FINANCIAL EXECUTIVES, CYBER SECURITY & BUSINESS CONTINUITY

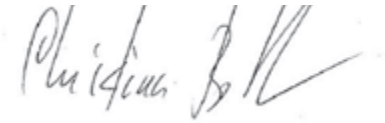
fei financial executives international canada

cferf canadian financial executives research foundation

IBM

ACKNOWLEDGEMENTS

We gratefully acknowledge the efforts of our survey respondents and our forum participants who took valuable time away from their day jobs to participate in this work. We are particularly grateful to our research partner, IBM, without whom this study would not have been possible.



Christian Bellavance
Vice President, Research and Communications
Financial Executives International Canada

First published in 2014 by CFERF.
1201-170 University Ave.
Toronto, ON
M5H 3B3

ISBN# 978-1-927568-12-5

CONTENTS

EXECUTIVE SUMMARY

Financial executives, most of whom are responsible directly or indirectly for Information Technology (IT), agree IT security and business continuity are important. Many have experienced disruptions due to common threats such as human error, natural or manmade disasters, data loss, security breaches or system failures. Financial executives are also concerned about future disruptions to their organization as a result of system failures or cyber attacks. Yet many organizations lack formal IT security and business continuity plans, or lack consistent application of these plans across the organization. Some of the key barriers to improvement include tight budgets and a lack of expert staff.

The overwhelming majority of survey respondents rated the importance of IT security as extremely important or important (93%) to their organizations.

Business continuity (defined as the uninterrupted flow of business) was rated even higher, with 95% of survey respondents rating it as extremely important or important to their organizations.

60% said they had experienced an IT system failure in the past 24 months, and 6% had experiences damages to brand or reputation. Many had experienced system disruption due to human error (52%), natural or manmade disasters (37%), data loss (backup/ restore issues) (29%), third-party partner security breach or system failure (23%), and cyber-security breach (23%).

Survey and roundtable participants echoed a common refrain throughout the study: the need for planning. Planning is needed, participants agreed, to maintain business continuity in the event of a power failure, natural disaster or human error, as well as a plan to identify weaknesses and protect organizational systems against hackers and other cyber threats.

Many of those with plans acknowledged that their cyber security and business continuity processes and policies were not consistently applied throughout the organization.

- 3 in 10 respondents said their company had a formal strategy that is applied consistently across their entire enterprise
- 3 in 10 said they had a formal strategy with inconsistent application
- 4 in 10 said their strategy was informal or "ad hoc"

Those respondents with formal strategies, applied consistently, were far more likely to agree that their leaders recognized that IT risks affected revenues (90% compared to 56% of those with ad hoc strategies or no strategy) and brand image (95% compared to 50% of those with ad hoc or no strategies).

According to one roundtable participant whose company was experiencing rapid growth, it was confusing to try to blend employees with very different backgrounds and attitudes towards security practices. The financial executive observed that the company must develop a unified consistent approach to be used by and applied to all company employees.

Given that one of the top barriers to improving cybersecurity at their organizations was a lack of resources, along with a lack of knowledge of the most up to date best practices, gaining the buy-in of colleagues to support improvements is clearly critical. To improve security, participants observed that it was necessary to obtain buy-in by the rest of the C-Suite, including the CEO and the board. This was best achieved not by painting an apocalyptic scenario, but rather by presenting a reasoned business plan complete with potential impacts to revenue generation, growth, the bottom line, brand and reputation, and potential operational downtime.

INTRODUCTION

Senior financial executives are carrying a heavy load of responsibilities. Beyond their traditional roles in finance, such as financial reporting, accounting, taxation, treasury, compliance, risk management, many also have assumed responsibility for IT. As IT grows more complex, so does the burden of keeping up with technological developments. The importance of business continuity is reiterated with every flood, ice storm, power failure or other disaster or breakdown. Likewise, the threats to cybersecurity are increasing daily as hackers grow more skilled, creating more pressure on executives to stay on top of best practices. Simple human error is an ever present risk. Personal mobile devices are used by employees for business. At the same time, many organizations are working with outdated infrastructure and budgetary constraints limiting their ability to stay on top of new developments, train staff and update their hardware and software.[1]

This study attempts to highlight some of the top concerns of Canadian senior financial executives around cyber security and business continuity and to explore the level of evolution of their plans. To what extent are Canadian financial executives responsible for cybersecurity and business continuity risk? What are some suggested next steps for financial executives to mitigate organizational risk, within their existing resource constraints of time, staff and budget?

METHODOLOGY AND DEMOGRAPHICS

Respondents completed an online survey which was distributed to financial executives in November and December, 2013. The survey respondents represented a range of industries and sectors, and included executives from small, medium and large organizations. 38% of respondents were CFOs, 11% VP Finance, 8% Controllers and 7% Director of Finance. For further demographic information, see Appendix A.

Insights were also gathered from an afternoon roundtable of financial executives, which took place on Dec. 3, 2013, during which participants from three cities (Toronto, Montreal and Calgary) were connected by videoconference. Due to the nature of the research topic, for the protection of the privacy of the round table participants, names and organizations were not used.

[1] Cawthray, Stewart. 10 Essential Security Practices. IBM Security Services. 2014 (See Appendix A)

RESPONSIBILITY AND KNOWLEDGE OF RESPONDENTS

Survey respondents, comprised mainly of senior financial executives, assume high levels of responsibility in their daily jobs. The vast majority of survey respondents were responsible for ensuring compliance, managing budgets, evaluating and managing business risk and setting financial priorities (see Chart1 on page 6). When it came to information technology security risk management, the majority stated they were knowledgeable about planning for IT security (71%) and the implementation of IT security measures at their organization (68%) (see Chart 2 and 3).

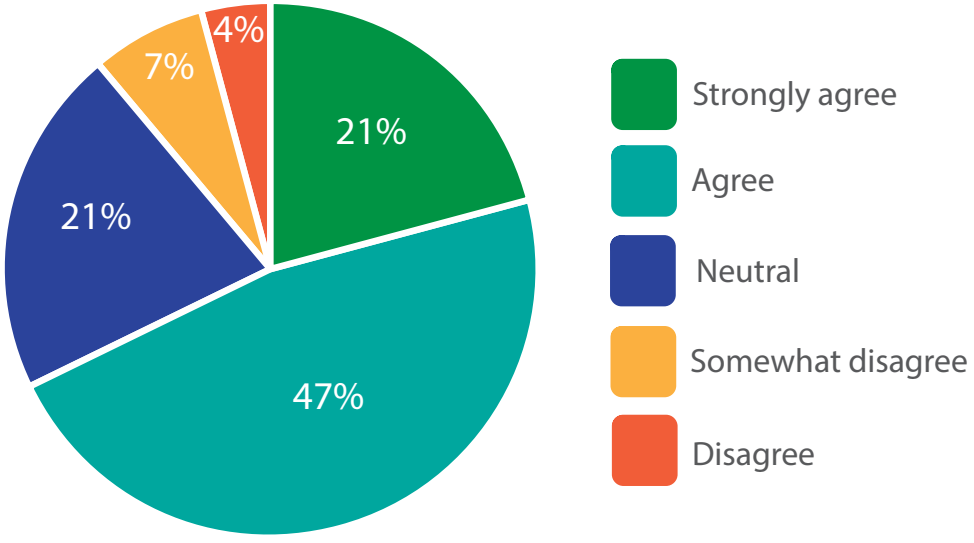
Many survey respondents were fully or mostly responsible for IT (42%), and an additional 30% shared responsibility for IT. 29% had limited responsibility.

CFOs hold direct responsibility for IT at many organizations. According to 68% of respondents, the CFO signs off and approves IT security spending, eclipsed only by the president and CEO, who has final approval of the plan at organizations employing 79% of respondents (see Chart 4).

