www.pwc.com/ca

# *EPICC*

# *Cyber Security and Business Continuity Management*

October 2016

pwc

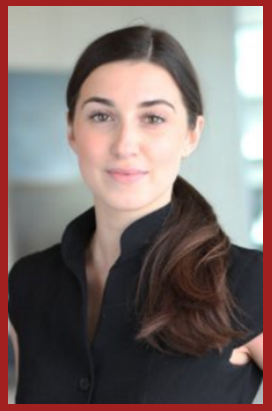
# *Meet the team*

*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.*

## *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*

*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*

**JPMorgan cyberattack largest ever bank hack**




**Chinese cyberattack forces computer shutdown at National Research Council**


CTV News Channel: NRC issues warning

Mercedes Stephenson says we may

CANADA

TRENDING Ferguson | Quinn | Cosby | NHL | Ghomeshi | Ottawa | Rosetta | Magnotta | ISIS | Ford

Toronto police website shut down in string of cyber attacks across Canada

# *Organizations today face four main types of cyber adversaries*

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

# *The Global State of Information Security® Survey 2016*

**10,000**

**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)

**17**

**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

# *The Global State of Information Security® Survey 2016*

## 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%**)

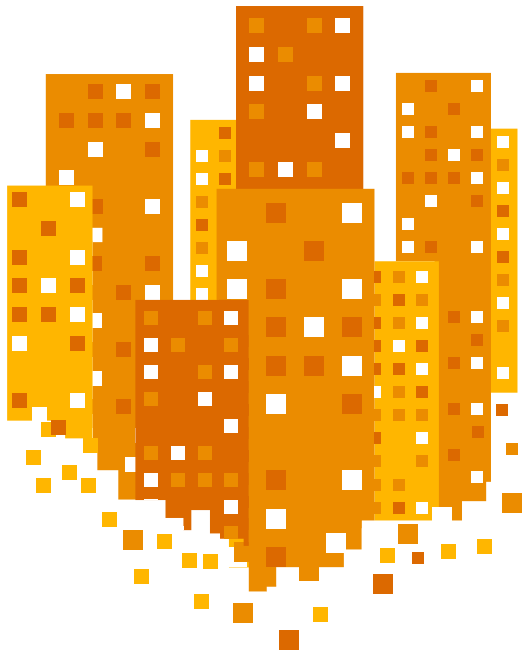
**Customer records** continue to be the most targeted data (**36%**)

**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)

# *The Global State of Information Security® Survey 2016*



**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*

| | | |
|---|---|---|
| NIST Cybersecurity Framework | 41% | 35% |
| ISO27001 | 29% | 40% |
| SANS Critical Controls | 24% | 28% |
| ISF Standard of Good Practice | 22% | 26% |
| Other | 17% | 18% |
| None | 8% | 8% |
| Do not know | 13% | 11% |

# *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 wit 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

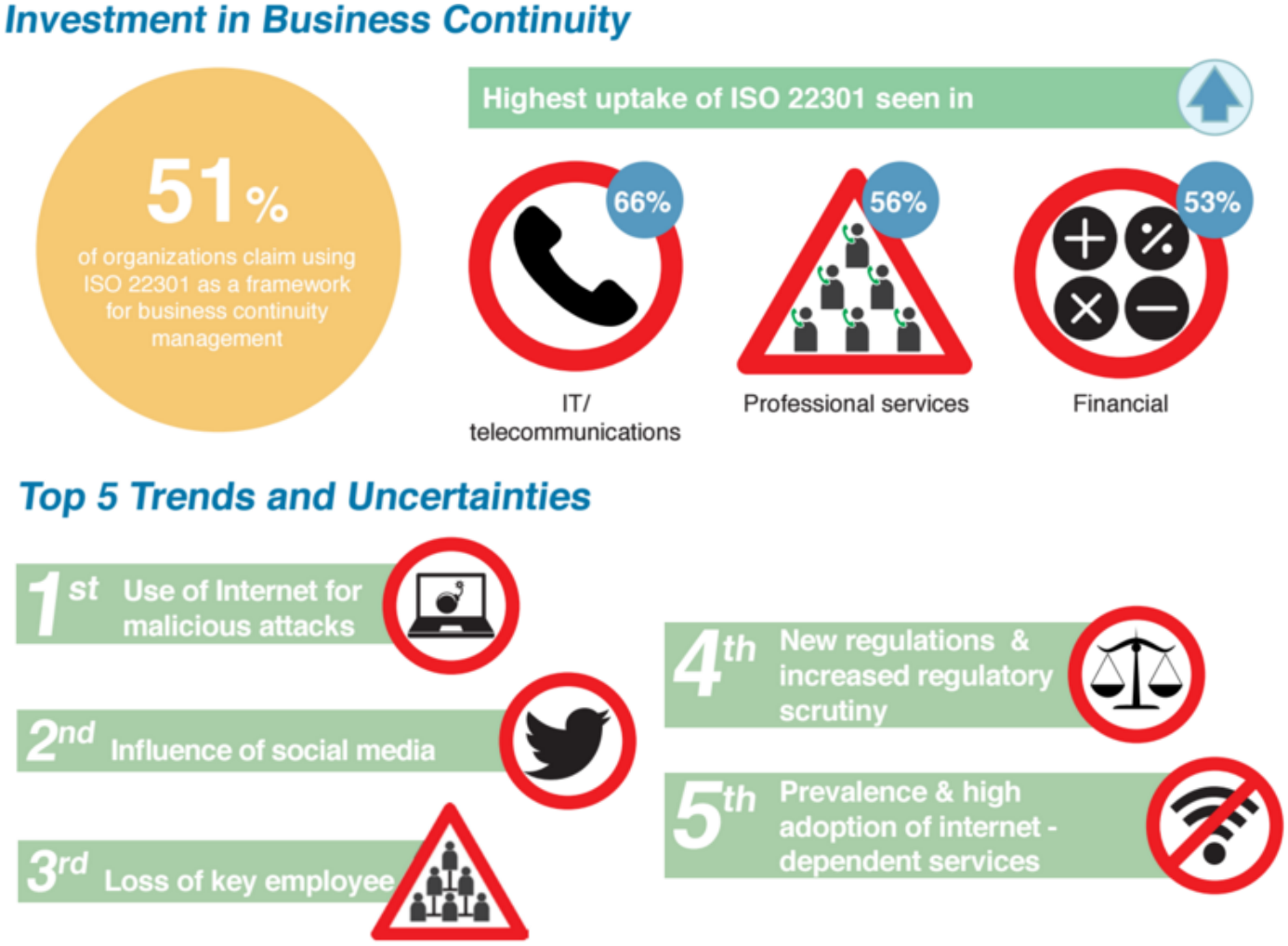
***Improving organizational resilience***

