Building a strong profession today, for tomorrow

The Canadian Institute of Financial Planners

Financial Services
Cyber Risk & Compliance

May 29, 2017

Agenda

- Introduction & Overview
- Preparing your Business Operations and Staff Against
  - Increasing Risks & Security Breaches
  - Top 5 Increasing Risks to Your Business
  - Focus on Cyber Security & Liability
  - Cyber Liability – What to Expect in 2017
  - Cyber Liability – Some Implications
- 2017 Cyber Risk Survey – Top Findings
- Mitigating your Risks
- What are your Options
  - Start with a Cyber Risk Assessment

Peter MacMillan

- CEO of 4Cast Services Inc. (www.4castservcies.com)
- Peter has over 30+ years experience at all leadership levels covering regional and national organization. An experienced entrepreneur who specializes in assisting organizations of all size develop resiliency and recovery strategies ensuring they can prosper and grow.

Eric Strong`

- President 4Cast Services Inc. (www.4castservices.com)
- Eric has over 25+ years executive leadership with diverse local and global organizations with a focus on delivering a portfolio of strategic recovery services utilizing human capital and business process expertise as well as current technologies.

Increasing Risks & Security Breaches

- Doing business today is tough.
- A study by Forrester Research found that 82% of business continuity decision-makers and influencers felt that their organization's risk level was increasing.
- A recent Cyber Risk Survey identified that in 2016:
  - A US$81 million cyber heist involving an attack against global financial messaging system SWIFT.
  - Large data thefts from social media networks, including Tumblr (65 million accounts), LinkedIn (117 million accounts), adultFriendFinder.com (339 million accounts), Myspace (427 million accounts) and Yahoo (500 million accounts).
  - The potential compromise of hundreds of point-of-sale systems, enabling hackers to remotely administer PoS devices located in retail outlets around the world.

Top 5 Increasing Risks to Your Business

1. Reliance on technology
2. Business complexity, international markets and regulations
3. Increasing frequency and intensity of natural disasters
4. Reliance on third parties who could cause you to fail
5. Data Security Breaches and Privacy Losses

- Data/Cyber Security Breach – it is **When** will it happen, not **If**
  - Blanket cyber attacks are happening almost every day.

Most people are starting to realize that there are only two different types of companies in the world: those that have been breached and know it and those that have been breached and don't know it.

Ted Schlein, Venture Capitalist at Kleiner Perkins Caufield & Byers

Cyber Liability – What to Expect in 2017

The following 5 key cyber security trends in 2017 should be on every Senior Executive, Officer and Risk Manager's radar.

1. Mandatory Data Breach Notification Is Coming

- It is anticipated regulations will come into force in 2017 for mandatory data breach notification and fines of up to $100,000 for non-compliance.
- You will be required to review your existing policies or implement new internal processes for identifying, recording and responding to data breaches.
- From an enforcement standpoint, violations of the breach notification or the record keeping requirements such as covering up a breach or failing to notify or keep records, can all trigger these fines.

Reference: Miller Thompson LLP, March 2017

Cyber Liability – What to Expect in 2017

2. Rising Rapid Growth in Cybersecurity and Privacy Litigation

- 2017 will see continued growth of class action certification of cybersecurity and privacy actions and further reliance on torts such as "inclusion upon seclusion" and "disclosure of private facts".
- Once mandatory data breach notification comes into force, litigation in this area will only increase.

3. Boards' Oversight – "Business Judgment Rule" Should Prevail

- Boards will increasingly need to be engaged in cybersecurity oversight by scrutinizing managements' strategy and plans to effectively identify, mitigate and respond to cyber threats.
- Boards will have to move from a passive oversight model (i.e., simply being informed about cyber risks) to an active oversight model (i.e., being engaged in an ongoing dialogue with management about cyber risks).

Reference: Miller Thompson LLP, March 2017

Cyber Liability – What to Expect in 2017

4. Vendor Management – Beware of the Weakest Link

- Recognizing that hackers may come at you through your vendors to access & compromise your network and your customers' networks. To protect yourself you will need to be proactive scrutinizing and developing policies surrounding your vendors' cybersecurity measures.