> “The challenge is as a finance person challenging the IT around what I call the techno-speak because I would be taken down some really interesting roads. I fortunately know enough about IT that I could ask for clarity, and very quickly discovered that I was being presented a lot of smoke and mirrors. I’m now in month 10 trying to put in what I think is a basic data recovery continuity program and leveraging some of the new technologies in and around doing some server virtualization and what’s appropriate to put on the Cloud.”

CHART 1 – FROM THE ACTIVITIES LISTED BELOW, WHICH TASKS FORM PART OF YOUR RESPONSIBILITIES?

CHART 2 – ARE YOU KNOWLEDGEABLE ABOUT THE IMPLEMENTATION OF IT SECURITY MEASURES IN YOUR ORGANIZATION?



RESPONSIBILITY AND KNOWLEDGE OF RESPONDENTS

CHART 3 – ARE YOU KNOWLEDGEABLE ABOUT PLANNING FOR IT SECURITY AT YOUR ORGANIZATION?

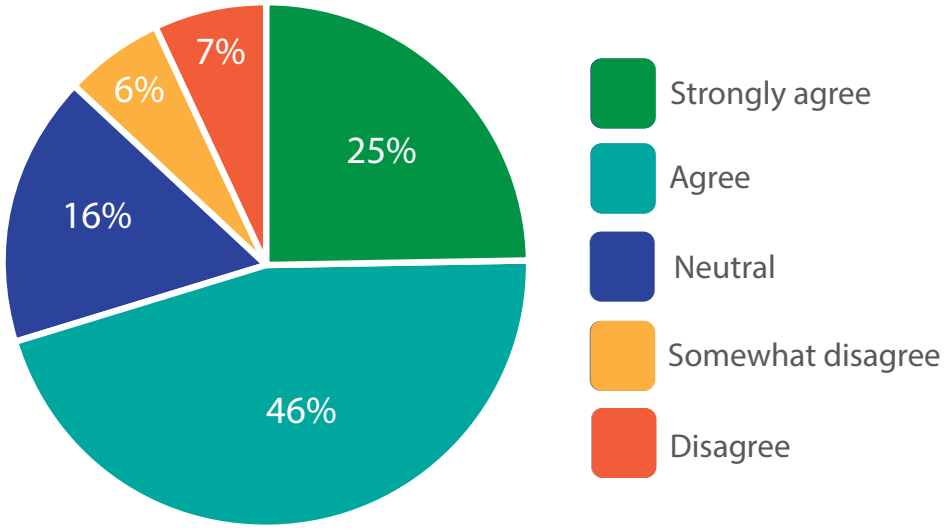
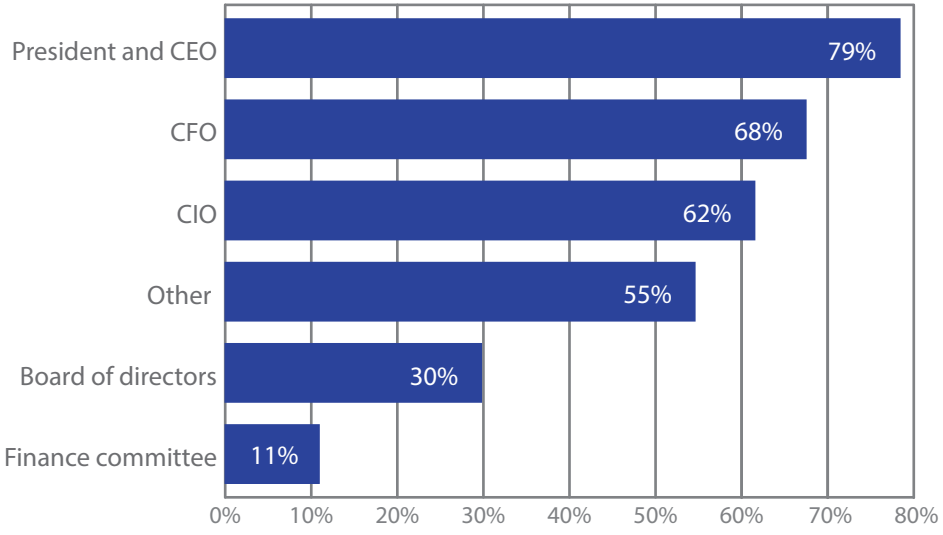


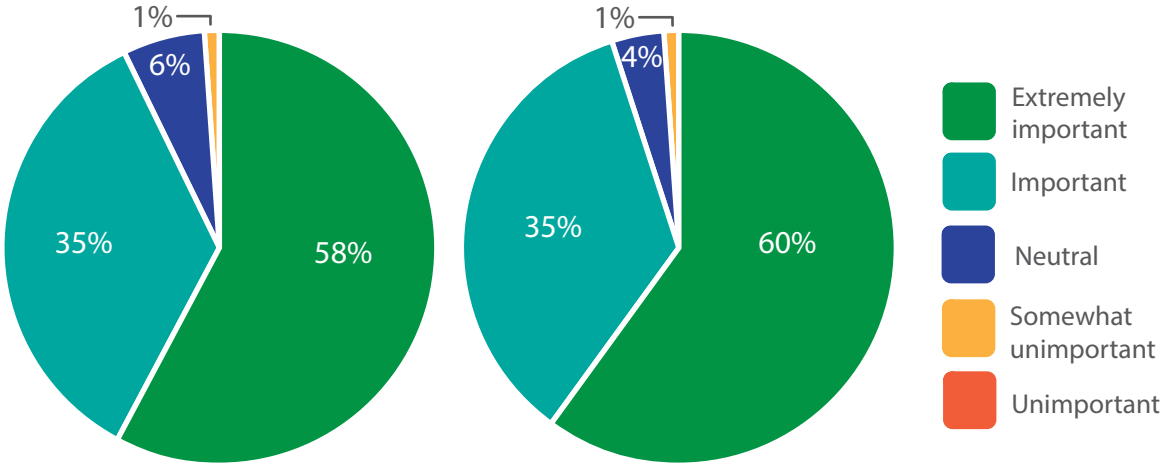
CHART 4 – BUSINESS CONTINUITY AND IT SECURITY PLANS ARE APPROVED AND SIGNED OFF BY MY ORGANIZATION'S:



IMPORTANCE OF IT SECURITY AND BUSINESS CONTINUITY TO ORGANIZATIONS

The overwhelming majority of survey respondents rated the importance of IT security as extremely important or important (93%) to their organizations. Business continuity, defined as the uninterrupted flow of business) was ranked even higher: 95% of survey respondents said it was extremely important or important to their organizations (See Chart 5).

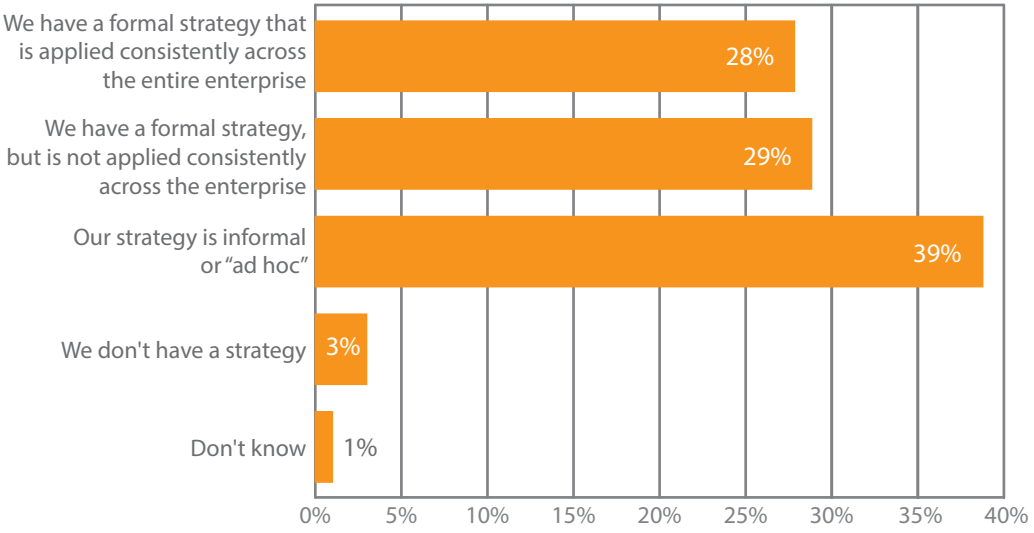
CHART 5 – PLEASE RATE THE IMPORTANT OF IT SECURITY AND BUSINESS CONTINUITY TO YOUR ORGANIZATION:



> "This subject is very close to my heart, because it's just interwoven right into our business model. We do a lot of business where we're enabled through government contracts. And the requirements or the ante to the poker game is redundancy. So I don't want to use the term bulletproof, but we do have a lot of redundant capabilities. We have to be 24/7. We're a global operation."

