EPICC

Cyber Security and Business Continuity Management

October 2016
Cyber security is top of mind for many organizations, and we’re seeing a large number undertaking initiatives to address risk. For some, these initiatives lead to tailor-made processes and controls to address risk.

Meet the team

**Ed Matley**
Director, Risk Assurance

Edward is a Director in PwC’s Risk Assurance practice, based in Vancouver. He leads our Business Resilience practice in Western Canada.

**Marie Lavoie Dufort**
Associate, Risk Assurance

Marie is an Associate in Vancouver’s Risk Assurance practice. She focuses on Business Resilience projects, with a particular focus on crisis management and communication.
Our interpretation of Cybersecurity

**Definition:**

Cyber security is not just about technology and computers. It involves people, information systems, processes, culture and physical surroundings as well as technology.

It aims to create a secure environment where businesses can remain resilient in the event of a cyber breach.
Cybersecurity and IT security are synonymous. They both relate to securing an organization’s IT systems.

True  False
Cybersecurity is achieved by securing digital assets with the use of robust firewalls to prevent potential attacks.

True  False
Cybersecurity is the responsibility of the CIO or Head of IT in an organization.

True  False
Cyber attacks are caused by individual hackers who want to steal valuable information.

True    False
What incidents are we seeing in Vancouver?

E-mail Phishing / Spear Phishing

Email ‘phishing’ attacks regarding payment requests have impacted numerous clients in recent months resulting in millions of dollars of financial fraud.

Malicious Software

Laptops, desktops and handheld devices are being hacked using malicious software resulting in exfiltration of sensitive and confidential corporate documents / intellectual property.

Internal Attacks

Disgruntled employees sabotaging information systems impacting the company’s business operations.
Recent global incidents

Russians behind JPMorgan Cyber attack: ‘It scared the pants off many people’
Washington Times, October 2014

JPMorgan cyberattack largest ever bank hack

JP Morgan = about 76 million households affected
Home Depot = about 56 million customer debit and credit card info compromised
Ebay = 233 million user information is compromised
### Organizations today face four main types of cyber adversaries

<table>
<thead>
<tr>
<th>Adversary</th>
<th>Motives</th>
<th>Targets</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation State</td>
<td>• Economic, political, and/or military advantage</td>
<td>• Trade secrets</td>
<td>• Loss of competitive advantage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sensitive business information</td>
<td>• Regulatory inquiry/penalty</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• M&amp;A information</td>
<td>• Disruption to critical infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Critical financial systems</td>
<td></td>
</tr>
<tr>
<td>Organized Crime</td>
<td>• Immediate financial gain</td>
<td>• Financial / payment systems</td>
<td>• Regulator inquiry/penalty</td>
</tr>
<tr>
<td></td>
<td>• Collect information for future financial gains</td>
<td>• Personally identifiable information</td>
<td>• Consumer and shareholder lawsuits</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Payment card information</td>
<td>• Brand and reputation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Protected health information</td>
<td>• Loss of consumer confidence</td>
</tr>
<tr>
<td>Hacktivists</td>
<td>• Influence political and/or social change</td>
<td>• Corporate secrets</td>
<td>• Disruption of business activities</td>
</tr>
<tr>
<td></td>
<td>• Pressure business to change their practices</td>
<td>• Sensitive business information</td>
<td>• Brand and reputation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Critical financial systems</td>
<td>• Loss of consumer confidence</td>
</tr>
<tr>
<td>Insiders</td>
<td>• Personal advantage, monetary gain</td>
<td>• Sales, deals, market strategies</td>
<td>• Trade secret disclosure</td>
</tr>
<tr>
<td></td>
<td>• Professional gain</td>
<td>• Corporate secrets</td>
<td>• Operational disruption</td>
</tr>
<tr>
<td></td>
<td>• Patriotism</td>
<td>• Business operations</td>
<td>• Brand and reputation</td>
</tr>
<tr>
<td></td>
<td>• Bribery or coercion</td>
<td>• Personnel information</td>
<td>• Loss of consumer confidence</td>
</tr>
</tbody>
</table>

Respondents
• 51% C-suite level
• 15% Director level
• 34% Other (e.g. Manager, Analyst, etc.)
• 39% Business and 61% IT (18% increase compared to 2014)

Industries represented
Top 5
• 22% Technology
• 10% Financial Services
• 8% Consulting/Prof. Services
• 7% Engineering/Construction
• 7% Consumer Products & Retail

Reported annual revenues
• 34% at least US$1B
• 48% US$25 to $999M
• 26% less than US$100M
• 3% non-profit

2016 Canadian insights at a glance

- **160% increase in detected incidents** in Canada (over 2014)
- Incidents attributed to **foreign nation-states** increased the most (up 67% over 2014) while **employees** continue to be the most cited **source of incidents** (66%)
- **Customer records** continue to be the most targeted data (36%)
- **Attacks on IoT devices and systems** are on the rise
- **Security spending** increased by 82% over 2014, currently at 5% of IT spend
- Average **financial loss** due to detected incidents is $1M (18% decrease from 2014)

65% 58%
Have an overall information security strategy

57% 53%
Employee training and awareness programs

55% 52%
Have security baselines / standards for third parties

50% 54%
Have a CISO in charge of security

50% 49%
Conduct threat assessments

54% 48%
Active monitoring analysis of security intelligence
Risk-based frameworks can help organizations design, measure and monitor progress towards an improved cyber program.