5. Accelerated Adoption of Cyber Insurance

- Canadian organizations will increasingly turn to cyber insurance as part of their cyber risk mitigation strategy.
- However, care needs to be taken to ensure you obtain the appropriate type of coverage based on your particular cyber risk profile.
- Most organizations will find they do not have the in-house skilled staff to help determine their corporate cyber risk profile and will need to engage outside experts.

Reference: Miller Thompson LLP, March 2017

Cyber Liability – Some Implications

- The Canadian **Digital Privacy Act (DPA)** makes extensive revisions to **PIPEDA** (Personal Information Protection and Electronic Documents Act).
  - A new era of privacy law and corporate liability has been ushered in with the passage of the DPA. [With its pending breach notification and record keeping provisions]
- **Canadian Anti-Spam Legislation (CASL)** The next phase of CASL is the Private Right of Action which will come into force July 1, 2017.
  - In order to mitigate their risks organizations are well advised to have a Compliance Program, documented and implemented for July 1, 2017.
- While the liability can be $200 for each breach per day, organizations sending out large numbers of targeted e-mails each day could have far higher liability, above and beyond any compensatory damages.
  - **E.g. 1,000 emails per hour X 1 day (8 hours) X $200 each = $1,600,000**
- Further, if implicated in the breach, officers, directors and agents of the organization can be jointly and severally liable for contraventions even if the business that committed the acts is not sued.

Reference: McMillan LLP, February 2017

Cyber Risk Survey 2017

Key findings

one

Awareness of cyber risk has increased as the problem grows – but concrete actions have not changed

two

Despite concerns about the increasing cyber threat, organisations remain complacent about reviewing and testing their own cyber resilience (and the cyber resilience of their suppliers)