However, despite the overwhelming importance of IT security and business continuity, as described by survey respondents, only three in 10 respondents said their company had a formal strategy that is applied consistently across their entire enterprise. Another three in 10 said they had a formal strategy with inconsistent application, and four in 10 said their strategy was informal or "ad hoc" (see Chart 6). The remainder did not have a strategy (or did not know). Most survey respondents said their organization's IT security management program was at best at either a middle or late-middle stage of development, with most program activities partially or fully deployed. Only one in ten survey respondent said that their IT security program activities were at a mature stage.

CHART 6 – PLEASE CHECK ONE STATEMENT THAT BEST DESCRIBES YOUR ORGANIZATION'S APPROACH OR STRATEGY TO IT RISK (SECURITY/BUSINESS CONTINUITY) MANAGEMENT.



Case study: Managing IT risk during rapid business growth

The rapid growth of new Canadian Internet provider TekSavvy from a family-run business to a medium-sized enterprise has brought some growing pains in terms of the introduction of consistent security policies and procedures. The company has grown exponentially over the last three years from 60 people to 500.

"We try to retain the family type of environment, which in itself creates its own exposure. We had staff coming from large organizations who had restrictions on the websites that they could access, and we try to refrain from doing that to allow the employees the sense of "family". However, not everybody has the best interest of the family in mind. Therefore, we've begun the process of streamlining and locking down accesses thus diminishing the culture that has made us where we are today. It's a very large struggle because that's how we try to differentiate ourselves from our competitors, and from the other employers in the marketplace. It's been a challenge. I had a meeting a week ago with an insurance company talking about cyber risk insurance coverage and it highlighted that we have some work ahead of us. We've been growing into a mid-size business and it has highlighted many things that the business can no longer allow but was able to do when you were a small business with 50 employees. From supporting our customer, the security for the customer and how the customer accesses their account, I believe we do a very good job. However, we need to protect ourselves more from those who could potentially bring our system down."

Jim King – VP Finance, TekSavvy

PERCEPTION OF IT RISK

Overall, most respondents said their organization's leaders recognize that IT risks affect revenues (75%) and brand image (71%).

Those respondents with formal strategies, applied consistently, were far more likely to agree that their leaders recognized that IT risks affected revenues (90% compared to 56% of those with ad hoc strategies or no strategy) and brand image (95% compared to 50% of those with ad hoc or no strategies) (See Charts 7 and 8).

> "I was at a board committee meeting where cyber risk got elevated to be its own risk. That was a new one for us. It used to be within our IT risk. It got promoted. So there is a very high awareness. One of the challenges for us is, because we're a small environment, my IT staff is too. And so it's really keeping that expertise in-house and using outside consultants for the expertise where appropriate."
>
> **Linda Pendrill – CFO, Canadian Investor Protection Fund**

CHART 7 – PERCEPTION OF LEADERSHIP RECOGNITION OF IT RISK ON REVENUES

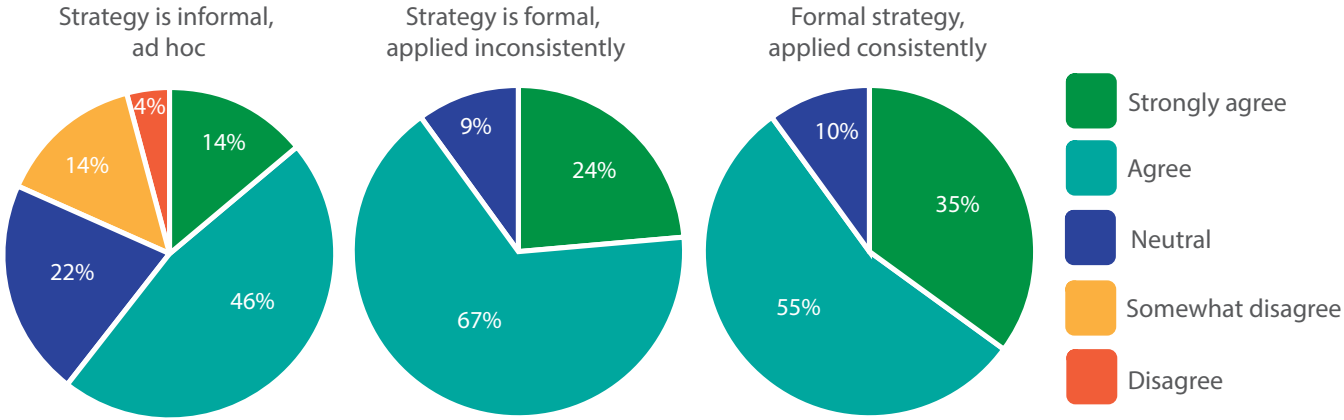
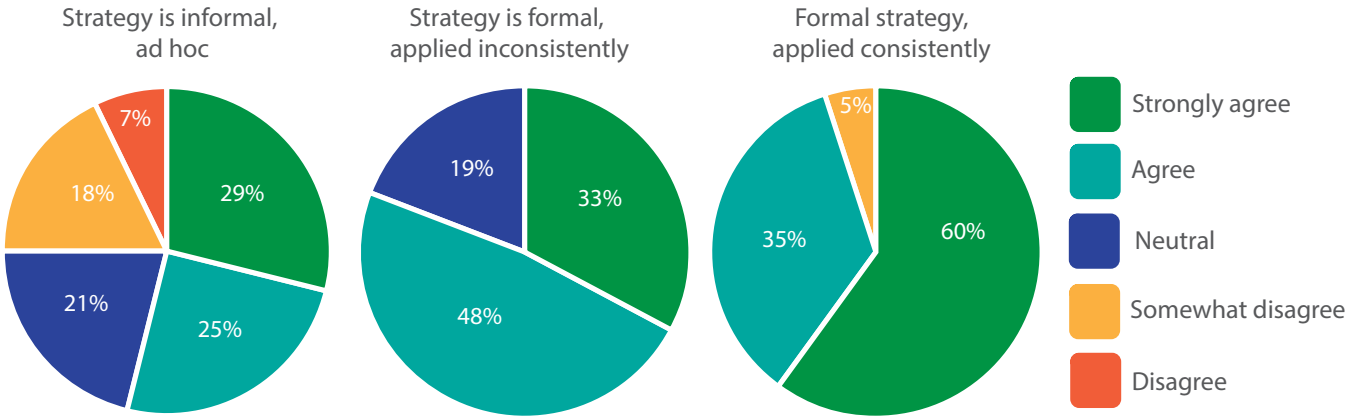


CHART 8 – PERCEPTION OF LEADERSHIP RECOGNITION OF IT RISK ON BRAND IMAGE



PERCEPTION OF IT RISK

Fortunately, though, disruptions to business process or IT services are rare events for most respondents, (79% agreed natural or manmade disasters are rare events at their organization, and 86% agree disruptions cause by cybersecurity breaches are rare events).

