Cybersecurity: Considerations for Internal Audit

IIA Atlanta Chapter Meeting
January 9, 2015
Agenda

• Key Risks
• Incorporating Internal Audit
• Resources for Internal Auditors
• Questions
Key Risks
2. Cost of Cybercrime Doubles for U.S. Retailers

Cyberattacks wreaked havoc in 2014, especially among large American retailers. A survey by the Ponemon Institute indicates the average cost of cybercrime for U.S. retail stores more than doubled from 2013 to an annual average of US$8.5 million per company in 2014. Attacks at big-name companies raised serious concerns about the effectiveness of the private sector's information security. No industry is immune, and during the past few months the largest cyberattack in history was carried out against independent media sites in Hong Kong.

Implications: Retailers are fighting back with the launch of a new Retail Cyber Intelligence Sharing Center (R-CISC). But despite the spotlight on cybercrime, many companies are not well-prepared. According to a 2014 survey (PDF) by Protiviti, there has been a significant year-over-year jump in the number of organizations without a formal documented crisis-response plan. One in three companies do not have a written information security policy, and more than 40 percent lack a data-encryption policy. One-fourth don't have acceptable use or record-retention/destruction policies.

Internal auditors can play a number of important roles in battling cybercrime, for example, assessing whether controls and policies are in place, verifying that the organization's incident response plans are robust, ensuring compliance with changing regulations/legislation pertaining to cybersecurity, and verifying that a breach notification plan is in place.
Key Risks

• Board and Management:
  – CIO, CAE, organizational leaders agree:
    ▪ Cyberthreats not only an IT problem, but a fully fledged business risk
  – Top 10 risk
    ▪ Separate from business interruption; loss of reputation and brand value; theft fraud and corruption
Key Risks

- Nature of attack:
  - Denial of service attacks (DoS)
  - Data security breaches

- Focus of attack:
  - Credit card data (e.g. retail)
  - Exploration data (e.g. oil and gas)
  - Intellectual property (e.g. technology, strategic information)
Key Risks

• Internal
  – Trusted employees
  – Business partners

• External
  – Stolen credentials
  – Remote access systems
Key Risks

• Threats
  – Rapidly evolving
  – Increasingly sophisticated
  – Methods continue to improve
Key Risks

• Cost of data breaches
  – Fixing the problem
  – Legal costs
  – Fines
  – Class Action Lawsuits
Incorporating Internal Audit
Incorporating Internal Audit

- Persistent threat
- Exposures
- Security posture
- Audit procedures
- Assisting management
- Resource application
Incorporating Internal Audit

- Be engaged at the strategic level:
  - Understand board’s approach to security
  - Better understand the value of business-critical data
  - Working with systems administrators
  - Being involved with new IT implementations
Incorporating Internal Audit

Focus on:
- Specific types of attacks they face
- Weaknesses inherent in business practices, culture, IT systems
- Educating the Board
  - Business risk
  - Risk to data
  - Critical assets
  - Nature of network traffic
- Prevention, Detection and Response
Incorporating Internal Audit

Key Elements:
- Leadership and governance
- Technical and operational controls
- Training and awareness
- Information risk management
- Response planning
- Crisis management
Incorporating Internal Audit

- Auditing defense mechanisms:
  - Secure firewalls
  - Up-to-date antivirus software
  - Open communication to ISPs
  - Effective network monitoring
  - Rapid response plans
Incorporating Internal Audit

- Auditing defense mechanisms:
  - Password management
  - Data categorization, segregation, access storage, and retention process
  - Suppliers’ cybersecurity practices; service agreements
  - Cloud services
  - Data security controls
  - Corporate insurance coverage
Incorporating Internal Audit

- IT Audit Resources:
  - Perform business and IT impact analysis and risk assessment
  - Cyberrisk assessment
    - External input on threats facing industry
    - Current attack methods
  - People, process and technology controls
  - Incident response program
  - Help optimize controls to prevent or detect cyber issues
  - Ongoing monitoring of changing cyberrisk
Incorporating Internal Audit

- Internal Audit Resources:
  - Drive discussion around risk and mitigation strategy
  - Independently assess and prioritize cyberrisks against other critical enterprise risks
  - Assess effectiveness of preparation
  - Identify and monitor issues and risk related to emerging technology deployments
Incorporating Internal Audit

- Supporting the Audit Committee:
  - Five Principles:
    1. Understand and approach to cybersecurity
    2. Legal implications
    3. Access to expertise
    4. Staffing and budget
    5. Risk avoidance
Resources