three

Cyber security is still (wrongly) seen as being primarily an IT issue

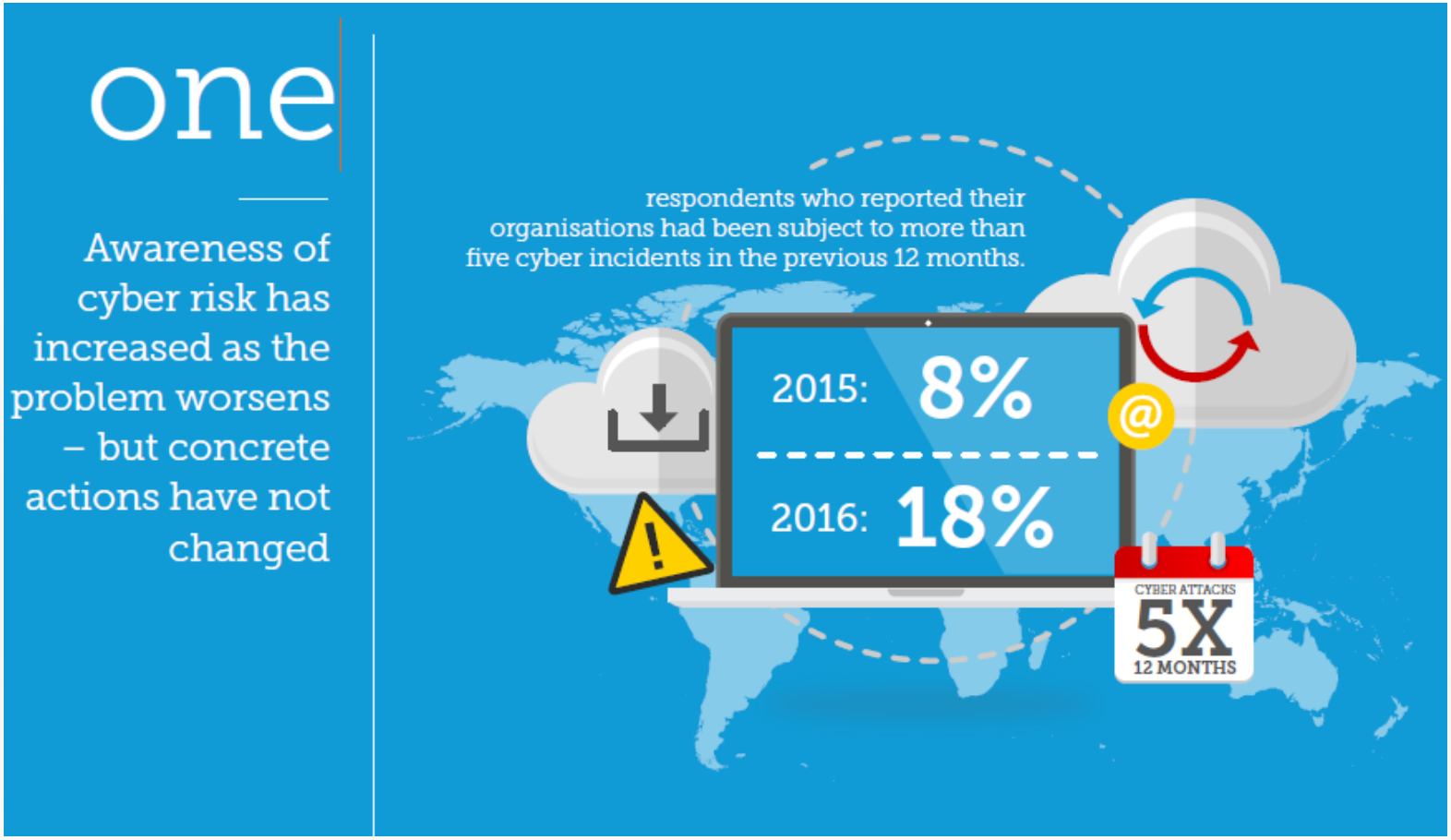
four

The privacy landscape is changing – both in Australia and overseas

five

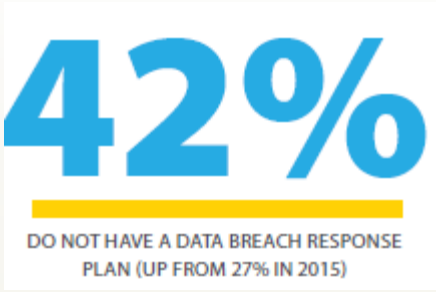
The increasing uptake of cyber insurance indicates some willingness to act on managing cyber risk

Cyber Risk – Increased Incidents



Cyber Risk – Increased Incidents

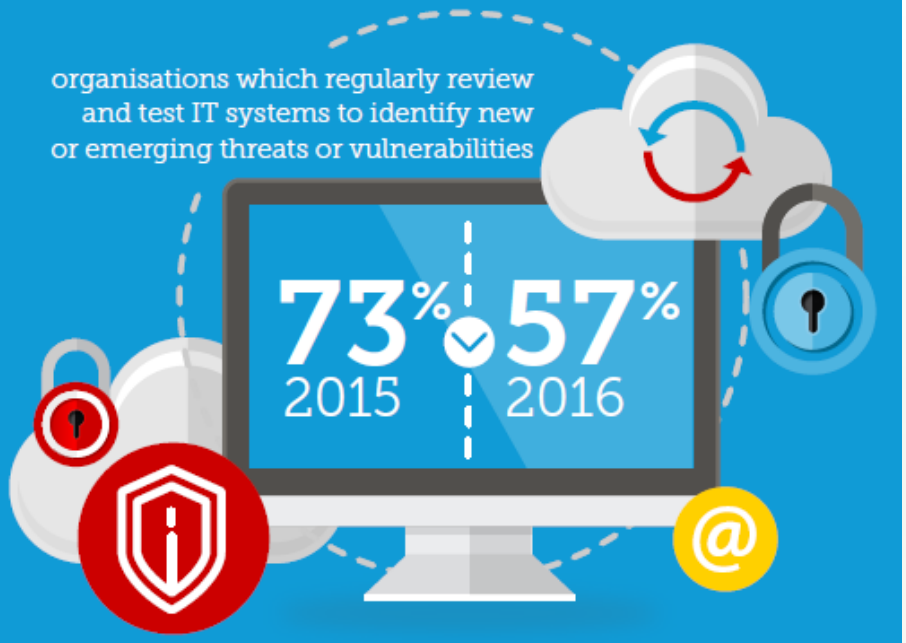
- 2016 saw a year-on-year increase in the number of reported cyber incidents, including many high profile incidents.
- 2016 was also the year of ransomware, with the number of daily ransomware attacks **increasing by 300%** over 2015
- The survey results show that, although organizations are aware of the ever increasing cyber security threat, many are still not taking appropriate steps to properly understand the extent of their exposure, and to implement necessary practical measures to mitigate cyber risk and improve their cyber resilience.



