Rethinking Information Security
Risk Management

CRM002

Speakers:
Tanya Scott, Senior Manager, Information Risk Management, Lending Club
Learning Objectives

At the end of this session, you will:

• Design a comprehensive framework to guide your information security risk management program

• Take steps to enhance information security risk management

• Develop tools that drive strategic risk discussions and investment decisions
Agenda

• Current State of Information Security Risk Management (ISRM)

• ISRM Program Considerations

• Showcasing the ISRM Value Proposition

• Closing Remarks

Disclaimer: The views expressed are my own and do not reflect the official policy or position of any of my current or previous employers and clients.
Current State of Information Security Risk Management
A Global Issue

Some estimates predict that between $9 and $21 trillion of global economic value creation could be at risk if companies and governments are unable to successfully combat cyber threats.

NACD Cyber-Risk Oversight, 2014

US DATA RECORDS BREACHED 2005 - PRESENT

Privacy Rights Clearinghouse (March 27, 2016)

898,458,345

COST OF A DATA BREACH

2015 Ponemon / IBM DBR

Average Consolidated Total Cost  $3.8M
Average Cost Incurred Per Record  $154
US Data Breaches

Sum of Records Breached by Year
Utilizing Privacy Rights Clearinghouse Breach Data as of 3/27/2016

- CARD
- HACKER
- INSIDER
- PHYSICAL
- PORTABLE
- STATIONARY
- UNINTENDED
- UNKNOWN

Trends in ISRM

Information security risk management is becoming more critical (and difficult) to implement:

• Increasing publication and transparency of incidents
• Value of information is increasing, information is often a competitive advantage
• Work environment and how we access information is changing
• Continuously changing technologies and threat environment
• Increasingly difficult to find skilled and experienced resources
• Changing compliance and regulatory requirements
• Increased scrutiny by stakeholders
ISRM Stakeholder Inquiries

- Board of Directors, Audit and Risk Committees
- Enterprise Risk Management
- Information Security Steering Committee
- Internal Audit
- Customers
- Regulators
Cyber-Risk Oversight
*NACD Director’s Handbook Series*

- Treat cybersecurity as an enterprise-wide risk management issue
- Understand the legal implications of cyber risks
- Cybersecurity expertise, and regular discussions about cyber-risk
- Set the expectation that management establish an enterprise-wide cyber-risk management framework with adequate staffing, budget
- Discuss risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach
## Current ISRM Practices

### Risk Governance
- Program Management
- Framework(s)
- Guidance
- Process(es)
- Risk Definition

### Risk Assessment
- Penetration Tests
- Vulnerability Scanning
- Incident Response
- Third Party Risk
- Project Security Risks
- Application Security Assessments
- Risk Response

### Risk Context
- Strategic
- Operational
  - Process
  - Asset

### Third Party Advice
- Commodity Service Offerings
- Focus on Capabilities

### Risk Monitoring & Reporting
- Risk Trending
- KRIs
- Emerging Risks
- Risk Reporting:
  - Sr. Mgmt.
  - ERM / BOD
The Gap in Expectations

- Network Breach
- Back office systems are breached and sensitive customer data is exposed.
- A key third party service provider suffered a major breach impacting our customers’ information.
- As a result of server theft, an unauthorized disclosure of sensitive customer data for all customers affected. Notifications were sent to regulators and affected parties.
- System addressed, but network infrastructure should be reviewed to highly secure systems.

- System 1: Non-existent
- System 2: Initial
- System 3: Repeatable
- System 4: Defined
- System 5: Managed

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.
Information Security Risk Management Program Considerations
### Develop a Compelling Vision

<table>
<thead>
<tr>
<th>Vision</th>
<th>Mission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deliver epic information security risk management capabilities that</td>
<td>Support management’s ability to make informed resource allocation</td>
</tr>
<tr>
<td>optimize investments and creates competitive advantage for the</td>
<td>decisions by providing visibility into key information security risks.</td>
</tr>
<tr>
<td>organization.</td>
<td></td>
</tr>
</tbody>
</table>

#### Guiding Principles for FYXX

- Develop a program for Information Security Risk Management which allows the organization to communicate in a common language understood by senior management and the Board
- Build foundational components with an emphasis on “fit” (within the culture and operating style)
- Guide management in proactively reducing the risks associated with high priority areas
- Make risk decisions at the appropriate level
- Make informed resource allocation decisions
- Establish relationships between the organization and key stakeholders
Select Framework(s)

- Corporate Governance
- IT Governance
- Information Security Governance
- Enterprise Risk Management
- IT Risk Management
- Information Security Risk Management
- Capabilities
- Internal Control

**BE CAUTIOUS OF "BEST PRACTICES" and CHECKLISTS!**
Consider a Nested Model
Define ‘Risk’

- Risk – an event that may occur and positively or negatively affect the achievement of objectives

- Risk = Threat + Vulnerability
  - Threat – an actor or event that could exploit a vulnerability
  - Vulnerability – a weakness

- Risk ≠ Vulnerabilities
- Risk ≠ Controls
- Risk ≠ Issue

- Risks are dynamic
Risk ≠ Threat
Risk ≠ Vulnerabilities

- **THREAT**
  - Hacker
  - Insider
  - Third Party
  - System Outage
  - Natural Event

- **CAPABILITY & CONTROL WEAKNESSES**
  - Threat & Vulnerability Management
  - Identity & Access Management
  - Asset Management
  - Physical Security
  - Incident Response

= **RISK**

- Threat exploits a vulnerability leading to XYZ (Consequences)
Risk ≠ Issue

• **Issue** - An issue is an event that currently exists – there is a 100% probability of occurrence.