• U.S. National Institute of Standards and Technology (NIST)
  – Framework for Improving Critical Infrastructure Cybersecurity
  – Consistent and effective evaluation of current security:
    ▪ Processes
    ▪ Procedures
    ▪ Technologies
  – Links to other security standards and approaches
<table>
<thead>
<tr>
<th>Function Unique Identifier</th>
<th>Function</th>
<th>Category Unique Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identify</td>
<td>ID.AM - Asset Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.BE - Business Environment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.GV - Governance</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RA - Risk Assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RM - Risk Management</td>
<td></td>
</tr>
<tr>
<td>PR</td>
<td>Protect</td>
<td>PR.AC - Access Control</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.AT - Awareness and Training</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.DS - Data Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.IP - Information Protection Processes and Procedures</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.MA - Maintenance</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.PT - Protective Technology</td>
<td></td>
</tr>
<tr>
<td>DE</td>
<td>Detect</td>
<td>DE.AE - Anomalies and Events</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.CM - Security Continuous Monitoring</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.DP - Detection Processes</td>
<td></td>
</tr>
<tr>
<td>RS</td>
<td>Respond</td>
<td>RS.RP - Response Planning</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.CO - Communications</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.AN - Analysis</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.MI - Mitigation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.IM - Improvements</td>
<td></td>
</tr>
<tr>
<td>RC</td>
<td>Recover</td>
<td>RC.RP - Recovery Planning</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.IM - Improvements</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.CO - Communications</td>
<td></td>
</tr>
</tbody>
</table>

## Table 2: Framework Core

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
</table>
| **IDENTIFY** (ID) |  |  | • CCS CSC 1  
• COBIT 5 BA109.01, BA109.02  
• ISA 62443-2-1:2009 4.2.3.4  
• ISA 62443-3-3:2013 SR 7.8  
• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2  
• NIST SP 800-53 Rev. 4 CM-8 |
|  | Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy. | ID.AM-1: Physical devices and systems within the organization are inventoried | • CCS CSC 2  
• COBIT 5 BA109.01, BA109.02, BA109.05  
• ISA 62443-2-1:2009 4.2.3.4  
• ISA 62443-3-3:2013 SR 7.8  
• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2  
• NIST SP 800-53 Rev. 4 CM-8 |
|  |  | ID.AM-2: Software platforms and applications within the organization are inventoried | • CCS CSC 1  
• COBIT 5 DSS05.02  
• ISA 62443-2-1:2009 4.2.3.4  
• ISO/IEC 27001:2013 A.13.2.1  
• NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8 |
|  |  | ID.AM-3: Organizational communication and data flows are mapped | • COBIT 5 APO02.02  
• ISO/IEC 27001:2013 A.11.2.6  
• NIST SP 800-53 Rev. 4 AC-20, SA-9 |
|  |  | ID.AM-4: External information systems are catalogued | • COBIT 5 APO03.03, APO03.04, BA109.02  
• ISA 62443-2-1:2009 4.2.3.6  
• ISO/IEC 27001:2013 A.8.2.1  
• NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14 |
|  |  | ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value | • COBIT 5 APO01.02, DSS06.03  
• ISA 62443-2-1:2009 4.3.2.3.3  
• ISO/IEC 27001:2013 A.6.1.1 |
|  |  | ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established | |

Resources

Cybercrime Audit/Assurance Program

• Aligned with the NIST National Initiative for Cybersecurity Education

http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybercrime-Audit-Assurance-Program.aspx
VI. Audit/Assurance Program

<table>
<thead>
<tr>
<th>Audit/Assurance Program Step</th>
<th>COBIT Cross-reference</th>
<th>COSO Cross-reference</th>
<th>Reference Hyperlink</th>
<th>Issue Cross-reference</th>
<th>Comments</th>
</tr>
</thead>
</table>

1. Planning and Scoping the Audit

1.1 Define audit/assurance objectives.
   - The audit/assurance objectives are high level and describe the overall audit goals.

1.1.1 Review the audit/assurance objectives in the introduction to this audit/assurance program.

1.1.2 Modify the audit/assurance objectives to align with the audit/assurance universe, annual plan and charter.

1.2 Define boundaries of review.
   - The review must have a defined scope. The reviewer must understand the operating environment and prepare a proposed scope, subject to a later risk assessment.

   1.2.1 Perform a high-level walkthrough of the processes related to cybercrime management.

   1.2.2 Establish initial boundaries of the audit/assurance review.

   1.2.2.1 Identify limitations and/or constraints affecting the audit.

1.3 Define assurance.
   - The review requires two sources of standards. The corporate standards defined in the policy and procedure documentation establish the corporate expectations. At minimum, corporate standards should be implemented. The second source, a good practice reference, establishes industry standards. Enhancements should be proposed to address gaps between the two.

   1.3.1 Determine if COBIT and the appropriate security incident management framework will be used as a good practice reference.

