KPMG

cutting through complexity

Risk & Regulatory Series

The New World of Cyber Resiliency

Presenter – Paul Hanley

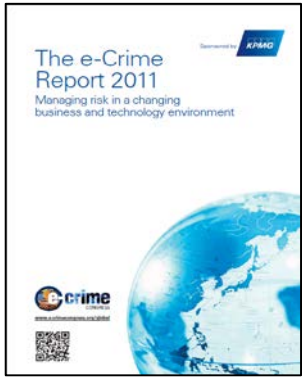
Paul Hanley

Partner, Risk Consulting IT Advisory

Cyber Security Lead Partner, Canada

KPMG Canada
Bay Adelaide Centre
333 Bay Street Suite 4600
Toronto, ON

Industry contributions:



Presenter – Kevvie Fowler

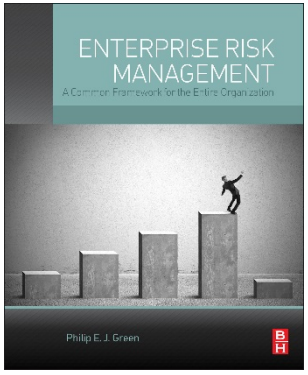
Kevvie Fowler

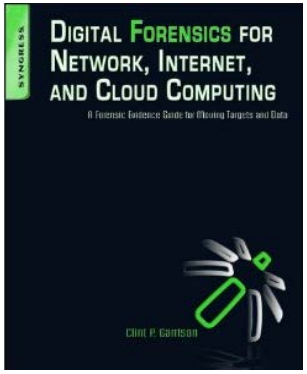
Partner, Risk Consulting

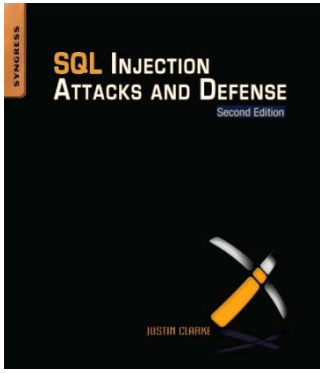
Cyber Forensics Lead Partner, Canada

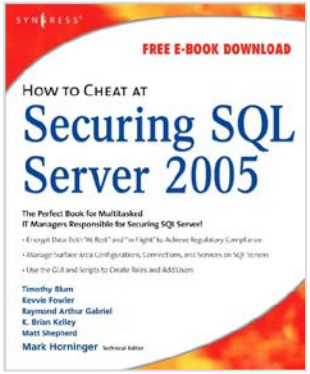
KPMG Canada
Bay Adelaide Centre
333 Bay Street Suite 4600
Toronto, ON

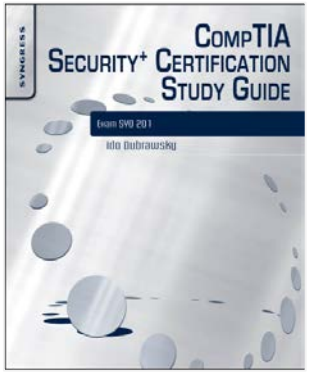
Industry contributions:











Agenda:

1 Cyber security

2 How to get it right

3 Board involvement

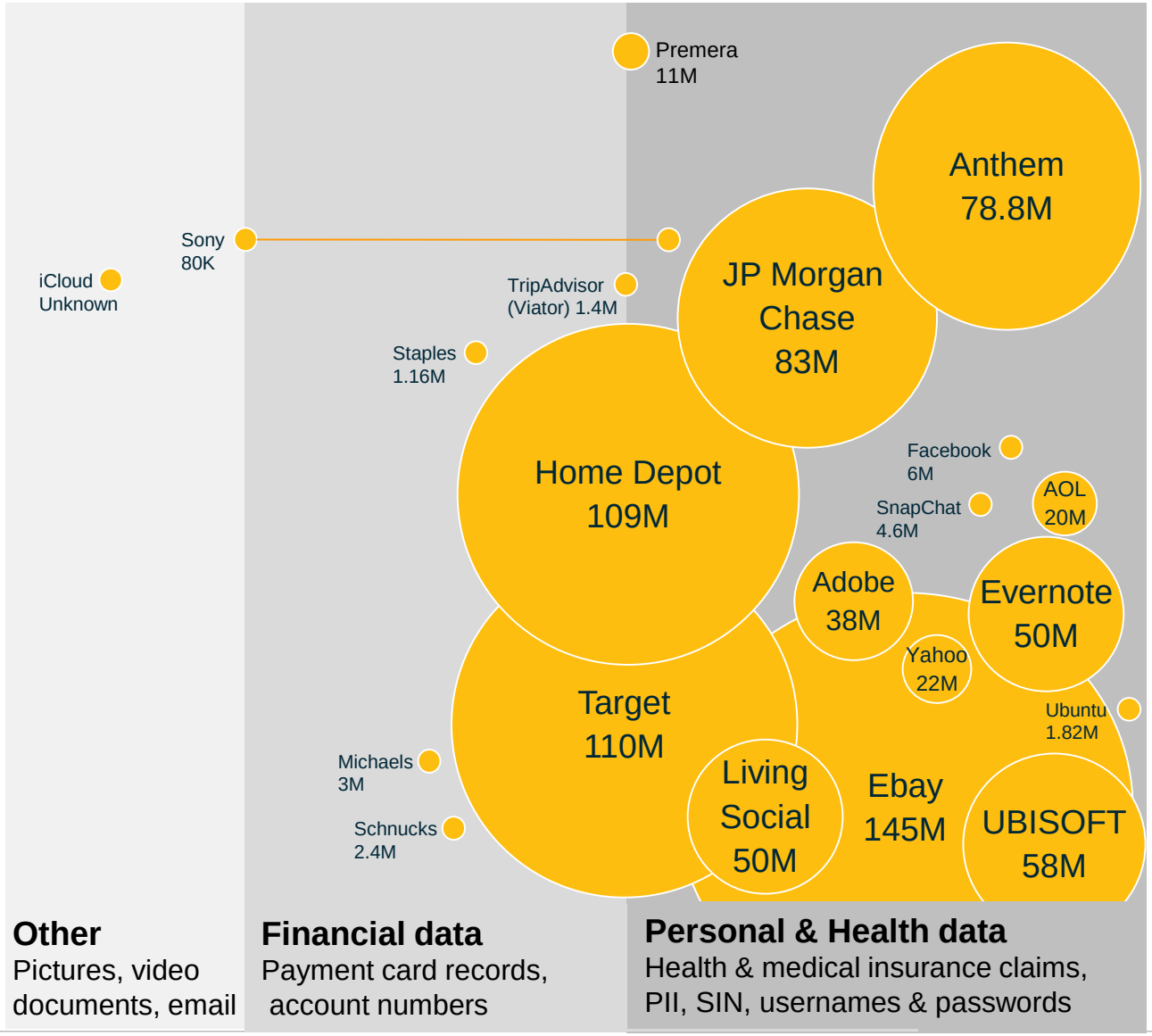
4 Cyber forensics

5 Questions & Answers

6 Who to contact

1.1 Cyber security | Key trends

1.2 Cyber security | The breach landscape



Top data breaches 2013 – Present

The number of breached records per recognized company by data type (>1M records)

Price of goods for sale in the underground economy (USD)

- **Username and passwords**
  $5.60 per record
- **Health/medical records**
  $47.62 per record
- **Social media accounts**
  $.05 - $8.00 per account

References:
-http://blogs.wsj.com/corporate-intelligence/2014/03/28/whats-more-valuable-a-stolen-twitter-account-or-a-stolen-credit-card/

http://blogs.wsj.com/riskandcompliance/2013/06/26/passwords-more-valuable-than-credit-card-data/

http://www.foxbusiness.com/technology/2014/01/15/e-bazaar-crooks-hawk-your-info-in-online-black-market/

1.3 Cyber security | The cyber criminals

Petty Criminals / Motives: Financial gain

Hacktivists / Motives: Political support

Organized / Motives: Financial gain

State / Motives: State agenda

2.1 Why do organizations get it wrong? | Themes 1

Common Themes of Organizations that Got it Wrong:

Security strategy:

- The security function operates independently of the business. The security function is non-collaborative and makes security appear as a dark art. No clearly defined and agreed RACI.

Security Fundamentals:

- Failing to build in security fundamentals, comprehensive security testing, and asset management creates a weak foundation. Security is additive so new challenges must be combined to existing challenges. A breach through not applying patches in a timely manner is unacceptable (but still quite common).

Threat intelligence:

- Not keeping up-to-date with the latest Cyber security threats and evolving your security approach around them. A lack of formal and informal threat intelligence means that you don't have the most relevant information on which to make informed decisions.