Cyber Risk – Lack of Action

two

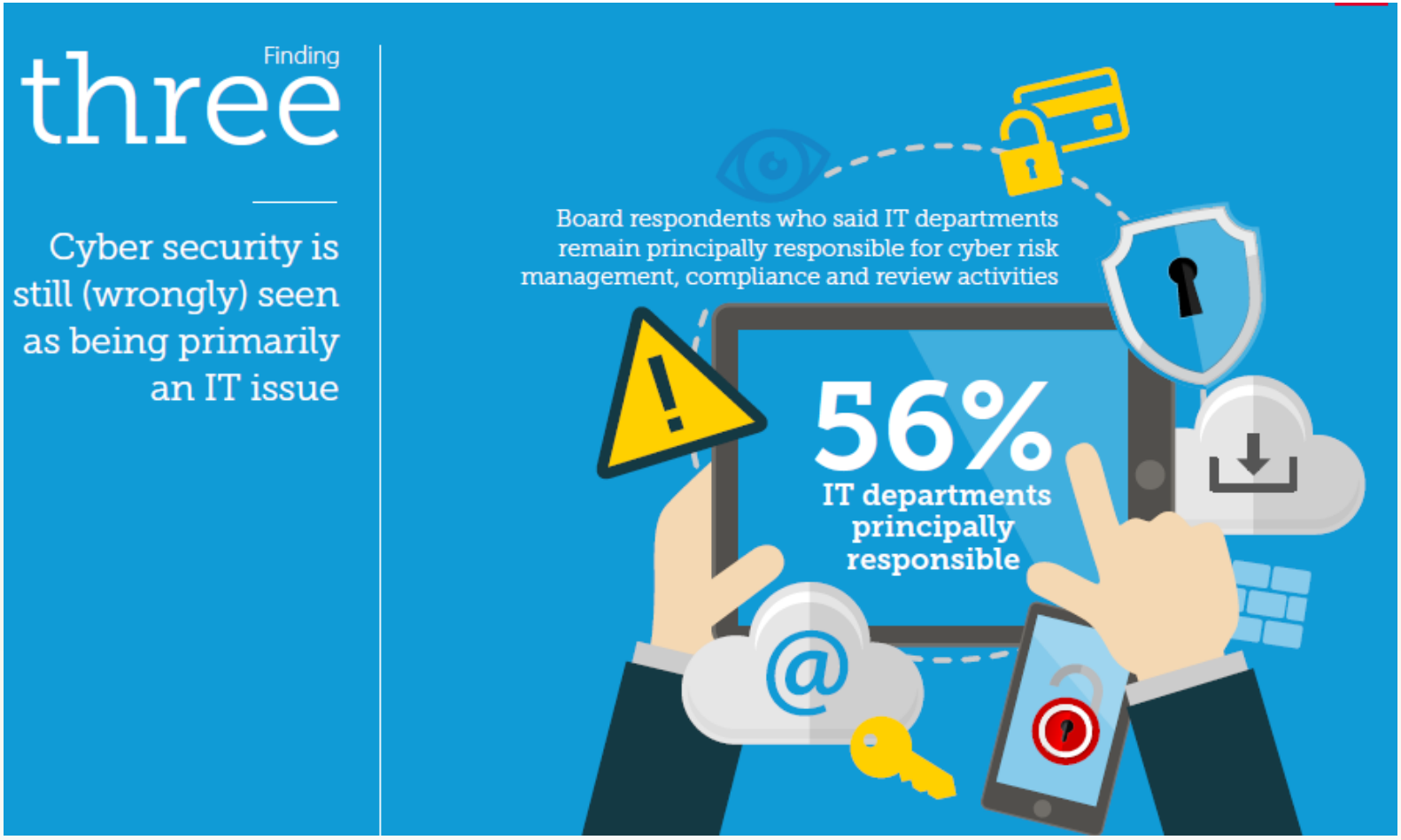
Despite concerns about the increasing cyber threat, organisations remain complacent about reviewing and testing their own cyber resilience (and the cyber resilience of their suppliers)