• **Risk** - A risk is an event that may occur and would have a positive or negative impact on the organization’s objectives. Note that a risk *may* occur. It is not a certainty (it has a less than 100% probability of occurring).

<table>
<thead>
<tr>
<th>Issue</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application ABC passwords are not in compliance with the password policy. This is an <strong>issue</strong> (100% known, non-compliance)</td>
<td>Application ABC passwords do not expire within 90 days. An attacker may be able to crack the password and obtain access to sensitive information. This is a <strong>risk</strong>. The event <em>may</em> occur.</td>
</tr>
</tbody>
</table>
Set Context with Risk Tiers

ERM / BOD Risks
(Tier 1)

- Information security events that would impact the achievement of strategic objectives

Information Security Operational Risks
(Tier 2 - Annual Assessment with Regular Monitoring)

- Information security events that would impact the achievement of operational objectives; align with BOD and Asset Level risks

Asset and Process Level Risks
(Tier 3 - Transactional with Regular Monitoring)

- Information security risks associated with specific assets or processes
Use Asset and Process Profiles

Profiles are intended to assess the ‘sensitivity’ or ‘criticality’ of an asset or process, prior to conducting a risk assessment

- Increases efficiency and speed of assessments
- Assists with prioritization of resources
- Enables balance of capabilities and controls

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ABC</td>
<td>25%</td>
<td>25%</td>
<td>20%</td>
<td>20%</td>
<td>10%</td>
<td>100%</td>
<td>HIGH</td>
</tr>
<tr>
<td>XYZ</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>HIGH</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>2.9</td>
<td>MODERATE</td>
</tr>
</tbody>
</table>
Document ISRM

• Vision, Mission, Principles
• Policy and Standards, Roles and Responsibilities
• Program Components, Framework, Process(es)
• Risk Assessment / Management Guidance
• ISRM Capability Maturity Model
• Timeline / Roadmap of Key Activities and Initiatives
• Cross-Functional ISRM Council/Committee and Charter
• Risk Reporting Audiences, Objectives, and Cadence
Mature ISRM Over Time

Sample Roadmap Highlighting Key Phases

Key Milestones:
- Establish Risk Program
- Conduct Quarterly Risk Assessments
- Risk Governance
- Risk Reporting
- Provide senior management with update on top risks and responses
- Automate Risk Tools
- Mature Risk Reporting with full catalog of KPIs
- Risk Aware Operations
- Investment Portfolio Management / Risk Valuation

Charts showing the maturity of the ISRM program increasing over time helps convey the program vision and the commitment to continuous improvement.
Showcasing the Value Proposition
Link Risks and Capabilities/Controls

- Hacker
- Insider
- Third Party
- System Outage
- Natural Event

Potentially Exploits

- Threat & Vulnerability Management
- Identity & Access Management
- Asset Management
- Physical Security
- Incident Response

= Threat exploits a vulnerability leading to XYZ (Consequences)
Advise Management on Risk Treatment Options

Show how each risk treatment option reduces risk AND adds value

Identify and Quantify Value Drivers

• Improves customer experience
• Increases customer trust and improves brand
• Supports talent acquisition
• Increases compliance
• Decreases cost
• Increase employee satisfaction
• Improves efficiency
• Increases agility, speed to market
A Balanced Approach
Define and Quantify Exposure

COST OF A DATA BREACH
2015 Ponemon / IBM DBR

Average Consolidated Total Cost $3.8M
Average Cost Incurred Per Record $154
Experiment With the Upside

Identify events that may create value and explore the potential positive impact on objectives

Opportunities:
• Trust centers
• Certifications
• Bug bounty programs
Closing Remarks
Key Considerations & Takeaways

• Review the ISRM program
  • Take a holistic approach to ISRM
  • Clearly define ‘risk’
  • Develop Information security risk tiers
  • Utilize asset and process profiles
  • Identify and measuring security capabilities
  • Document the program and roadmap

• Maximize the use of information security risk data
  • Inform resource allocation decisions
  • Guide internal audit efforts
  • Advise management on risk treatment options
  • Highlight information security events that create value
Learning Objectives

At the end of this session, you will:

• Design a comprehensive framework to guide your information security risk management program

• Take steps to enhance information security risk management

• Develop tools that drive strategic risk discussions and investment decisions
Questions?
Resources

Framework Related Resources

• ISO 31000:2009 – Risk Management Principles and Guidelines
• ISO/IEC 31010:2009 – Risk Assessment Techniques
• ISO 27000 series – Information Security Standards
• NIST – Cybersecurity Framework and Special Publications on Information Security & Risk (SP 800-37, 39, 53, 161)
• ANSI/ASIS/RIMS Risk Assessment Standard (RA.1-2015)
• OCEG “Red Book” 2.0: 2009 – A Governance, Risk and Compliance Capability Model
• ISACA: COBIT 5, COBIT 5 for Information Security, COBIT 5 for Risk
Resources, cont.

Research

- IBM and Ponemon Institute 2015 Cost of Data Breach Study
- Verizon Data Breach Digest
- Verizon 2015 Data Breach Investigations Report
- NACD Cyber-Risk Oversight Resource Center
- Gordon-Loeb Model
- Privacy Rights Clearing House
- Corporate Executive Board
- Gartner
- Forrester