Global compliance:

- Not considering global security compliance and regulation, even if you don't operate globally. Not meeting security compliance requirements can lead to significant financial penalties including fines, potentially 5% of global revenues, or even custodial sentences. Being reactive to security compliance requirements is always a mistake.

2.2 Why do organizations get it wrong? | Themes 2

Common Themes of Organizations that Got it Wrong:

Third party due diligence:

- Many successful Cyber attacks occur through compromising the security of a third party supplier. A contract with the supplier to prevent or disclose breaches is not sufficient. Weaker organizations do not have an ongoing supplier assurance process.

Only considering prevention:

- The world has changed and the prevention of security incidents is no longer enough. Detection of security incidents and the appropriate reaction to security incidents are also key.

Failing to react correctly:

- Reacting incorrectly after a breach can significantly increase the severity of the breach and brand damage. It can also increase the likelihood of fines, as well as making you be seen as a softer target, increasing the likelihood of a further breach.

Security is seen as a tick-box exercise:

- Basic security will at best thwart the basic attacker. Many organizations that have been breached, approached security as a checklist they needed to complete, rather than linking good security to the specific risks and threats of the business.

3.1 How to get it right | Step 1: Build a Cyber Defensible Position

How to get security right:

- Build a Cyber Defensible Position helps you say:
  - We followed best security practice (NIST, ISF, OSFI, ISO27001)
  - We used external consultancies to help improve our security
  - We regularly reviewed our risks, keeping up-to-date with the latest threats and vulnerabilities
  - We had strong technical controls
  - We had good patching
  - We had good security awareness
  - We conducted Cyber breach simulation exercises
  - We dealt with the incident in a timely and forensically sound manner
  - We followed good practice for the prevention, detection and reaction to security incidents

- The result:
  - A reduction in the likelihood of fines from regulators or Government bodies
  - A reduction in the backlash from customers who may otherwise take their business elsewhere
  - A reduction in the impact to share-price and the reaction to this from shareholders
  - Less attention paid to your breach by the media
  - Overall protection of your brand

3.2 How to get it right | Obtaining your Cyber Defensible Position

Finding and maintaining your Cyber defensible position:

- Link the three most frequently asked board questions on Cyber security to the organizations maturity for Preventing, Detecting & Reacting to Cyber Security incidents:

Board Questions:	Input:	Phase:	Defensible Position Status:	Typical action:
1. Where are we regarding Cyber Security?	• Identify business specific Cyber risks & threats • Identify compliance requirements (legal & regulatory) • Identify 'Crown Jewel' data	ASSESSMENT	None	• Cyber Maturity Assessment/ Cyber Security review • Vulnerability assessment • Red teaming
2. Where do we want to be regarding Cyber Security?	• Complete a business impact assessment • Complete a gap assessment	GAP ANALYSIS & FACILITATED DISCUSSION	Defined	• Facilitated discussion to consciously accept or remediate risks
3. How do we get there?	• Sign off budget • Decide on metrics to track progress (KPIs)	CYBER SECURITY STRATEGY & TRANSFORMATION PROGRAM	Plan Created	• Cyber security Strategy & Transformation Plan
EXECUTE & VERIFY PROGRESS (ONGOING)			Achieved	• Delivery of security programs & ongoing assessments

3.3 How to get it right | Think Holistically

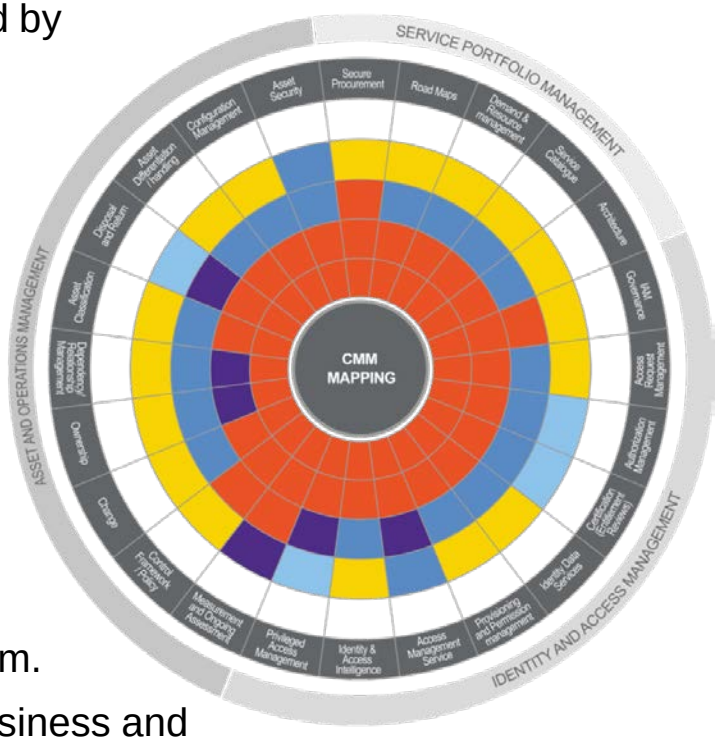
Cyber security is a business challenge:

- Embed good security practice across the business

3.4 How to get it right | Security governance

Understanding the best approach for security governance in an organization can be a challenge:

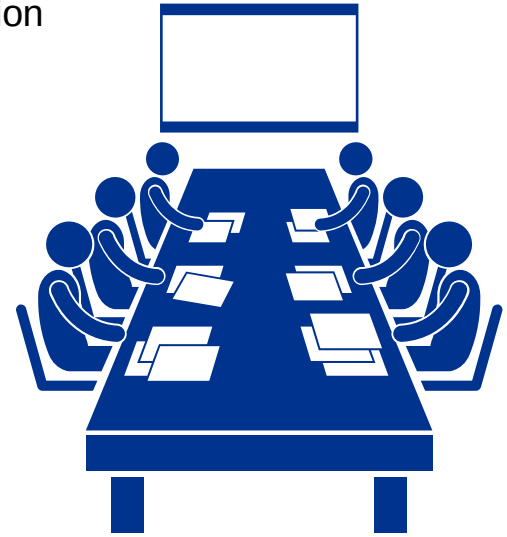
- A new security regime will only be successful when supported by efficient security governance.
- Ensure that security is at the right level (including the board).
- Identify the security operating model (centralised, decentralised, hybrid).
- Create and agree on a security RACI and keep it up-to-date (role changes, businesses merge, JV's, etc.)
- Be clear on your current level of security risk.
- Identify your defensible position (CMM's can help).
- Make sure the security function is aligned to the needs of the business.
- Identify your security resourcing challenges and deal with them.
- Ensure that security is seen as an enabling function of the business and that it is engaged with on day one.
- Like the rest of the business, the security organization will need to remain flexible and adapt over time.



3.5 How to get it right | Expectations of the Board in Cyber Security

The Role of the Board is Critical to Effective Cyber Security:

- Obtain and agree answers to the three fundamental questions regarding Cyber security:
  1. Where are we?
  2. Where do we want to be (your defensible position)?
  3. How do we get there?
- This should not be a debate about Cyber security, but a business-led discussion about protecting corporate value
- Understand the value of your various data sets, and whether appropriate resources are devoted to classifying and securing the most critical assets
- Ensure Cyber security is a regular topic and break it into three: items for *Information*, items for *Action*, items for *Decision*
- Ensure you get the right management information and metrics on the status of security on a regular basis
- Request regular Cyber incident reports to monitor Cyber attacks and trends
- Ensure all board members are aware that they are one of the biggest risks
- Be an active participant in your company's cyber-incident response plan
- Conduct periodic Cyber risk assessments and consider the need for an independent risk assessment – use it to identify where to invest
- Finally if a Cyber risk is raised to you, either mitigate it or risk accept it; do not ignore it.



