Effective Cyber Risk Management & Trends in Cyber Risk Quantification

SIFMA IAS Seminar | December 3, 2018 | New York
Agenda

Introductions

Mike Hodges

The Fundamentals: PwC's Cyber Risk Management Program

Eric Lantz

Emerging Capabilities: Trends in Cyber Risk Quantification

Charlie Leonard

Questions and Answers

All
The digital revolution is transforming industries without exception – and catching many off guard. Demand and competition are subject to radical and rapid changes.
In addition to changing company and market dynamics, the digital revolution also changes the concept of digital and technology risk.
Companies are being driven to change the way they manage risk

Increased role of Boards and the CEO in cyber risk oversight is driving demand for better methods to measure and articulate business and economic impacts of cyber risks.

Cyber security breaches erode companies’ share prices permanently and have resulted in billions of dollars in market valuation being erased since 2013⁴ - as new regulations require better breach reporting financial markets will respond.

Companies are becoming digital and current approaches to cyber risk management must evolve from subjective, checklist and compliance driven methods to data-driven risk models.

Top Questions Boards and Executives are asking risk and cyber leadership:

1. What are our top cyber risks and how much exposure do they represent?

2. Where are we allocating resources and dollars? Are we investing too little or too much?

3. How effective are our investments in risk reduction (return on security investments)?

⁴CGI-Oxford Economics Study: Cyber-Value Connection
They are realizing benefits from leading the way in digital transformation

**Executives** who:

1. call their organizations more innovative than those of their peers, and
2. consider their risk management programs to be more effective

...are **three times more likely** than their less-effective and less-innovative peers to anticipate revenue growth.
They are doing more to engage risk and security early in the transformation

91% of enterprise-wide digital transformation include security and/or privacy personnel as stakeholders.

53% include proactive management of cyber and privacy risks by design in the project plan and budget "fully from the start."

q1060: Earlier you said that your company is currently involved in an enterprise-wide digital transformation project. To what extent is proactive management of cyber and privacy risks included by design in the project plan and budget?
These efforts present challenges and opportunities for auditors

**Technical Prowess**
*How can IA attract and retain the right skills to provide an effective Third Line of Defense?*

**IA Program**
*How can IA find the right balance between scope, coverage, and frequency while minimizing “audit fatigue” in Operations due to continuous Risk Oversight?*

**Focus**
*How can IA balance the demands of expanding audit activities beyond 1st Line of Defense cyber risk control testing, maintain focus on the effectiveness of the overall cyber risk program, and challenge the 2nd Line of Defense?*

**Stakeholders**
*How can IA meet regulators’ expectations and audit committee demands for more effective cyber risk audits?*
The Fundamentals

PwC’s Cyber Risk Management Program
Organizations continue to struggle with common pitfalls

**Pitfalls**

- Evolving cyber function from risk assessors to risk managers
- Applying risk management discipline to strategic cyber planning

**Response**

- Elevate cyber function to be an enabler of Business Strategy using a robust, yet agile risk framework

**Methods**

- Modelling dependencies between threats, assets and capabilities
- Frameworks and/or compliance driven approach to evaluating risks and prioritizing investments

**Reporting**

- Articulating cyber and value connection in business friendly terms
- Meaningful metrics and actionable risk intelligence that answer the “so what” question and drive actions

**Data driven risk management**, leveraging threat-asset-capability relational data model and probabilistic Value at Risk techniques

**Quantify risks into tangible metrics that can be used for informed decision making**
Pain points in effectively managing and overseeing cyber risk

It is challenging to achieve a common understanding of cyber risk management efforts that spans the 3 lines of defense

<table>
<thead>
<tr>
<th>No. 1</th>
<th>No. 2</th>
<th>No. 3</th>
<th>No. 4</th>
<th>No. 5</th>
<th>No. 6</th>
<th>No. 7</th>
<th>No. 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber risk tolerance and risk appetite is not established or understood</td>
<td>Security strategy does not align with business objectives or risk appetite</td>
<td>Enterprise risk parlance is not used to articulate cyber risks</td>
<td>The Board and Executive Leadership has limited visibility into impact of cyber risks</td>
<td>Risk management “ownership” is not established</td>
<td>Roles and responsibilities across the three lines are often ambiguous</td>
<td>Controls are not designed to address risk but to manage compliance</td>
<td>Audit fatigue due to proliferation of compliance requirements</td>
</tr>
</tbody>
</table>
PwC’s Cyber Risk Management Program Components