Cyber Risk – Lack of Action

- Per the survey, only 57% of organizations regularly review and test their key IT systems to identify new or emerging threats or vulnerabilities (down from 73% in 2015).
- At the same time, only 33% of organizations regularly audit their suppliers' IT security practices (largely unchanged from 2015).
- Organizations must improve their own cyber resilience by taking proactive steps to identify and mitigate supply chain risk.

Cyber Risk – Incorrect Focus on IT

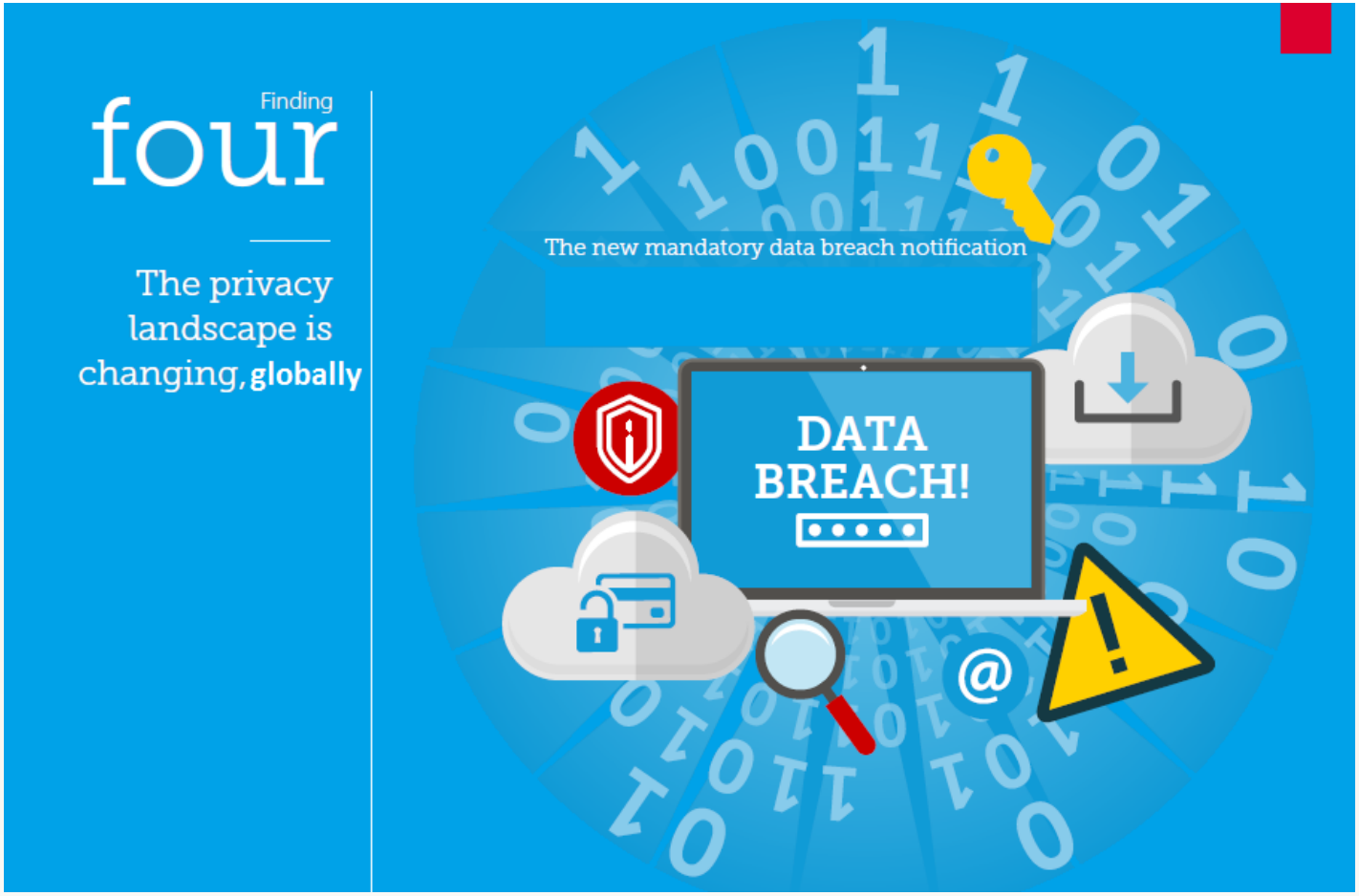


Cyber Risk – Incorrect Focus on IT

- Just over half of the Board survey respondents told us that their IT departments remain principally responsible for cyber risk management, compliance and review activities (largely unchanged from last year).
- About 44% of Board survey respondents told us their Boards are only briefed on cyber security issues annually or on an ad hoc basis
- While 13% told us that their Boards received no briefings at all.
