Internal audit of cybersecurity

Presentation to the Atlanta IIA Chapter
January 2015
Agenda

Executive summary

Why is this topic important?
► Cyber attacks: increasing complexity
► Market insights: What are we seeing so far?
► Key risks associated with cybersecurity

What’s the fix?
► Cybersecurity: what organizations can do

How can Internal Audit help?
► Cybersecurity: internal audit review

EY Point of view
► Differentiators/tools/enablers
► Thought leadership
► Case studies

What’s next?
Executive summary

Situation
► As the threat landscape rapidly changes and risks increase, companies need to change their mind-set and approach toward information security and privacy to address a new normal. They need to operate under the assumption that unauthorized users are accessing the company’s information technology (IT) environment on a daily basis – to assume “they’re in.”
► Several recent high-profile, front-page-headline cyber-attacks are serving as a wake-up call for the C-suite. In fact, executive and board-level awareness of cyber risk appears to be at an all-time high — and growing.

Complication
► Inadequate understanding of cybersecurity risks results in companies focusing their attention and spending on areas that do not reflect the greatest risks.
► Key cybersecurity risks at a broad level covering all business areas that may occur separately or have an overlap are:
  ► Censure and embarrassment
  ► Client loss
  ► Direct fraud
  ► Sabotage or disruption of business operations
  ► Cyber espionage

Solution
► Your organization should consider including the following in the portfolio of security projects:
  ► Hardening of web browser, laptop and mobile device configurations
  ► Further enhancement of application security assessment and developer training efforts
  ► A solid approach to security controls and monitoring of cloud applications and services
► You can work with management to prioritize cybersecurity risks and conduct audits that will provide management and the audit committee with an assessment of the controls and recommendations to enhance the control environment.
Why is this topic important?
Cyber attacks: increasing complexity

Unsophisticated attackers (script kiddies)
You are attacked because you are on the internet and have vulnerability.

Sophisticated attackers (hackers)
You are attacked because you are on the internet and have information of value.

Corporate espionage (insider)
Your current or former employee seeks financial gain from selling your intellectual property (IP).

State-sponsored attacks
Advanced persistent threat (APT)
You are targeted because of who you are, what you do, or the value of your IP.

Initial exploitation
Data exfiltration
Intelligence gathering
Privilege escalation
Command and control

State-sponsored espionage

Experimentation
Monetization
Corporate espionage
Attacker resource and sophistication

APT life cycle
Why is this topic important?
Market insights: what we are seeing so far?

60% of organizations see increased risk from using social networking, cloud computing and personal mobile devices at work.

But only 52% of organizations indicate data leakage is a top “new” increased risk.

87% of organizations believe the damage to reputation and brand is the most significant issue related to data loss.

Yet only 10% of respondents indicated that examining new and emerging trends is a very important activity for the information security function.

61% are not making policy adjustments or increasing security awareness to address these new threats.

Source: EY's Global Information Security Survey
Why is this topic important?

Key risks associated with cybersecurity

- **Physical environment**
  - Physical access to critical infrastructure is provided to unauthorized personnel.
  - Company assets are not properly safeguarded against environmental disruptions (natural disasters, man-made catastrophes and accidental damage).

- **Governance and strategy**
  - Strategy is not aligned to business requirements.
  - Policy lacks cybersecurity robustness to protect against current and upcoming threats to production availability, integrity and information confidentiality.

- **Logical access**
  - Users are provided with inappropriate access to systems and data.
  - Systems have not been configured to provide an adequate level of logical security to prevent unauthorized access to programs and data.
  - Unauthorized software products are used to process business data.

- **Cybersecurity risks**
  - Attacks and malicious activity may not be detected.
  - The extent of damage from an attack may not be identified, contained or remediated.
  - Attacks and malicious activity may not be detected.

- **Outsourcing**
  - Vendors do not support security policies, leading to compromise of security controls or poor service levels.
  - Service levels are not defined or not aligned to business requirements.

- **Technical security**
  - Company assets are not properly safeguarded against environmental disruptions (natural disasters, man-made catastrophes and accidental damage).

- **Incident management**
  - Strategy is not aligned to business requirements.
  - Policy lacks cybersecurity robustness to protect against current and upcoming threats to production availability, integrity and information confidentiality.