Cyber Risk Governance, Strategy and Operating Model

The foundation of the Cyber Risk Management Program is defined and aligned to the enterprise risk appetite and strategy. Some of the key activities include:

- Defining the operating model
- Setting cyber risk appetite for the enterprise or lines of business
- Establishing risk committees
- Defining Cyber Risk Management policies & standards for second line of defense

Cyber Risk Identification and Assessment

Cyber risks and threats that could potentially impact the enterprise are identified, as well as the controls that are in place to mitigate them. Some of the key activities include:

- Risk identification and threat profiling
- Determining inherent risk, identifying and evaluating controls and residual risk estimation

Cyber Risk Monitoring and Reporting

A formal and repeatable process is established to monitor key performance indicators and report their evolution to the board of directors or appropriate risk committees. Some of the key activities include:

- Design a cyber risk dashboard and reporting platform
- Define second line of defense key performance indicators and establish a mapping to the enterprise key risk indicators

Cyber Risk Response

A plan is defined to treat risk and manage risk exposure. Some of the key activities include:

- Analyze risk appetite vs current risk exposure to determine the appropriate risk treatment decision (i.e. treat, terminate, transfer, tolerate)
- Identify mitigation actions and implement according to determined plan

Establishing an effective Cyber Risk Management Program enables organizations to consistently identify, assess, respond to, monitor, and report on existing and emerging cyber risks.
Beyond the financial services sector most organizations have limited enterprise risk management capabilities. Hence, Cyber Risk Management is still evolving from a traditional security-focused function to managing cyber risks with an enterprise risk lens.

**Evolving Approaches in Managing Cyber Risks**

**Business Complexity**
- Rate of growth
- Change in market dynamics
- Operational complexity
- Regulatory landscape
- Outsourcing
- Alliances
- Product complexity
- Mergers & acquisitions

**Security-Focused**
- Responsibility and accountability limited to Information Security team
- Meet minimum regulatory requirements
- No understanding of risk tolerance
- Executive and Board’s role in risk management/oversight is very limited

**Past and Current Generation Models**

**Integrated Risk and Compliance Management**
- Risk management drives compliance management and security standards
- Reduced audit fatigue
- Business is engaged in risk conversations
- Nascent definitions of risk tolerance
- ERM not integrated with digital risk
- Board and Executives briefed on maturity, but lack a view of risk

**Next Generation Model**

**Mature Cyber Risk Management**
- Common enterprise risk taxonomy defines technology and cyber risk
- Board and Executive Leadership clearly understand business impact of cyber risks
- Enterprise approach to risk management
- Defined processes and tools to identify, assess, monitor, and report cyber risk relative to risk tolerance and other enterprise risks
- A formally defined governance and operating model for risk management (e.g., three lines of defense)
- Ability to constantly monitor threat landscape and evolve the risk management capability
- Control mechanisms to ensure board and management accountability for priority risks
- Compliance and its monitoring are inherent in ongoing risk management activities

Beyond the financial services sector most organizations have limited enterprise risk management capabilities. Hence, Cyber Risk Management is still evolving from a traditional security-focused function to managing cyber risks with an enterprise risk lens.
In heavily-regulated industries (e.g., Financial Services), allocating key functional attributes and responsibilities across three distinct lines of defense promotes transparency and accountability for cyber risk ownership, oversight, and assurance.

### Board and Committee(s) Oversight

<table>
<thead>
<tr>
<th>Mature Model in Heavily Regulated Industry</th>
<th>Less Mature Model in Less Regulated Industries</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1st Line of Defense CIO/CISO and Business Units</strong></td>
<td><strong>1st Line of Defense CIO/CISO and Business Units</strong></td>
</tr>
<tr>
<td>Owns the risks</td>
<td>Owns the risks</td>
</tr>
<tr>
<td>Operates the controls</td>
<td>Operates the controls</td>
</tr>
<tr>
<td>Monitors risk, threats and controls on an ongoing basis</td>
<td>Monitors risk, threats and controls on an ongoing basis</td>
</tr>
<tr>
<td>Independently oversees risks</td>
<td></td>
</tr>
<tr>
<td>Owns framework</td>
<td></td>
</tr>
<tr>
<td>Sets policy</td>
<td></td>
</tr>
<tr>
<td>Provides credible challenge</td>
<td></td>
</tr>
<tr>
<td>Independently aggregates and reports on material cyber risks</td>
<td></td>
</tr>
<tr>
<td><strong>3rd Line of Defense Internal Audit</strong></td>
<td><strong>3rd Line of Defense Internal Audit</strong></td>
</tr>
<tr>
<td>Independently tests controls</td>
<td>Independently tests controls</td>
</tr>
<tr>
<td>Evaluates program adherence by first and second lines of defense</td>
<td>Evaluates program adherence by first line of defense</td>
</tr>
<tr>
<td>Evaluate overall cyber risk management effectiveness</td>
<td></td>
</tr>
</tbody>
</table>
The traditional role and organizational positioning of Chief Information Security Officers (CISOs) is evolving, especially in regulated industries and more complex organizations, and may be determined or complemented by the establishment of a second line independent cyber risk function and officer independent from the Chief Information Officer (CIO) and the CISO. Most organizations are in the process of implementing a second line of defense for Cyber Risk Management:

Security Focused

- Tech & Ops Leader (e.g., CIO)
- Head of Technology Risk / CISO
- Governance
- Threat Mgmt. and Risk Assurance
- Risk Reporting
- Technology / Security Operations

Risk Focused Oversight of Security Operations

- Chief Risk Officer (CRO)
- 2nd Line Leader for Cyber / Technology Risk / CISO
- Technology / Security Operations
- Governance
- Threat Mgmt. and Risk Assurance
- Risk Reporting
- Chief Security Officer (CSO)

Incremental capabilities in addition to what exists in first line
PwC’s Cyber Risk Management Program - Benefits

- Efficiency through improved focus on cyber risks with enterprise risk implication
- Enhanced awareness by those ultimately accountable – Board of Directors
- Clearer accountability and roles and responsibilities between risk ownership and risk oversight
- Preservation of profits and market cap
- Increased stakeholder and regulator confidence, and all that entails for brand and reputation
- Value-added, actionable cyber risk intelligence – Executive Management’s decision making
- Independent, credible challenge of operations by officers/functions outside CIO’s span of control
Emerging Capabilities

*Trends in Cyber Risk Quantification*
Companies are investing in technology that accelerates risk oversight

Successful risk management functions are investing in these areas for greater efficiency, visibility, and risk mitigation

1. Analytics, Visualization and Insights

- Advanced analytics, modelling and quantification of cyber risks
- Decision-oriented risk visualization tools

2. Data Fusion and Platform

- Data lakes and integrated data model to tackle siloed data
- Applying artificial intelligence and machine learning to data sets

3. Data Sources and Processes

- Integrating threat modelling, threat hunting and risk assessment capabilities
- Orchestration / Automation of risk and compliance processes and controls
They are building an enterprise view of risk with aggregated metrics

Board & Executive Committee
- Significant incidents
- Cyber / Operational / Financial Risk
- Key Strategic Risk Indicators

Lines of Business & Accountable Executives
- Risk Tolerance
- Program Status
- Key Risk Indicators
- Key Performance Indicators

Risk & Security Operations Teams
- Control KPI
- Compliance
- Program Status
- Remediation Efforts

Cyber Risk Oversight
Cyber Risk Ownership
Cyber Risk Operations
They are maturing the way that risk oversight operates and communicates.

Metrics will reflect the results of management’s efforts to integrate cyber risk into overall enterprise risk function. This is a journey and metrics will mature through these phases.

Understanding Risk
- Inventory assets
- Assess maturity
- Assess threat and risk
- Understand 3rd party obligations

Prioritizing Risk
- Formalize governance
- Interpret risk assessments
- Build remediation plans
- Allocate resources
- Inventory assets
- Assess maturity
- Assess threat and risk
- Understand 3rd party obligations

Monitoring Risk
- Develop meaningful metrics
- Actively engage in discussions about efforts to improve
- Observe peers and competitors for signals
- Formalize governance
- Interpret risk assessments
- Build remediation plans
- Allocate resources
- Inventory assets
- Assess maturity
- Assess threat and risk
- Understand 3rd party obligations
They are reaping the benefits of enhanced knowledge and visibility

**Message**
Promote the value & effectiveness of your cybersecurity program to executives – in simple business and economic terms

**Risk Portfolio**
Understand your aggregate portfolio of cyber risk and track how well your cyber capabilities are performing in managing your Value at Risk

**Capability Optimization**
Transform information into insights to help you manage diminishing returns in your cyber capabilities

**Capital Agility**
Develop a defendable cyber investment strategy that allows you to effectively allocate limited resources and funds and respond to unexpected resource constraints
They are using digitized inputs to make value-based strategic decisions.