# *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

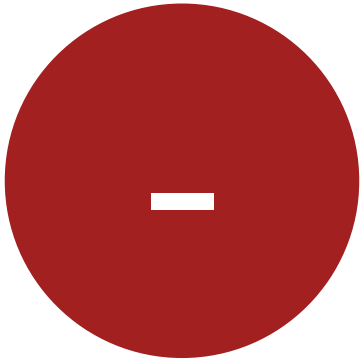
**Cyber attacks are top of mind**

# *Current developments in BCM*



# *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*

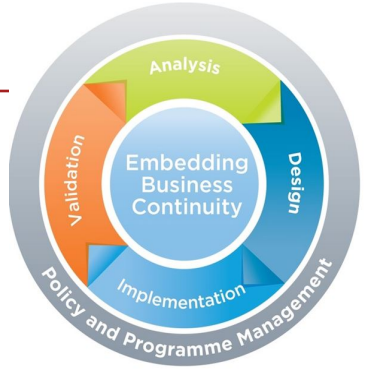
*Integrating cybersecurity and BCM*


1

## Analysis

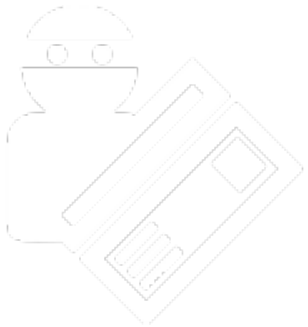
- Identification of, “crown jewels,” information assets
- Engaging IT resources early
- Performing an explicit cyber risk assessment
- Identification of operational controls gaps

# *Design*



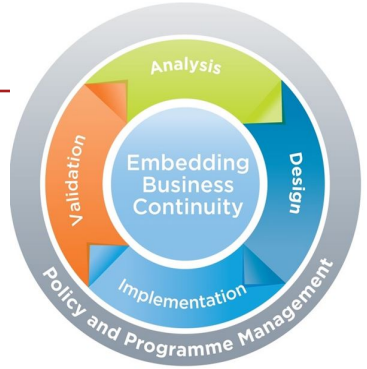

**Objective:**

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



# *Design*

*Integrating cybersecurity and BCM*



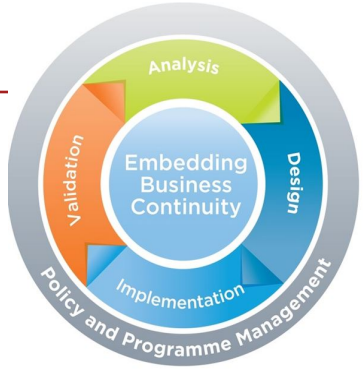

1

## 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*

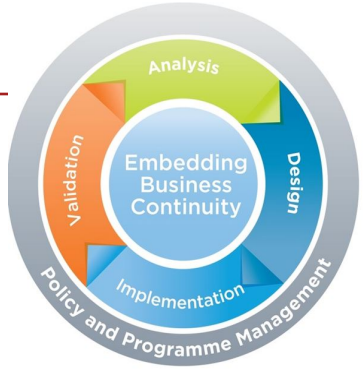



## Objective:

Executes the agreed strategies and tactics through the process of developing the Business Continuity Plan.

# *Implementation*

*Integrating cybersecurity and BCM*

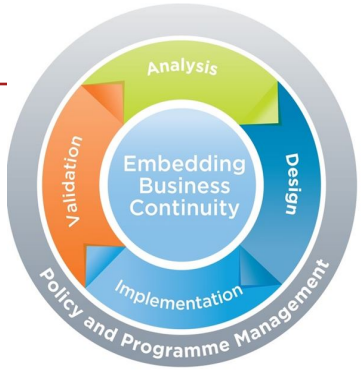



1

## 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*

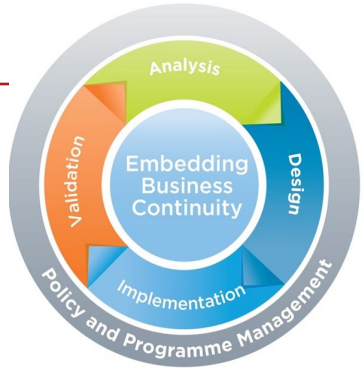
*Integrating cybersecurity and BCM*


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*


1

## 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*


1

## 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