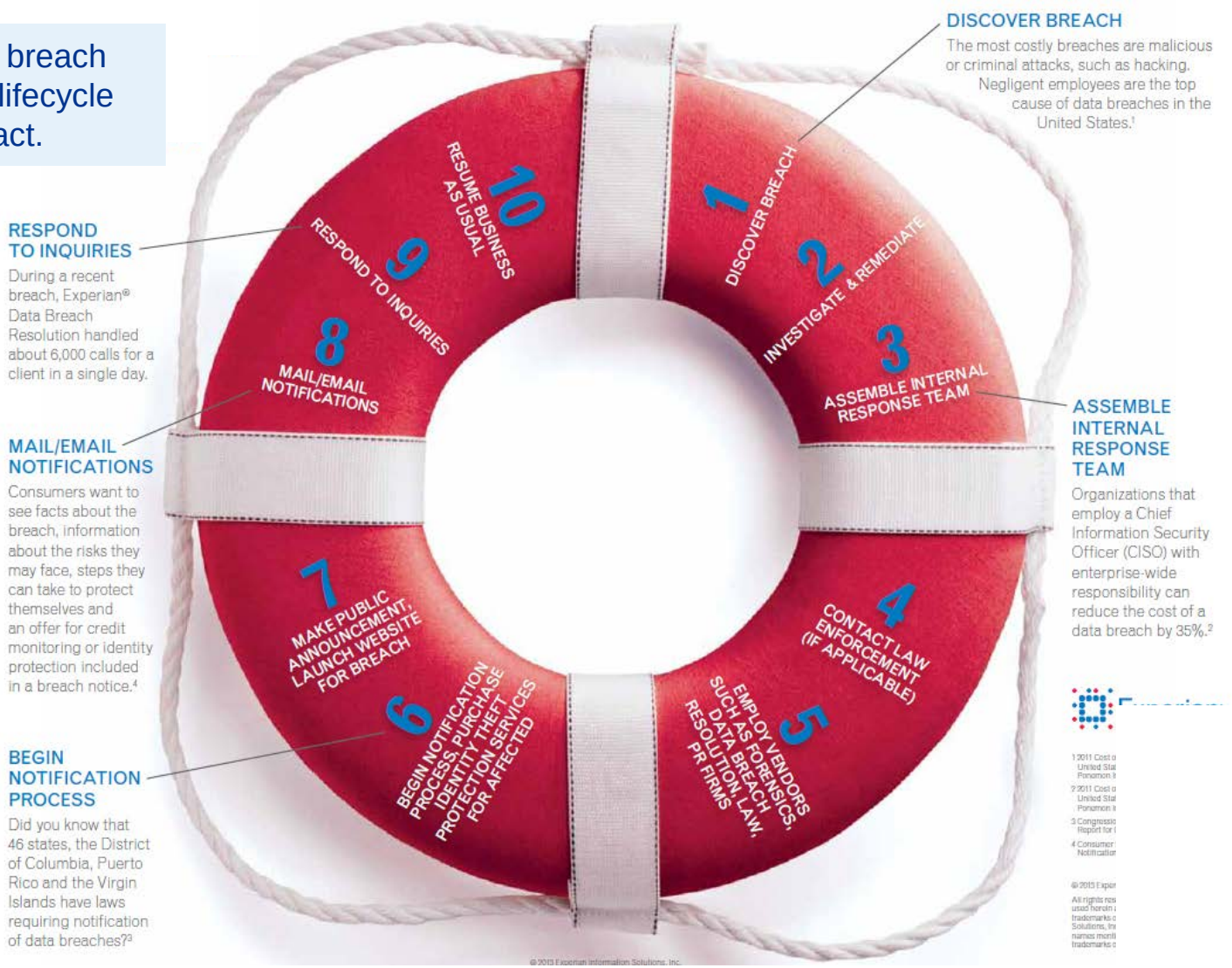
3.6 How to get it right | Other points

Build in the right practices:

- Be secure-by-design
- Consider prevention, detection and reaction
- Help ensure effective, ongoing supplier assurance
- Implement both formal and informal Cyber intelligence, including I-4 and other collaboration groups
- Help ensure your Cyber security approach is sustainable and adaptable
- Help ensure that there is commitment from the top for an effective security culture and that this message is cascaded to all employees
- Consider the latest security techniques to combat the latest security threats:
  - Red Team security testing
  - Targeted attack reviews

4.1 Cyber forensics | Life cycle of a breach

Effectively managing a breach throughout the breach lifecycle will reduce overall impact.



