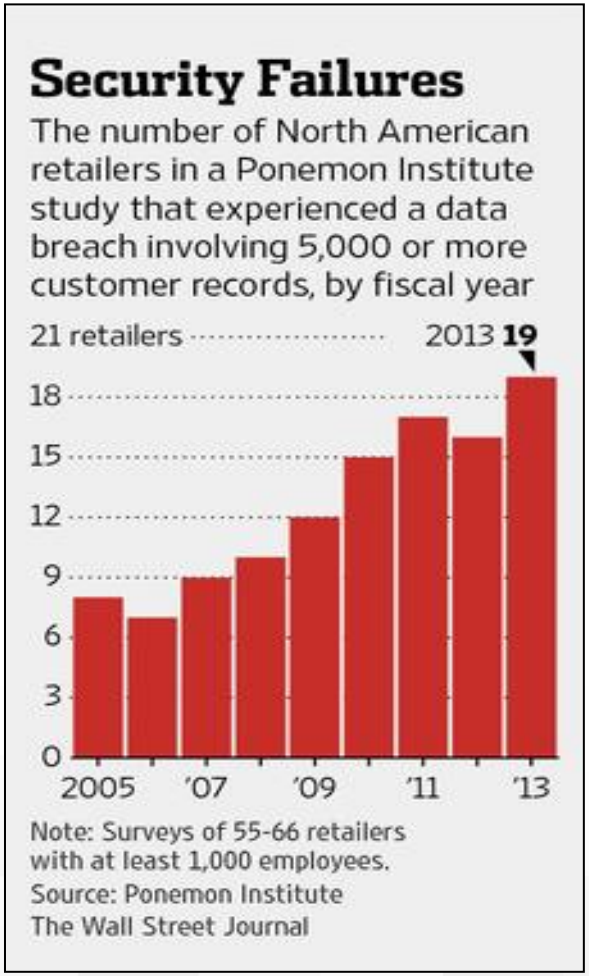
Cyber Risk – The Boardroom Perspective

MARCH, 2016

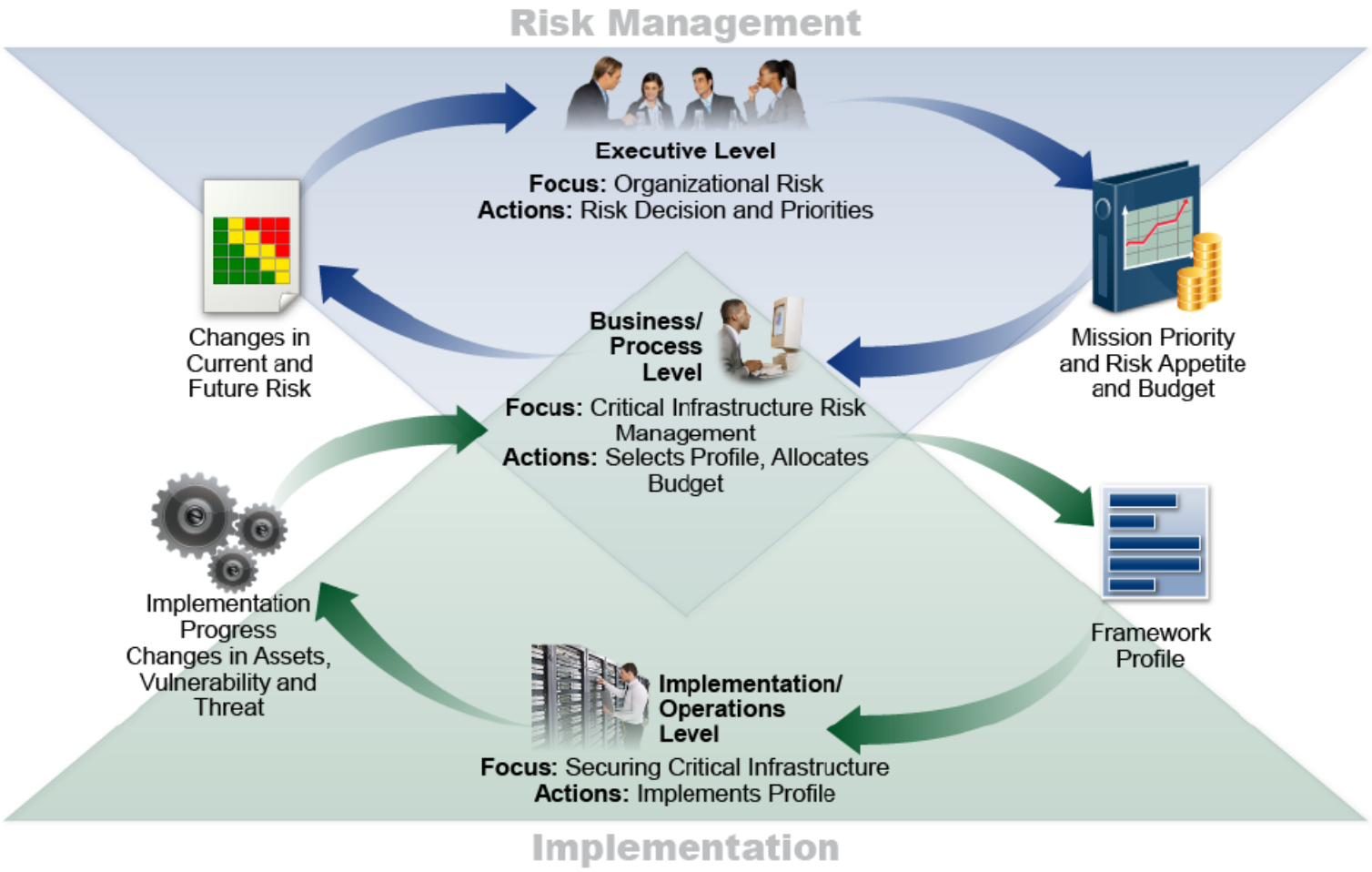
Threat Landscape

Cybercrime is not new but the sophistication and intensity of the attacks are increasing at an alarming rate.

- Well-funded and businesslike adversaries using targeted attacks
- Threats increasing on Point of Sales (POS) platforms
- Malware increasingly available at a price to make cybercrime affordable
- Security programs were compliant but compliancy does not equal security
- Ransomware attacks soared 113% in 2014
- Distributed Denial of Service (DDoS) attacks on the rise in 2016



Cyber Risk Management



Common Cyber Risk Management Challenges

Organizations across the country point to several strategic and tactical cyber risk concerns that contributed to ineffective information risk management and control

"We have not assessed our risks in terms of impacts to our business operations"

"Our cyber incident response and management control processes are weak"

"We have too many outages and we are always reactive. We don't learn from our mistakes"

"We have not defined a formal risk and security management strategy that is aligned with business objectives"

"We have unfortunately over-relied on our third party provider, and forgotten our risk management responsibilities"

"Our patching/upgrades processes are poor, and largely reactive"

"We do not have a mature cyber risk management strategy and program and have many pending audit issues"

"We do not know our real risks and it is because we have no real way of identifying threats and vulnerabilities"

"We have struggled to enhance our risk and security management program – The business expects adequate protection of its information but won't pay for it"

Coalfire

Industry Insights & Perspectives

Enterprises are increasingly facing strategic and tactical cyber risk issues resulting in incidents, breaches, & bad press

Strategic Issues