<table>
<thead>
<tr>
<th>Framework</th>
<th>Canada</th>
<th>World</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST Cybersecurity Framework</td>
<td>41%</td>
<td>35%</td>
</tr>
<tr>
<td>ISO27001</td>
<td>29%</td>
<td>40%</td>
</tr>
<tr>
<td>SANS Critical Controls</td>
<td>24%</td>
<td>28%</td>
</tr>
<tr>
<td>ISF Standard of Good Practice</td>
<td>22%</td>
<td>26%</td>
</tr>
<tr>
<td>Other</td>
<td>17%</td>
<td>18%</td>
</tr>
<tr>
<td>None</td>
<td>8%</td>
<td>8%</td>
</tr>
<tr>
<td>Do not know</td>
<td>13%</td>
<td>11%</td>
</tr>
</tbody>
</table>
Risk-based frameworks can help organizations design, measure and monitor progress towards an improved cyber program

NIST Cybersecurity Framework

A voluntary framework – based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure.

ISO 27001

The ISO 27000 family of standards helps organizations keep information assets secure.

SANS Critical Controls

The CIS Critical Security Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. A principle benefit of the Controls is that they prioritize and focus a smaller number of actions with high pay-off results.

ISF Standard of Good Practice

The ISF Standard of Good Practice for Information Security is the most comprehensive information security standard in the world, providing more coverage of topics than ISO...
Risk-based frameworks and controls

NIST Cybersecurity Framework
- Response plans (Incident Response and Business Continuity)
- Recovery plans (Incident Recovery and Disaster Recovery)
- Risk Assessment

SANS Critical Controls
- Incident response and management

ISO 27001
- Information security aspects of business continuity management
- Information security continuity

ISF Standard of Good Practice
- Business continuity strategy
- Business Continuity Program
- Resilience
- Crisis Management
- Business Continuity Planning
- Business Continuity Arrangements
- Business Continuity Testing
Integrating Cybersecurity and BCM
What is BCM?

A holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.
The Business Continuity Management Lifecycle

Shows the stages of activity that an organization moves through and repeats with the overall aim of improving organizational resilience.
Current developments in BCM

WEF Global Risk Report respondents were asked to select the three global risks that they believe are the most likely to occur in North America.

Cyber attacks are top of mind.
Current developments in BCM

Investment in Business Continuity

51% of organizations claim using ISO 22301 as a framework for business continuity management

Highest uptake of ISO 22301 seen in:
- IT/telecommunications: 66%
- Professional services: 56%
- Financial: 53%

Top 5 Trends and Uncertainties

1st Use of Internet for malicious attacks
2nd Influence of social media
3rd Loss of key employee
4th New regulations & increased regulatory scrutiny
5th Prevalence & high adoption of internet-dependent services
Pros and cons

+ Clarity
+ Efficiency
+ Risk Management

- Level of detail
- Organizational silos
Analysis

Objective:

1. Business impact analysis
   Identify & prioritize most time sensitive business activities

2. Continuity requirements
   What resources does our organization need

3. Risk assessment
   Limit the impact of disruptions on an organizations key services
Analysis

Integrating cybersecurity and BCM

Analysis

1. Identification of, “crown jewels,” information assets
2. Engaging IT resources early
3. Performing an explicit cyber risk assessment
4. Identification of operational controls gaps
**Design**

**Objective:**
Identifies and selects appropriate tactics to determine how continuity and recovery from disruptions will be achieved.
Design

Integrating cybersecurity and BCM

1. Design
   - Is the BCP program team a cyber security threat?
   - Are appropriate security resources included in the BCP program?
   - Is there appropriate physical security for facilities and logical security over data?
   - Consider security in IT recovery strategy selection
   - Cyber considerations for third party selection
   - Integration of incident management team / escalation
Implementation

Objective:
Executes the agreed strategies and tactics through the process of developing the Business Continuity Plan.
Implementation
Integrating cybersecurity and BCM

1. Implementation
- Do you need more than one incident management process?
- Consider controls required to protect Personally Identifiable Information (PII)
- Consider requirements to control where/how information is posted during a crisis
- Ensure that leadership and IT response teams have regular touchpoints
- Ensure that crisis communications for cyber incidents is aligned with the overall program
- Recording activities
Validation

Objective:
Confirms that the BCM programme meets the objectives set in the BC policy and that the organization’s BCP is fit for purpose.
Validation

Integrating cybersecurity and BCM

1. Validation
   - Use cybersecurity incident as an exercise scenario
   - Integrate audit / reviews / post incident reviews
   - Consider impact on maintenance update frequency
Policy and programme management

Objective:

Is the start of BCM lifecycle. It is the professional practice that defines the organizational policy relating to BC and how that policy will be implemented, controlled, and validated through a BCM programme.
Policy and programme management

Integrating cybersecurity and BCM

Policy and programme management

- Policy alignment
- Integration
- Use of cyber resources on program team
Embedding business continuity

Objective:
Ongoing activity resulting from the BCM policy and programme management stage of the BCM lifecycle. It seeks to integrate BC into day-to-day business activities and organizational culture.
Embedding business continuity
Integrating cybersecurity and BCM

Embedding Business Continuity

• Senior management posture
• Awareness bang for your buck
• Develop organisation’s, “intuition.”
Questions?
Thank you!

Marie Lavoie Dufort
Associate, Risk Assurance Services
Tel: 604 806 4195
Marie.Lavoie.dufort@ca.pwc.com

Edward Matley
Director, Risk Assurance Services
Tel: 604 806 7634
Email: edward.matley@ca.pwc.com

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2014 PricewaterhouseCoopers LLP. All rights reserved. In this document, “PwC” refers to PricewaterhouseCoopers LLP which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.