Source: http://www.experian.com/assets/data-breach/brochures/response-guide.pdf

4.2 Cyber security | proactively preparing for reaction

3 steps to revitalize your cyber incident response process

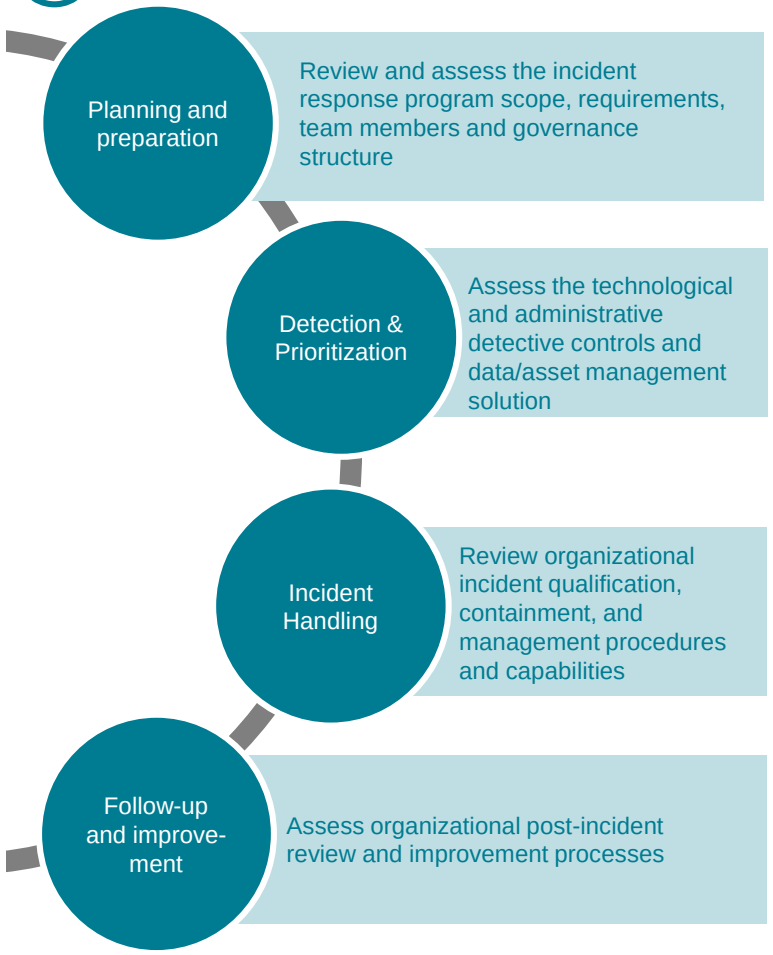
1 Define data assets

Define what is important to your organization and the hackers.

2 Identify cyber threats

Identify likely threats and associated impact to your organization.

3 Assess detection & response capabilities



5.1 Cyber Security Foresight | What we believe is coming

Foresight of Predictions:

- Crypto/Ransomware will continue to adapt and transform whilst new competitive variants will emerge during 2015. It is likely that there will be an increase in nano-ransoms, whereby a hacker will demand $1 for unlocking mobile devices.
- Targeted, content-based infections will continue to rise, with malware targeting shoppers of enterprise services and software with bespoke attacks, such as those wishing to purchase security tools.
- As the cost of stolen Credit Card and email credentials continue to fall due to the volume of information available for sale on the Darknet, hackers will be forced into more provocative crimes, including DDoS.
- DDoS attacks will increase in frequency, potency and sophistication: they could target telephony services, or could be combined with a DDoS mitigation tool zero-day exploit.
- As security compliance requirements increase, we will see many companies working hard to comply with specific compliance requirements, such as the “Right to be forgotten”. Those that fall fowl will be given significant fines as a warning to others.
- Cyber extortionists will continue to thrive. Terrorists are now involved in this market, as so many companies simply pay up.
- There is likely to be an increase in Crime as a Service (CaaS). With the increasing use of smart devices, enhanced capabilities and power of the devices and bandwidth to access data, smart devices will be used even more as part of CaaS attacks. Applications allowing hackers to attack organizations via an icon on their smart phone will be developed, and could be used by anyone, anywhere in the world, at any time.
- A coordinated cross industry attack will occur: FS organizations, Telco, Oil & Gas, Transport.

5.2 Cyber Security Foresight | What we believe is coming

Foresight of Predictions (continued):

- Fraudsters will increasingly target business customers rather than personal accounts due to the prospect of a potentially higher return.
- Nation State-sponsored attacks will increasingly extend from espionage to sabotage.
- More advanced, stealthy and widespread targeted attacks will occur (such as a Carbanak 2).

Other Presentations

The other presentations that were presented as part of the Risk and Regulatory series are:

- IFRS 9 Classification, Measurement and Impairment (Insurance Sector): Initial Considerations
- Market Conduct
- ORSA – Next Steps
- Regulatory Compliance Management

Presenters

Paul Hanley
Partner, Risk Consulting - IT Advisory
National Leader, Cyber Security
KPMG LLP
416 777 8501
pwhanley@kpmg.ca

Kevvie Fowler
Partner, Risk Consulting - Forensic
National Leader, Cyber Forensics
KPMG LLP
416 777 3742
kevviefowler@kpmg.ca

cutting through complexity