**Digital Risk models based on:**
- Current security posture
- Asset prioritization
- Threat prioritization

**Are able to give insights like:**
- Value at risk across the business portfolio
- Investment evaluation
  - Risk reduction benefits
  - Security posture gain
- Capability relevancy assessment
- Business objectives alignment
- Capability improvement ideation
- Risk metrics analysis
They are making decisions faster and achieving greater impact.

Phase 1
Define Tier 1 Enterprise Risks ⇒ Apply Impact Quantification

Phase 2
Expand Model Scope ⇒ Monitor Appetite, Mitigation Decisions
What should auditors be thinking about; how can they take action?

<table>
<thead>
<tr>
<th>Return to Fundamentals</th>
<th>Emerging Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>What are you doing to address the current state of fundamentals?</td>
<td>How are you laying the groundwork for successful embrace of emerging capabilities?</td>
</tr>
</tbody>
</table>
Thank you.

Questions?
Appendix
The first step to develop a Cyber Risk Management program is to identify the risks and threats that are realities of doing business in today’s environment. Once risks and threats have been identified for your organization, those risks must be assessed to understand the existing control environment which enables the organization to make risk response decisions.

**Identify Risk and Threats**
- **Critical Asset Identification**
- **Threat Profiling**
- **Identify Risks for Assessment**

**Assess Risks**
- **Determine Inherent Risk**
- **Identify/Evaluate Controls**
- **Determine Residual Risk**

- **Focus on the alignment of critical assets with relevant business risks and cyber threats:**
  - What are the “Crown Jewels”?
  - Who/what are the potential threat actors, motives, and vectors?
  - What are our business risks (i.e., data breach, fraud)?

- **Focus on the alignment of identified risks with relevant cyber controls:**
  - What are the potential impacts (i.e., monetary, legal)?
  - What controls are in place to mitigate the risks?
  - Is the residual risk in line with our risk tolerance?
Cyber Risk Response

Formally setting a risk appetite for the enterprise and / or lines of business will help organizations understand and respond to adverse changes to their risk profile. This will help drive decision making including deployment of new controls and more successful risk mitigation strategies.

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Very High</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
<th>Very Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Magnitude of consequences</td>
<td>S</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>S</td>
</tr>
</tbody>
</table>

Risk appetite vs. risk exposure influences risk treatment decision... and... that is based also on the specific level of considered risk.

- **Treat** - directly manage and implement corrective controls (designed to reduce unacceptable vulnerability)
- **Terminate** - try to eliminate the cause of this risk, implement preventive controls (designed to limit the possibility of an undesirable hazard event occurring)
- **Transfer** - not directly managed, implement directive control (e.g., transfer to insurance)
- **Tolerate** - benefits outweigh disadvantages; affordable contingencies; detective control (to identify impacts)

Identify potential risk mitigation actions including risk reduction, risk transfer and risk acceptance.

Select mitigation actions:
- Advantages and disadvantages (e.g., cost-benefit ratio)
- Project cost and schedule benefits vs. implementation costs
- Standards and company rules

Implement mitigation.
To make the right decisions, Executive Leadership and the Board of Directors must have the necessary information at its fingertips. An effective Cyber Risk Dashboard and Reporting Capability enables an organization to monitor and dynamically respond to changes in its cyber risk profile.

1. Disparate sources of data are aggregated in a dedicated Cyber Risk Dashboard and Reporting Platform.

1. The platform is used by members of the Cyber Risk Operations Team to perform scheduled and ad-hoc reporting on a variety of key topics (e.g., recent cyber incidents, their duration, the assets that were targeted, related external events etc.).

1. The Operations Team provides ongoing reports to the Cyber Risk Governance and Oversight Committees.

1. Reports provided the Cyber Risk Oversight Committee contain the status of various activities being performed to address cyber threats and improve cyber resiliency across the organization.

1. The Cyber Risk Governance and Cyber Risk Oversight Committees provide periodic reporting to Executive Leadership.
Cyber Risk, Threats and Controls Library

An integrated risk and controls library enables continuous risk management and cross-functional coordination (i.e., within Security and between Security, Risk Organizations, and Business Units).

Example Control Domains:
- Architecture and Operations
- Threat and Vulnerability Management
- Information and Asset Protection
- Identity and Access Management
- Business Continuity
- Third Party Management
- Incident and Crisis Management
- Risk, Compliance, and Policy Management
- Strategy, Governance, and Management
- Physical and Environmental Security