Sometimes the perception of IT risk can vary within an organization. For instance, employees of a Canadian subsidiary of a European parent found their parent company was more risk averse than they were.

> "Every year we invest and spend a lot of money and time to secure our systems, to do assessments, but being a European company in North America, it's more difficult because the understanding is very different compared to a North American company. I would say our parent company culture is more conservative, really risk averse. That creates some issues when we team up with North American partners. . . . Overall, maybe we spend more because we cannot always go with the most practical or most efficient solution. The best example is that our ERP servers are in Europe, which makes tthings more difficult if you want to make some changes . . . and we require 24/7 support. It's user support and efficiency versus perfection of security, which our headquarters tries to accomplish. They have been very successful, there are very good reasons to be careful, but I think it's very difficult to explain it to our North American partners."

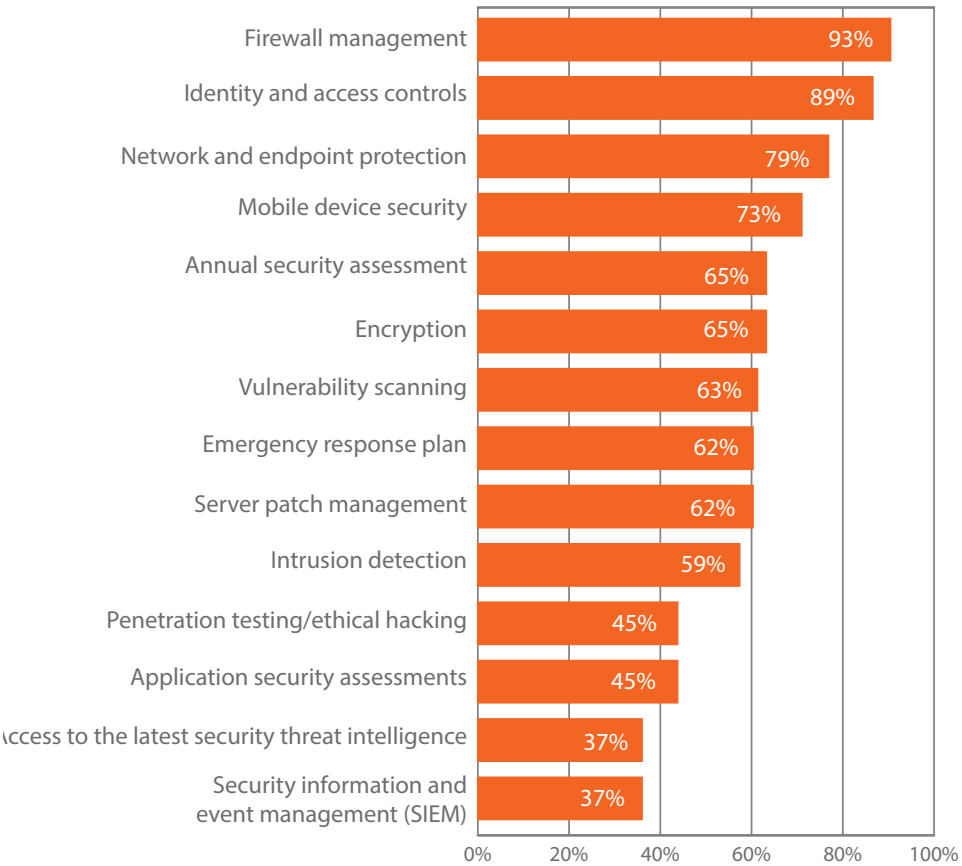
> “To get the board on side, you can’t argue the world’s going to end. It’s that business value component. I was very lucky to walk into a well-educated board and it was a three-sentence discussion saying: ‘We don’t have this, this and this.’ It was: ‘Okay, just go and make it happen.’ If you can tie in – not ‘the world’s going to collapse’ – but here is the impact either on our bottom line or on our brand or on our reputational risk, then payback is significant.”

> “At our company we’ve got around five people working on IT security and they are responsible for planning to upgrade all our security software. I know that they have to change the antivirus and anti spam software, so they will need to look at the mobile device security also because mobile use is going up. People want to have access remotely to all business applications so we need to be careful because with the mobile you can use it within wifi, public zone or somewhere that is not very secure. So we need to be aware of this. Our team is responsible for that. So they have to give us a plan each year to ensure that we will have a good level of security.”

IT SECURITY CONTROLS

The most common IT security control in place amongst respondents is the firewall, followed by identity and access controls (See Chart 9). Fewer than half of respondents said they have ethical hacking testing in place or planned. (An ethical hacker is an IT expert who attacks a computer or network's security system on behalf of its owners, in order to discover weak points that a malicious hacker could also identify.)

CHART 9 – PLEASE CHECK THE IT SECURITY CONTROLS YOUR ORGANIZATION HAS IN PLACE OR PLANS TO IMPLEMENT IN THE NEXT 12 MONTHS (PLEASE CHECK ALL THAT APPLY)



"I am the last guy who's got a technological background, and like many CFOs, IT seems to report up into the CFO. We have 15 people in IT and the dollar investment is in the millions. My role is to try to shape the strategy: value for money, risk mitigation and then just provide the strategic leadership of trying to keep ahead of it. It's changing every day, and I'm starting to see where future activities and potential vulnerabilities could be inside the organization. We're pretty good on the outside with the parameters, all the conventional firewalls and encryption and VPNs and all that stuff, but how do you protect your people from themselves. That's a tough one. You can have the best written policy and procedure manual, but how do you know that somebody didn't open an email they shouldn't have opened and now you're infected. How do you protect your organization from its own people?"

BYOD: Bring your own device

"We have a policy around bringing your own device, because younger employees tend to prefer their own devices. We have a company policy in place that ensures that, if employees wish to use their own device at work, they must agree to install an application that enables remote control of the device. If anything happened, say the device was lost or the employee left, then that software can trigger the complete immobilization of the device. So that's essentially how we get around the security issues. It works quite effectively."

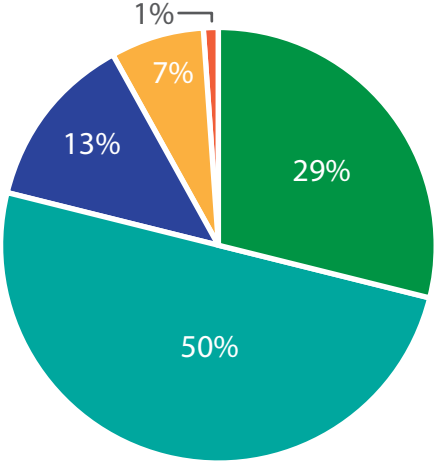
Bill Ross – VP Finance, Enbridge Pipelines

DISRUPTION

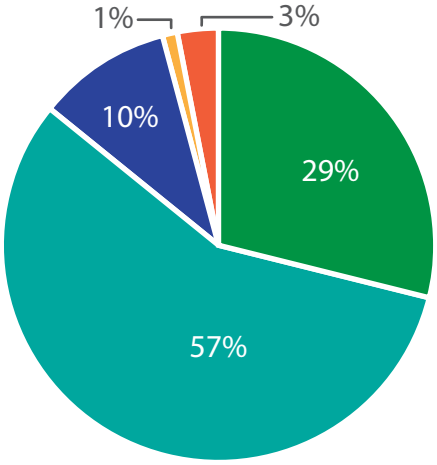
Most survey respondents said that disruptions to business processes or IT services are rare events (See Chart 10).