- Lacking or immature cyber risk management strategy and program
- Misalignment of risk and security initiatives with business objectives
- Limited executive insight and awareness of cyber risk posture
- Reactive approaches to cyber risk mitigation – negatively impacting Incident Response
- Inadequate IT internal controls and associated strategy

Tactical Issues

- Limited visibility of threats and vulnerabilities
- Poor change and configuration management resulting in ineffective system hardening
- Weak design, implementation, and enforcement of cyber security controls
- Risk management is not embedded into daily activities
- Ineffective incident response capabilities

Coalfire

Top Priorities

Observed cyber risk challenges highlight a set of key priorities for businesses

Strategic Alignment

- Ensure cyber risk and security initiatives are linked to business strategy and operational objectives

Program Management

- Manage cyber risk and security posture, operating procedures, and controls

Governance & Compliance

- Maintain visibility into cyber risk and security posture ensuring enforcement and alignment to business strategies and objectives.

Incident Response & Recovery

- Establish the framework for identification, response, and recovery of cyber events and incidents impacting the organization

Coalfire

Boardroom Priorities – Strategic Alignment

Consistency in communicating cyber risk amongst leadership, key stakeholders, and peers is pivotal to ensuring strategic alignment with organizational objectives, initiatives, and strategy

Key objectives:

- Facilitate a shared understanding between the business and IT on the contribution of cyber risk initiatives to business strategy
- Enable board and executive understanding of strategic cyber risk and cyber risk posture
- Define the overarching strategy for cyber risk management and operations
- Ensure business operations, initiatives, strategies, and drivers receive proper cyber risk considerations

