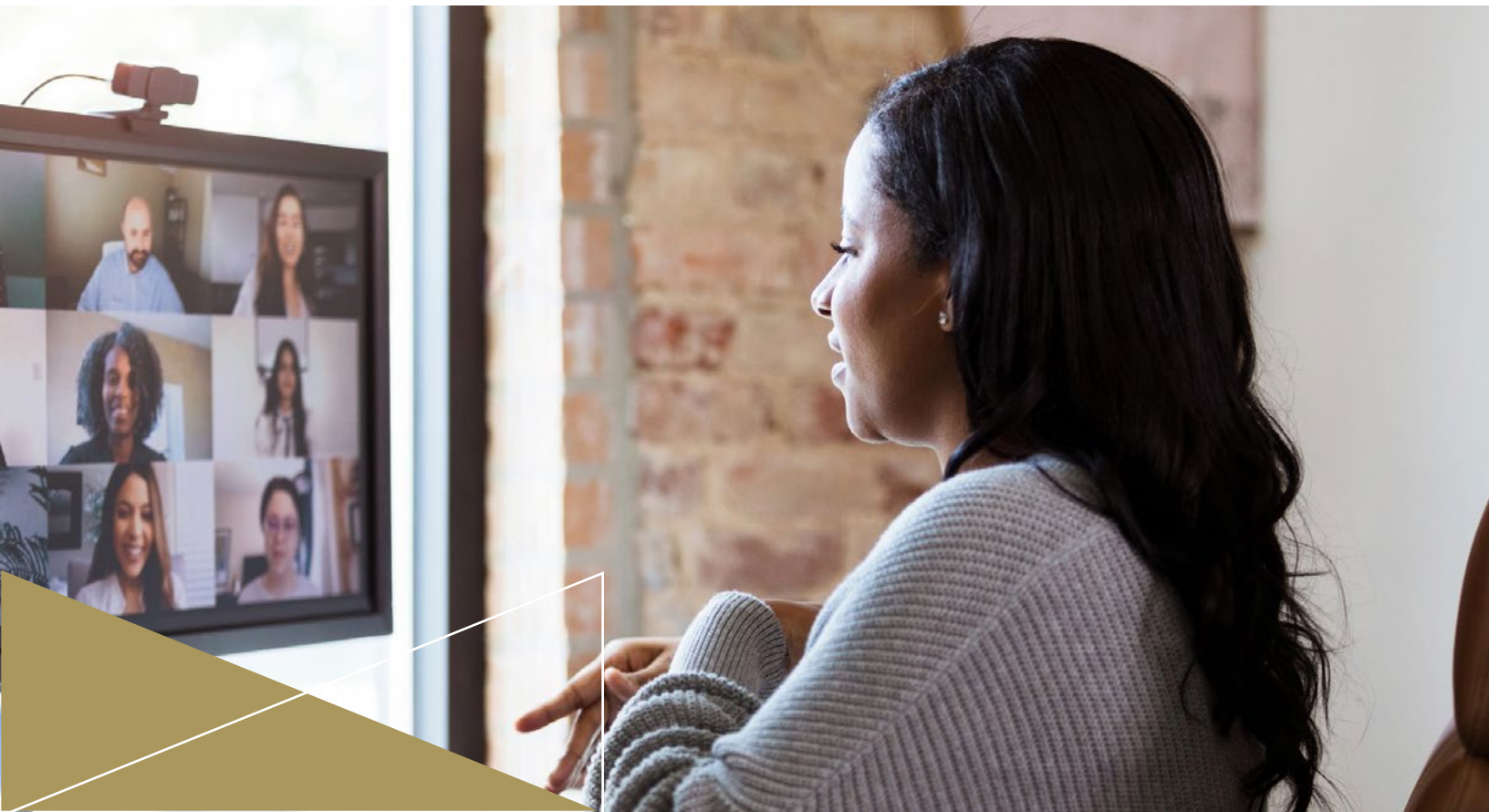
Are we sending data encrypted at all times? (eg. Emails)

There are a few simple steps that can support stronger resiliency. For example, organizations should consider using the latest Transport Layer Security (TLS) for sending data outside their IT environments to clients, counterparties and vendors. TLS consists of cryptographic protocols that provide a secure method to transmit data and information over a computer network.

Consider how you are managing your outsourced vendors: are their security programs as mature as your security programs?

From a technology perspective, CIBC Mellon has multiple layers of preventative and detective controls regardless of where employees are working from. Today's cyber program needs to extend beyond the brick walls of the corporate office and play a role in each of our employees homes and devices they are working off of.

Working across our global enterprise, engaging with vendors and working to monitor updates from the cyber intelligence community, our teams place emphasis on the fundamentals of technology security – protecting remote work infrastructure, VPN and Citrix environments, securing our end points through patching and applying and fixes, and closely monitoring for renewed vulnerabilities and threats.



Conclusion

Financial market participants globally continue to hone their focus on risk management, governance and risk assurance. The Canadian market may offer insights and tools for global participants as they seek to deliver assurance – in particular when the focus moves to protecting data managed both internally and externally by vendors.

The pandemic put a large focus on people risk, for example, absenteeism workforce planning and COVID-19 incident response. The same planning and preparation needs to be made in regards with technology. Back-up office equipment, access to your data and records, even things like residential internet service providers and cellular services, and going one step further, the resiliency and preparation of key service providers. The holistic approach to the continuity planning of people, tech and processes is essential as organizations look to maximize their resiliency through the pandemic and beyond.

Fostering a sustainable risk culture and demonstrating powerful resiliency is a staple of success in the evolving technology landscape and financial services industry.

For more information

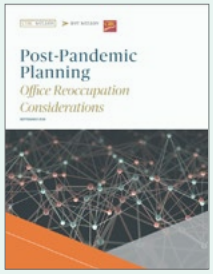
To learn more, contact your Relationship Executive, Service Director or Corporate Communications at corporate_communications@cibcmellon.com

Additional Resources

For more information on CIBC Mellon's business continuity planning and thought leadership regarding COVID-19, we are pleased to provide you with the following resources:

CIBC Mellon Statement on Preparations Regarding the 2019 Coronavirus (COVID-19)

Business Continuity Considerations: Pandemic Preparedness



Post-Pandemic Planning and Office Reoccupation Considerations

CIBC MELLON

A BNY MELLON AND CIBC JOINT VENTURE COMPANY℠

BNY MELLON

www.bnymellon.com

CIBC

www.cibc.com

000 - KL43 - 08 - 21