CHART 10 – DISRUPTION TO BUSINESS PROCESSES

In my organization, disruption to business processes or IT services caused by **natural or manmade disasters are rare events.**



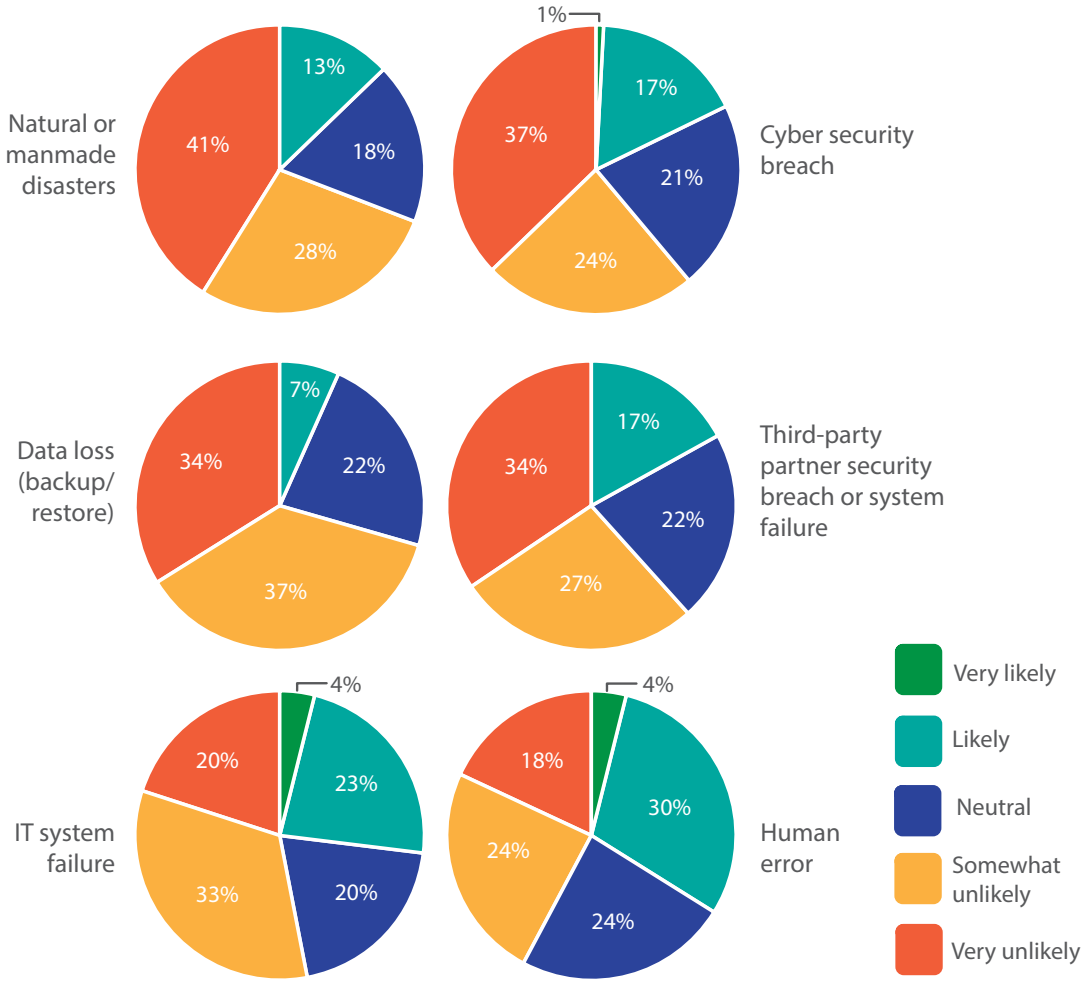
In my organization, disruption to business processes or IT services caused by **cyber security breaches are rare events.**



When asked about disruptions over the past 24 months, however, respondents let us know the following:

	IT system failure	Human error	Cyber security breach	Data loss (backup/ restore)	Natural or manmade disasters	Third-party partner security breach or system failure
Average number of disruptions (in past 24 months)	4	3	2	2	2	2

CHART 11 – IN THE NEXT 24 MONTHS, HOW OFTEN DO YOU ANTICIPATE YOUR ORGANIZATION WILL EXPERIENCE DISRUPTIONS TO BUSINESS OR IT OPERATIONS DUE ANY OF THE SIX COMMON THREATS LISTED BELOW?



Interestingly, a significant minority of survey respondents said they anticipated future disruptions to business or IT operations. For instance, 34% of respondents said they expected disruption due to human error, and 27% said disruption due to IT system failure was likely or very likely. In comparison, only 7% said it was likely or very likely that the organization would experience data loss due to a failure to backup information. Less than 13% expected disruptions due to natural or manmade disasters (See Chart 11).

Case study of a virus

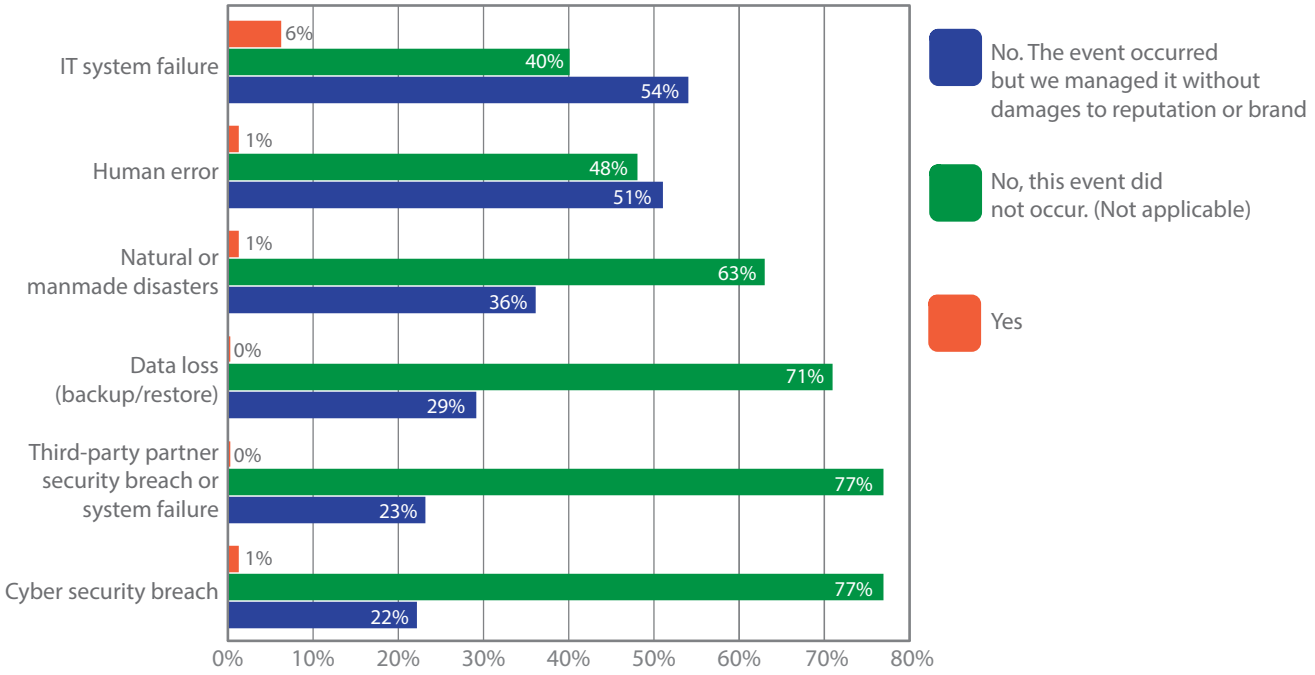
This happened quite recently. So we haven't officially located the source, although we know it's come through an email. So for us, developing a plan on implementing one of the things we've done is we've realized that the server that we had our ERP system on coincidentally had some vulnerabilities due to the age of the equipment. We are looking at implementing a multi-level security system so that it's authenticated to being real and then the one thing we're looking at implementing specifically is locking our people, because interestingly enough, the system where some data tables were deleted, these were all happening at really odd hours. So one of the ways we are looking at implementing this is limit all users to accessing the system at a certain time frame which is typically our work day. The risk of course of doing something like that means that for instance, somebody has been sick all day but tonight they're feeling better and they want to do the work, but they can't. So there are some risks to setting that kind of level of security. So we are definitely looking at a higher level of encryption and a backup system for us has been huge because we actually use a backup system and learned that that doesn't tell you when there are errors in the database. We lost about a weeks' worth of work, which wasn't too bad considering other scenarios. And so we're currently looking at not just implementing a security measure, but at the same time, how do we test that measure from time to time to make sure that it is actually effective.