Coalfire

Boardroom Priorities – Cyber Risk Program Management

Protecting organizational information assets and systems, as well as ensuring its integrity and confidentiality, entails developing and maintaining a cyber risk management program

Key objectives:

- Promote an understanding of priority and categorization of enterprise information assets
- Translate business, risk and compliance requirements into an overall cyber risk program plan
- Ensure consistent reporting and auditing across enterprise information assets and systems
- Implement access controls aligned to business function and operational need.
- Facilitate proactive protection measures throughout developmental, transactional, and operational life cycles
- Enable monitoring and testing of cyber risk response and resilience capabilities

Coalfire

Boardroom Priorities – Governance & Compliance

Establishing a framework for managing cyber risk posture, corporate governance and compliance requirements, aids in defining and maintaining cyber risk program value

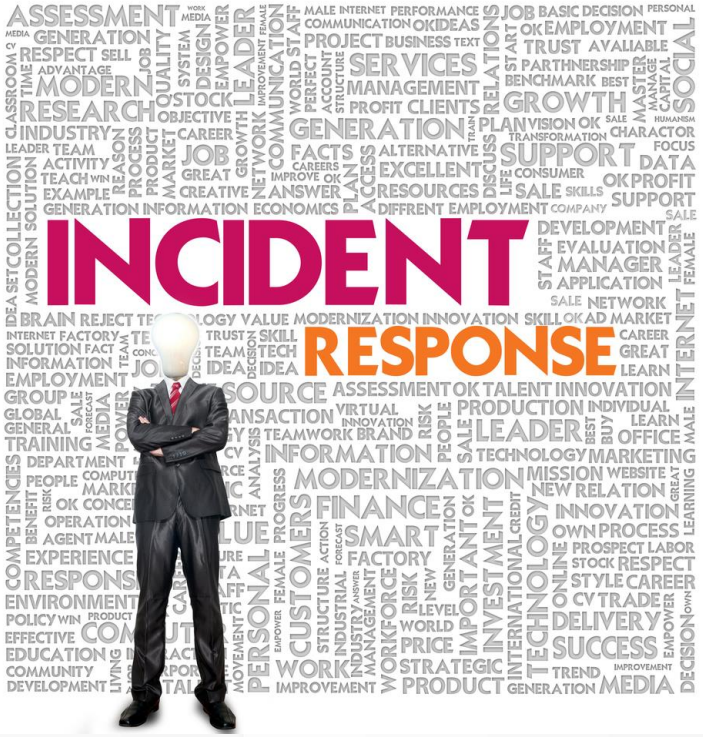
Key objectives:

- Deliver clear and concise expectations of cyber risk posture management across the organization
- Create a platform for defining and enforcing enterprise cyber risk policies
- Establish standards, guidelines, procedures and policy controls governing cyber risk
- Preserve the value, availability, integrity, and confidentiality of enterprise information assets and systems
- Institute metrics to periodically measure the effectiveness of cyber risk and control initiatives
- Comply with organizational and regulatory statutory requirements

Coalfire

Boardroom Priorities – Incident Response & Recovery

Defining a process for detecting, identifying, responding to, and recovering from, an event or incident is critical in mitigating damage to operations, systems, financials, or reputation



Key objectives:

- Establish and define an event and the escalation flow to incident declaration
- Determine business impact from an event or incident
- Institute strategic tactical roles responsibilities necessary for efficient response recovery efforts
- Develop and document procedures facilitating effective response and recovery
- Monitor and test the effectiveness of response procedures
- Facilitate continuous improvement

Guidance and Advisory Services

Seek out advisors that focus on helping enterprises define, deploy and sustain strategic initiatives that proactively mitigate current and emerging information risk

- Provide a deep understanding of current industry and cyber risk climate
- Assist in rationalizing current risk posture and cyber risk investments
- Collaborate across the enterprise to align cyber risk with business drivers and strategies
- Promote the formation of cyber risk programs and governance models
- Support the enterprise with the design and implementation of cyber controls
- Advise on policy creation, maintenance and support
- Guide the development of Incident Response planning and testing

Coalfire

Ask Yourself…

- Are we already compromised?
- Who have we identified as our threats?
- How have we aligned our cyber security approach to our business and organizational strategies?
- Where are the gaps and what are our plans to close those gaps?
- How are we evolving our cyber security approach to match the changing technology and security risk landscape?
- Where is our critical data and how is it protected from our threats?

Coalfire

Questions

Brian Prendergast
Office 303-554-6333 ext. 5326
Brian.Prendergast@Coalfire.com