- In addition to the reputational harm to the organization that may result from a cyber incident, there is the potential for substantial legal exposure (including personal liability on the part of directors and employees).

Percentage of Boards briefed annually, on an ad hoc basis or not at all

Cyber Risk – Privacy & Reporting



Cyber Risk – Privacy & Reporting

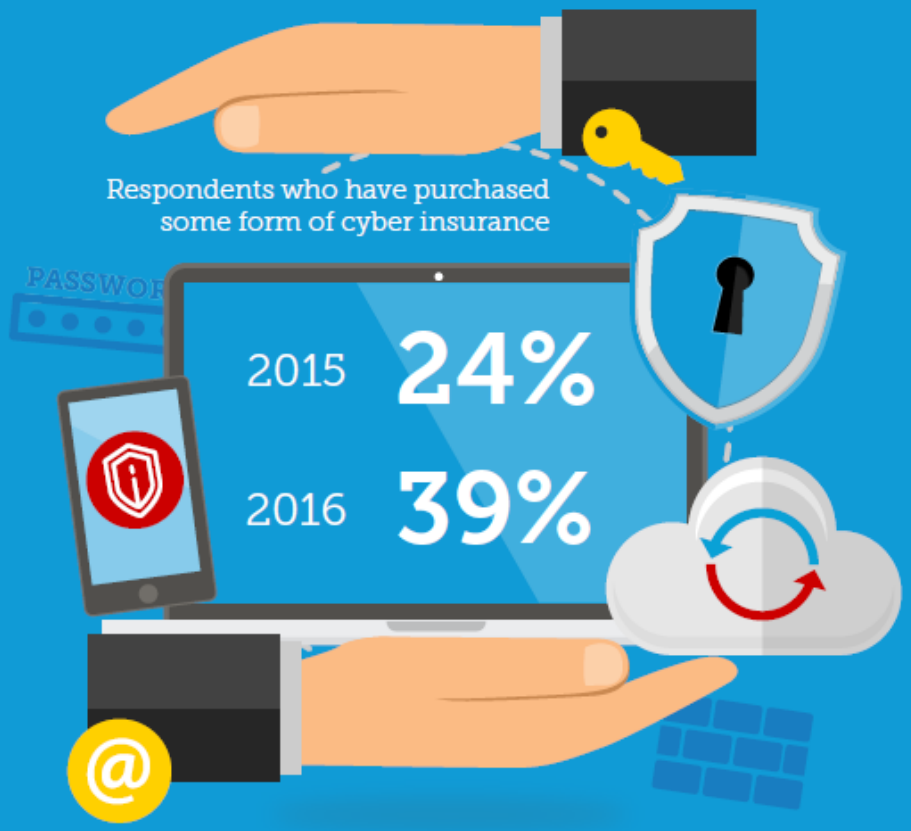
- New changes will impose new obligations on organizations that are subject to the privacy act to:
  - Carry out a reasonable and expeditious assessment if they have *reasonable grounds* to suspect that there may have been an eligible data breach (and to take reasonable steps to complete that assessment within 30 days).
  - Unless an exemption applies, make the prescribed notifications to the applicable regulatory agencies (and, if practicable, to affected individuals) as soon as they are aware that there are reasonable grounds to believe that there has been an eligible data breach.