Marietjie Bower – VP and CFO, Commerx Corp.

CONSEQUENCES: DAMAGES TO BRAND VALUE

60% said they had experienced an IT system failure in the past 24 months, and 6% had experiences damages to brand or reputation. Many had experienced system disruption due to human error (52%), natural or manmade disasters (37%), data loss (backup/ restore issues) (29%), third-party partner security breach or system failure (23%), and cyber-security breach (23%).

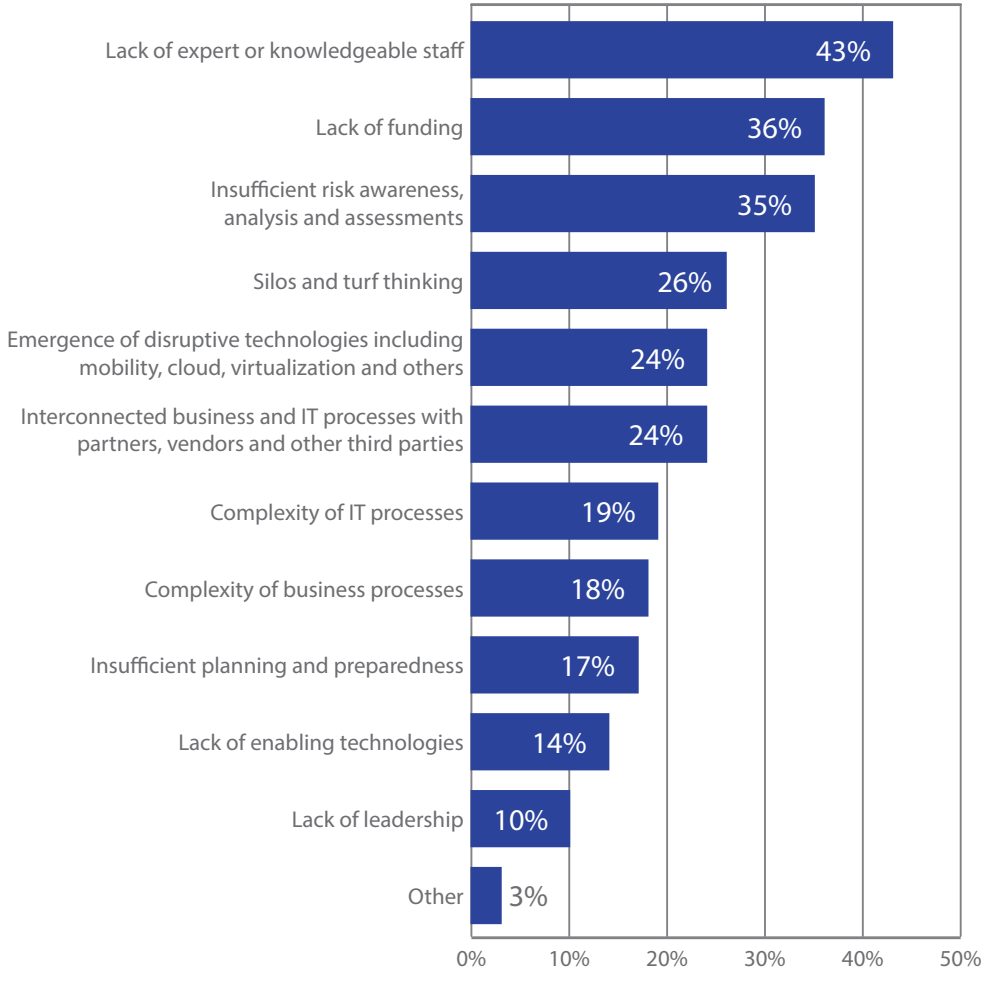
CHART 12 – IN THE PAST 24 MONTHS, HAS YOUR ORGANIZATION EXPERIENCED DAMAGES TO HIS REPUTATION OR BRAND VALUE DUE TO ONE OR MORE OF THE SIX COMMON THREATS LISTED BELOW?



BARRIERS TO IMPROVEMENT

The greatest barrier to achieving a highly effective IT risk management program (encompassing both security and business continuity) is a lack of expert staff (43%) followed by a lack of funding (36%) and insufficient risk awareness, analysis and assessments (35%) (See Chart 13).

CHART 13 – WHAT DO YOU SEE AS THE MOST SIGNIFICANT BARRIERS TO ACHIEVING A HIGHLY EFFECTIVE IT RISK (SECURITY/BUSINESS CONTINUITY) MANAGEMENT PROGRAM WITHIN YOUR ORGANIZATION? PLEASE SELECT YOUR TOP TWO CHOICES.



Lack of funding

"It's very time consuming, there's a lot of information that has to be gathered. And sometimes the resources are not available to focus and do a good job at it."

Employee risk management

"Where there is an area of risk is when you are dealing with a company with thousands of employees and you have to terminate people. Whether they are terminated or they leave on their own, you have to have a robust system to ensure that the employee doesn't leave with the computer, and that all their system access is disabled and deactivated."

NEXT STEPS

Survey respondents suggested a range of next steps that their organizations could take to improve IT security and business continuity. These include:

PLANNING:

- For business interruption
- Redundancy
- Increase frequency of system review

EDUCATION:

- Staff training
- C-suite and executive buy-in
- Board awareness (e.g. risk management)

ALLOCATING RESOURCES:

- Calculating security budgets
- Making a business case

According to some 2013 Gartner studies on IT spending, the average firm surveyed was spending between 3.5 to 5% of their IT budget on security spending. Gartner found financial services were higher, more than 9%. IBM's own informal research of its customers found that as customers became more mature with their security programs, their overall spending decreased closer to the 3.5% of their overall IT budget. But according to Stewart Cathray of IBM Canada, the actual dollar spend remained the same, but was allocated within divisional budgets because companies embedded security into their operational areas and security became part of IT staff responsibility. Areas that were deemed pure security remained the security intelligence, the incident response and governance, whereas issues like patch management and network security actually got distributed to the different groups from an operational level. However, the threat management, threat response and governance remained as a dedicated security spend. So the more mature organizations became, they would actually see their dollar overall spend come down.

> “It is very much an employee learning experience. If you teach your employees to do something that they wouldn’t do at home, you’re almost three-quarters of the way there to implementing an effective security protocol. That said, the proliferation of mobile devices and the ability to facilitate the dissemination of information ultimately leads to good efficiencies. So I find we are increasingly paying more attention to security, employee training around this. You want to focus on some of the dangers, particularly if you’re in an off-site location and you’re communicating with unencrypted data from a device. So that’s generally our philosophy. Security is constantly being enhanced, leading to more spending in this area.”
>
> **Bill Ross – VP Finance, Enbridge Pipelines**

CONCLUSION

Survey and roundtable participants echoed a common refrain throughout the study: the need for planning. Planning is needed, participants agreed, to maintain business continuity in the event of a power failure, natural disaster or human error, as well as a plan to identify weaknesses and protect organizational systems against hackers and other cyberthreats.

Many of those with plans acknowledged that their cyber security and business continuity processes and policies were not consistently applied throughout the organization. According to one roundtable participant whose company was experiencing rapid growth, it was confusing to try to blend employees with very different backgrounds and attitudes towards security practices. The financial executive observed that the company must develop a unified consistent approach to be used by and applied to all company employees.