1.4 Identify and document risk.
   - The risk assessment is necessary to evaluate where audit resources should be focused. The risk-based approach assures utilization of audit resources in the most effective manner.

   1.4.1 Identify the inherent business risk associated with cybercrime threats.

   1.4.2 Identify the technology risk associated with cybercrime threats.
Figure 2—Maturity Model for Internal Control

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Status of the Internal Control Environment</th>
<th>Establishment of Internal Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Non-existent</td>
<td>There is no recognition of the need for internal control. Controls is not part of the organization’s culture or mission. There is a high risk of control deficiencies and incidents.</td>
<td>There is no intent to assess the need for internal control. Incidents are dealt with as they arise.</td>
</tr>
<tr>
<td>1 Initial/ad hoc</td>
<td>There is some recognition of the need for internal control The approach to risk and control requirements is ad hoc and disorganized, without communication or monitoring. Deficiencies are not identified. Employees are not aware of their responsibilities.</td>
<td>There is no awareness of the need for assessment of what is needed in terms of IT controls. When performed, it is only on an ad hoc basis, at a high level and in reaction to significant incidents. Assessment addresses only the actual incident.</td>
</tr>
<tr>
<td>2 Repeatable but Intuitive</td>
<td>Controls are in place but are not documented. Their operation is dependent on the knowledge and motivation of individuals. Effectiveness is not adequately evaluated. Many control weaknesses exist and are not adequately addressed; the impact can be severe. Management actions to resolve control issues are not prioritized or consistent. Employees may not be aware of their responsibilities.</td>
<td>Assessment of control needs occurs only when needed for selected IT processes. Determining the current level of control maturity, the target level that should be reached, and the gaps that exist. An informal workshop approach, involving IT managers and the team involved in the process, is used to define an adequate approach to controls for the process and to motivate an agreed-upon action plan.</td>
</tr>
<tr>
<td>3 Defined</td>
<td>Controls are in place and adequately documented. Operating effectiveness is evaluated on a periodic basis and there are an average number of issues. However, the evaluation process is not documented. While management is able to deal predictably with most control issues, some control weaknesses persist and impacts could still be severe. Employees are aware of their responsibilities for controls.</td>
<td>Critical IT processes are identified based on value and risk drivers. A detailed analysis is performed to identify control requirements and the root cause of gaps, and to develop improvement opportunities. In addition to facilitated workshops, tools are used and interviews are performed to support the analysis and ensure that an IT process owner owns and drives the assessment and improvement process.</td>
</tr>
<tr>
<td>4 Managed and Measurable</td>
<td>There is an effective internal control and risk management environment. A formal, documented evaluation of controls occurs frequently. Many controls are automated and regularly reviewed. Management is likely to detect most control issues, but not all issues are routinely identified. There is consistent follow-up to address identified control weaknesses. A limited, tactical use of technology is applied to automate controls.</td>
<td>IT process criticality is regularly defined with full support and agreement from the relevant business process owners. Assessment of control requirements is based on policy and the actual maturity of these processes, following a thorough and measured analysis involving key stakeholders. Accountability for these assessments is clear and enforced. Improvement strategies are supported by business cases. Performance in achieving the desired outcomes is consistently monitored. External control reviews are organized and conducted.</td>
</tr>
<tr>
<td>5 Optimized</td>
<td>An enterprise-wide critical control program provides continuous and effective control and risk issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management and compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analyses. Employees are proactively involved in control improvements.</td>
<td>Business changes consider the criticality of IT processes and cover any need to reassess process control capability. IT process owners regularly perform self-assessments to confirm that controls are at the right level of maturity to meet business needs and they consider high maturity attributes to find ways to make controls more efficient and effective. The organization benchmarks to external best practices and seeks external advice on internal control effectiveness. For critical processes, independent reviews take place to provide assurance that the controls are at the desired level of maturity and working as planned.</td>
</tr>
</tbody>
</table>

Source: ISACA IT Assurance Framework™ (ITAF™)
Source: ISACA IT Assurance Framework™ (ITAF™)
Resources

Cybersecurity Fundamentals Certificate
- Knowledge-based certificate offered by ISACA

Implementing NIST Cybersecurity Framework Using COBIT 5
- Focused on the CSF, goals, implementation steps and application
Cybersecurity Tool Talk for Auditors: Leveraging Free Information and Free Software

Auditor’s Guide to Cybersecurity Vulnerability and Penetration Testing

CyberAudits of Identity and Access Control Management

Simplifying Audits of Network Cybersecurity
Internal Audit Focus

- Evaluating security risk and threats
- Data at risk
- Secure infrastructure
- Monitoring capability
- Rapid identification, response, containment and recovery
Questions?

Sabrina Serafin
sabrina.serafin@frazierdeeter.com