Cyber Risk – Insurance Considerations

Finding

five

The increasing uptake of cyber insurance indicates some willingness to act on managing cyber risk



Cyber Risk – Insurance Considerations

- Whether the policy provides coverage for the new assessment and notification obligations under the mandatory data breach reporting scheme
- Whether the insurer offers urgent breach coaching or cyber incident response services (providing access for insured organizations to IT professionals, forensic accountants, public relations professionals and lawyers).
- Any limitations on an organization's preferred response to a cyber incident (for example, does the insurer require an insured organization to obtain written permission prior to paying a ransom?).
- The availability of value-add services, such as credit monitoring, to assist organizations in establishing and maintaining goodwill with customers following a data breach

Mitigating your Risks

Corporate / Board Cyber Resilience

- Adopt written cyber security policies, procedures and internal controls, including:
  - Clearly setting out who in management has primary oversight of cyber security issues.
  - Adopting and regularly reviewing the company's data breach response plan.
  - Maintaining a responsive approach to new threats or elevated threats against an agreed risk appetite.
  - Receiving and reviewing regular reports on cyber security incidents.
  - Supporting cyber awareness and training across the organization.

Embedding cyber resilience within an organisation involves more than just keeping the Board regularly informed of cyber risk issues.

Corporate / Board Cyber Resilience

- Appoint a Board member who has cyber security expertise, or alternatively, appoint an independent expert who can present to the Board on cyber security issues.
- Adopting a cyber ‘value-at-risk’ model that not only quantifies cyber risk in financial terms, but enables the Board to formulate strategies and controls in relation to cyber risk, to treat cyber resilience as a potential differentiator, and to track the organization's cyber maturity across time.
- Review annual budgets for IT security and data protection expenditure (including for cyber insurance).

Boards must be cyber risk aware, and there are a number of steps they can take.

Personal Cyber Resilience

- Be aware and understand your personal liability as it relates to handling client or partner confidential and private information
- Take the cyber risk & security training offered by your organization, refresh throughout the year
- *Employees are the last line of defense* and need to become an additional security layer when (not if) attacks make it through all the corporate technical filters.

Password Strategies

What Not To Do

- Do not use these Top 10 most used passwords of 2016::

1.	123456 or any variation of 123…0 or 0987…1	[.25 milliseconds]
2.	qwerty	[.25 milliseconds]
3.	111111	[.25 milliseconds]
4.	1234567890	[.25 milliseconds]
5.	1234567	[.25 milliseconds]
6.	password	[.25 milliseconds]
7.	123123	[.25 milliseconds]
8.	Qwertyuiop	[13 hours, 48 minutes]
9.	Mynoob	[24 seconds]
10.	123321	[.25 milliseconds]

If you are using any of these, change your password(s) immediately as the “black hats” will have access to your valuable information within any where from a fraction of a millisecond to a few hours.

Password Strategies

What Not To Do

- Do not use your network username
- Do not use easily guessed passwords, such as “password” or “user”
- Do not use passwords based on your personal information such as your or a family member’s birthday, anniversary, SIN number, phone number.
- Do not use words that can be found in the dictionary. Password-cracking tools (that are freely available downloads) come with dictionary lists.