Given that one of the top barriers to improving cybersecurity at their organizations was a lack of resources, along with a lack of knowledge of the most up to date best practices, gaining the buy-in of colleagues to support improvements is clearly critical. To improve security, participants observed that it was necessary to obtain buy-in by the rest of the C-Suite, including the CEO, and the board. This was best achieved not by painting an apocalyptic scenario, but rather by presenting a reasoned business plan complete with potential impacts to revenue generation, growth, the bottom line, brand and reputation, and potential operational downtime.

APPENDIX A: EFFECTIVE APPROACHES TO ADDRESSING SECURITY AND BUSINESS CONTINUITY

Financial executives and other C-level executives concerned or having responsibilities for IT risk in their organizations may find the following resources, suggestions and best practices useful:

SECURITY (IBM'S 10 ESSENTIAL PRACTICES)

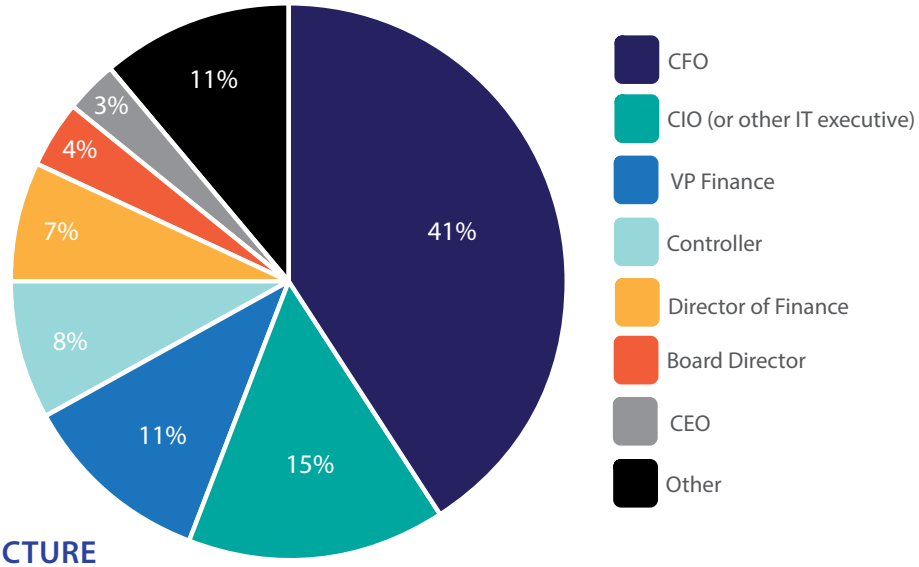
1. Build a risk aware culture and management system.
2. Manage security incidents with greater intelligence.
3. Defend the mobile and social workplace .
4. Security-rich services, by design.
5. Automate security "hygiene".
6. Control network access and assure resilience.
7. Address new complexities of cloud and virtualization.
8. Manage third-party security compliance.
9. Secure data and protect privacy.
10. Manage the identity lifecycle.

BUSINESS CONTINUITY

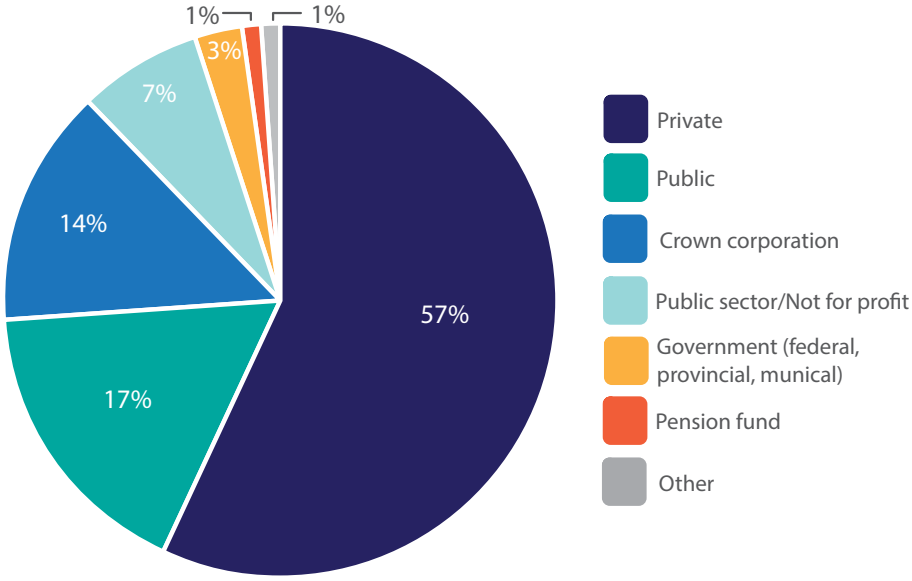
1. Ensure Disaster Recovery plans/processes are up to date and tested.
2. Make sure Disaster Recovery is a Boardroom agenda item.
3. Understand that increased demand for availability can be different by Business Unit and/or Application.
4. Disaster Recovery planning needs to encompass more that IT. For example consider using reputational Risk as a metric and consideration for ROI.
5. Look for new Business Continuity approaches that improve resiliency and recovery options, save costs and reduce risk
6. Leverage new technologies to enable the enterprise and workforce.
7. Understand how operations will function. For example, what is your business continuity plan for critical support functions like payroll?
8. Ensure you have effective communications with your workforce, the public, suppliers, partners, authorities, shareholders and the media. This includes the use of social media.
9. Ensure you have identified alternatives to regain access to information and technology to resume tasks – whether physical, mobile or virtual facilities.
10. Understand the impact of thirdparty service/product suppliers that support your business model. For example, make your third party providers adhere to the same continuity standards as your own company.

APPENDIX B: DEMOGRAPHICS

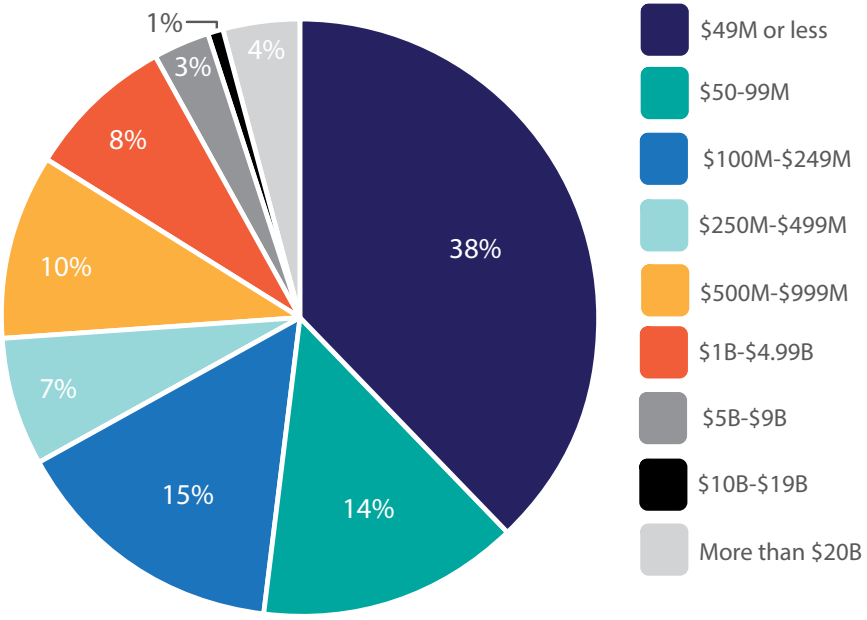
POSITION TITLE



CORPORATE STRUCTURE

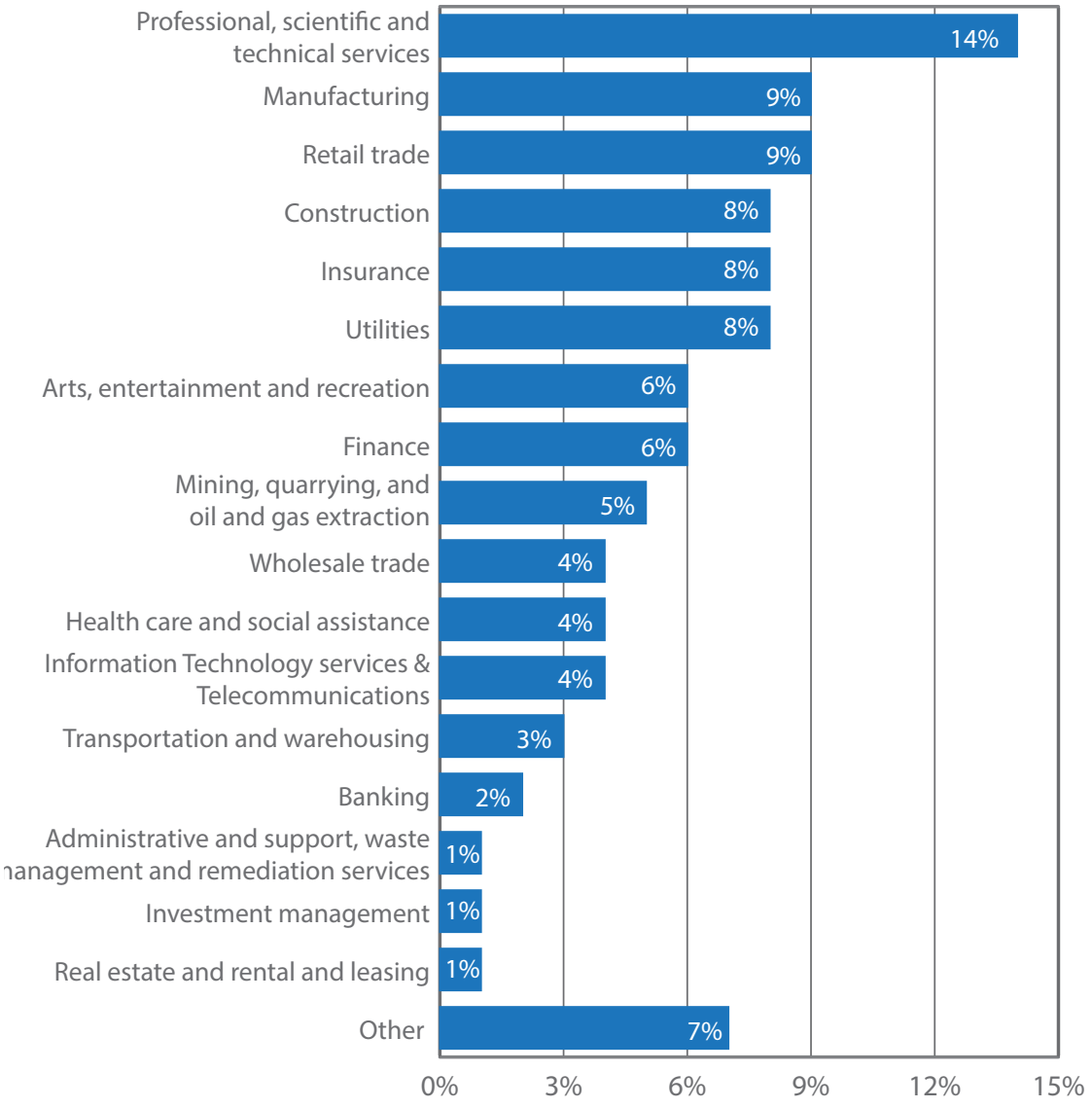


ANNUAL REVENUE



APPENDIX B: DEMOGRAPHICS

INDUSTRY CLASSIFICATION



APPENDIX C: ROUND TABLE PARTICIPANTS

Forum Chair:	Michael Conway – President and CEO, FEI Canada
Moderators:	Christian Bellavance – VP, Research & Communications, FEI Canada Stephen Smith – Executive, Security Services, IBM Canada
IBM Canada:	Stewart Cawthray – Chief Security Architect, IBM Security Services, IBM Canada Peter Gladwish – Executive, Business Continuity and Resiliency Services, IBM Canada
Toronto Participants:	Bruce Bailey – VP Finance, Alcohol Countermeasures Corp. George Chiarucci – CFO, Prism Medical Catherine Fels-Smith – VP, Finance and Operations, Toronto Region Board of Trade Jim King – VP Finance, TekSavvy Danielle Parent – VP Finance, Platform Products Group, Fujitsu Linda Pendrill – CFO, Canadian Investor Protection Fund Derek Petridis – CFO, Principal, Shikatani Lacroix Design Judith Purves – CFO, IBM Canada
Montreal Participants:	Yanic Brisson – Director, Revenue Assurance and Investigations, Videotron Markus Weiss – Director, Shared Services North America and Financial Controller, Rheinmetall Group
Calgary Participants:	Marietje Bower – Controller, Commerx Corporation Bill Ross – VP Finance, Enbridge
Observers:	Megan Bell – Communications and Events Coordinator, FEI Canada Laura Bobak – Research and Communications Manager, FEI Canada Steve Bower – VP Programs, FEI Canada Willie Wong – Marketing Manager – Global Technology Services at IBM Canada

THE CANADIAN FINANCIAL EXECUTIVES RESEARCH FOUNDATION (CFERF) is the non-profit research institute of FEI Canada. The foundation's mandate is to advance the profession and practices of financial management through research. CFERF undertakes objective research projects relevant to the needs of FEI Canada's 1,700 members in working toward the advancement of corporate efficiency in Canada. Further information can be found at www.feicanada.org.

FINANCIAL EXECUTIVES INTERNATIONAL CANADA (FEI CANADA) is the all industry professional membership association for senior financial executives. With eleven chapters across Canada and 1,700 members, FEI Canada provides professional development, thought leadership and advocacy services to its members. The association membership, which consists of Chief Financial Officers, Audit Committee Directors and senior executives in the Finance, Controller, Treasury and Taxation functions, represents a significant number of Canada's leading and most influential corporations. Further information can be found at www.feicanada.org. Follow on Twitter @financial_execs

IBM is a globally integrated enterprise operating in over 170 countries. IBMers around the world bring innovative solutions to a diverse client base to help solve some of their toughest business challenges. In addition to being the world's largest IT and consulting services company, IBM is a global business and technology leader, innovating in research and development to shape the future of society at large. IBM's prized research, development and technical talent around the world partner with governments, corporations, thinkers and doers on ground-breaking real world problems to help make the world work better and build a smarter planet.

IBM in Canada has played an important role in the corporation's history for over a century. We make significant contributions to our nation's economy as one of the country's largest research and development investors and IT exporters. We attract, develop and retain highly-skilled Canadians, engaging them in meaningful work that impacts not just Canada, but the world. And we make significant investments in new offerings for the Canadian market, such as the more than $165 million we invested in datacentre expansion in 2012.

CORPORATE DONORS:

GOLD ($10,000 +):
Bell Canada
Husky Energy Inc.

SILVER ($5,000-10,000):
Agrium Inc.
Brookfield Partners Foundation
CGI Group Inc.
Imperial Oil Ltd.

BRONZE ($1,000-5,000):
Altagas
Canadian Western Bank Group
Intact Financial Corporation
OpenText Corporation
PotashCorp
Shikatani Lacroix Design

FEI CANADA'S RESEARCH TEAM:

Michael Conway – President and Chief Executive Officer

Christian Bellavance – Vice President, Research Communications

Laura Bobak – Research and Communications Manager

170 University Avenue, Suite 1201
Toronto, ON M5H 3B3
T 416.366.3007
F 416.336.3008
www.feicanada.org

cferf℠