Password Strategies

What Not To Do

- Do not use the same password for multiple sites.
- Do not allow your browser to store your passwords.
- NEVER use your email password for any online site or account. If the site gets hacked, someone will be reading your email very soon.
- Do not store your passwords on your computer or phone in plain text.
  - Experts recommend making a list of the applications and websites you visit with your login name. Beside each DO NOT write the password, instead use a clue that has meaning only to you to help you remember the password. If you forget the password, the application administrator or website will email you a temporary password so you can reset it.

Password Strategies

What To Do

- Length is key to higher password security
  - Each character you add to your password makes it an order of magnitude harder for the bad guys to break it.

- Create unique passwords that use a combination including numbers, symbols and words using BOTH upper and lower case letters.

Password Strategies

What To Do

- If you must use a dictionary word as a password then:
  - Change the case of one or more of the letters, and
  - Add both a numeral and a punctuation symbol to it.

- Better: Use an easy to remember phrase combination:
  - E.G. The opening line of your favorite novel:
    - It was the best of times, it was the worst of times (A Tale of Two Cities, Dickens)

- Best: Insert a symbol and number into the phrase

Public Hotspots (Wi-Fi)

A hotspot is a physical location where you can obtain Internet access, typically using **Wi-Fi** technology, via a wireless local area network.

- Examples of public hotspots include:
  - Airports, libraries, coffee shops & restaurants, etc. . ....
- What you do on a public hotspot is open for any snooper to see. If you connect to your bank, unless it is encrypted, what you are typing, username, password, everything, is not just open to be seen using tools such as ***Firesheep***, but it can be hijacked using tools such as ***Wireshark***.
- Do not do anything such as banking, using credit cards , paying bills or accessing sensitive data on a public Hotspot.

Public Hotspots (Wi-Fi)

- To protect yourself on a public hotspot, set your browser to allow access only to secure **HTTPS** websites that will direct to encrypted pages when they are available.

- When connecting to a public hotspot, never select the “Home Network” option. Only select the “Public Network” Wi-Fi option which ensures Windows is not sharing any files or data with other machines on the local network.

- If you need to use public hotspots often, you will want to pay for a VPN (Virtual Private Network) service and browse only through it while on public Wi-Fi.

What are your Options

Call to Action

Start: Cyber Risk Assessment Questions

Q1:

Who is in charge of your cyber security?

Multiple internal stakeholders often share core cyber responsibilities. Are they integrated? Are there gaps?

Q2:

Does everyone know his or her role?

A clear chain-of-command and established roles are critical to an effective cyber security program. Does the left hand know what the right hand is doing?

Q3:

Who conducts risks analysis, when and with what assets or third parties?

It is vital that your company has experts examining its cyber risks and threats and that such analyses are conducted regularly.

Q4:

Are you keeping abreast of the latest threat intelligence?

Cyber threats and vulnerabilities change on a daily basis, and you are expected to monitor both.

Q5:

What's your process for integrating risk analyses, threat assessments and results?

All relevant information must be continually plugged into your cyber security programs.

Q6:

Are you partnering with law enforcement and industry peers?

You can share key information and build relationships with many groups to establish a smooth network in the event of an attack.

Q7:

Do you have response teams inside and outside the company?

Outside vendors often provide fresh eyes and additional, advanced technical support.

Q8:

Are you assuming a breach or other successful attack is inevitable?

If no, why not?
Not acknowledging this inevitability is a recipe for failure.

Q9:

Are you adequately managing third-party risks?

Many cyber attacks originate from third parties, so vendors, contractors and consultants need to be considered in any cyber security plan.

Q10:

What are you doing to manage and minimize your legal risks and exposures?

Many significant cyber security costs result from post-event investigations and litigation.

Thank You

Eric Strong, 4Cast Services Inc.

- www.4castservices.com
- eric.strong@4castservices.com
  - Cell: (416) 846-0122
  - Office: (845) 397-0515
  - Skype: ericrstrong

Peter MacMillan, 4Cast Services Inc.

- www.4castservices.com
- peter.macmillan@4castservices.com
  - Cell: (905) 691-7335
  - Office: (905) 876-3969