- **Tangible benefits are not defined, resulting in non-profitable or non-strategic security projects being delivered.**

- **High risk**
  - High risk

- **Moderate risk**
  - Moderate risk
What’s the fix?
Cybersecurity: what organizations can do

In a hyper-connected world, no organization can be 100% secure. But organizations need to ensure that they are secure enough to protect customer information and intellectual property and avoid potential lawsuits, brand damage and loss of shareholder value.

| 1. Identifying and quantifying the real risks | The risk management life cycle is a process that: defines how the external threats specially apply to the company; estimates their potential business impact; defines the possible legal consequences; considers the risk management options based on a cost/risk reduction analysis; presents a prioritized financial-based set of risk management options for all relevant risks; makes a business decision based on the company’s risk tolerance; and executes the decision. |
| 2. Protecting what matters most | That means protecting the most important information that impacts your bottom line. Senior executives should champion a risk management strategy to protect business growth, brand and high-value data and systems, as well as improve processes that control liability by putting in place programs that help detect, deter and respond to breaches both internally and externally. |
| 3. Sustaining an enterprise-wide program | The management of technology risks needs to be a board-level priority, where executives understand that well-established risk management practices need to be applied to security-related risks. |
| 4. Optimizing for business performance | Aligning all aspects of technology risks with the business, including information/cybersecurity, privacy, and physical and business continuity/resiliency, will not only protect the bottom line, it will also generate cost efficiencies and improve performance. |
| 5. Enabling business performance | Safeguarding against cyber breaches and protecting the organization’s critical assets should not be only IT’s responsibility. It is rapidly emerging as a board fiduciary responsibility. And when done well, the proposed enterprise-wide program can enable business performance through faster product launches, more effective customer communication and higher-quality information for decision-making. |
# How can Internal Audit help?

## Cybersecurity: internal audit review

<table>
<thead>
<tr>
<th>Scope</th>
<th>Objective and areas covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance and processes</td>
<td><strong>Objective:</strong> Identifying gaps in the policies and procedures implemented in the organization pertaining to information security and IT infrastructure and the associated risks  &lt;br&gt; <strong>Areas covered:</strong>  &lt;br&gt; - Review the cybersecurity policies, procedures, guidelines and strategies  &lt;br&gt; - Testing of operating effectiveness as per the policies and procedures established in the organization on sample basis for the IT processes  &lt;br&gt; - Security operations – log analysis, event monitoring, antivirus management  &lt;br&gt; - End user security awareness and training</td>
</tr>
<tr>
<td>Network architecture and security review and behavioral analysis</td>
<td><strong>Objective:</strong> Assessment of network architecture to evaluate whether the security architecture supports the client’s thresholds for risk, while still supporting key business objectives  &lt;br&gt; <strong>Areas covered:</strong>  &lt;br&gt; - Review of security architecture and devices  &lt;br&gt; - Network topology and zoning  &lt;br&gt; - Log-in procedures and authentication requirements  &lt;br&gt; - Behavioral analysis of the existing network infrastructure  &lt;br&gt; - Assessment of vulnerabilities pertaining to protocol</td>
</tr>
<tr>
<td>Proactive APT review</td>
<td><strong>Objective:</strong> Mitigation of the risk of information leakage and eavesdropping and used to foresee the expected attacks and threats that the network might be subjected to  &lt;br&gt; <strong>Areas covered:</strong>  &lt;br&gt; - Root cause analysis  &lt;br&gt; - Deep packet inspection  &lt;br&gt; - Malware identification  &lt;br&gt; - Code-based malware analysis (static analysis)  &lt;br&gt; - Behavioral analysis (dynamic analysis)</td>
</tr>
</tbody>
</table>
### How can Internal Audit help?
#### Cybersecurity: internal audit review

<table>
<thead>
<tr>
<th>Scope</th>
<th>Objective and areas covered</th>
</tr>
</thead>
</table>
| **Baseline security review**       | **Objective**: Identifying security risks in the network  
**Areas covered**:  
- Redundancy testing for security related network components to ensure secure communication over the network, along with the assessment of perimeter security of the network  
- Vulnerability analytics  
- Conduct of penetration test of the network and servers from internal and external network  
- Review of security patch upgrades on all end user and server systems  
- Review of licenses and inventory of all vendor-specific applications (S/W assets) operating in the organization  
- Review of baseline configuration of all OS and DB deployed |
| **Cyber attack identification and response** | **Objective**: Evaluating procedures and processes that enable discovery and reporting of cyber attack incidents  
**Areas covered**:  
- Response team  
- Reporting  
- Investigation  
- Recovery and follow-up  
- Law enforcement |
| **Vulnerability identification and mitigation** | **Objective**: Help discover the vulnerability exploited and the associated application so that the appropriate fix can be applied to the infected part and stringent steps can be taken to strengthen the capability to combat such attacks  
**Areas covered**:  
- Identification of exploited vulnerability using analysis (code-based and behavioral) of captured malware  
- Identification of exploited applications  
- Deployment of security fixes, patches and updates of the exploited vulnerability  
- Antivirus signature preparation against the captured malware |
EY has developed a detailed information security maturity model that fully covers a cybersecurity maturity assessment. All elements in the overall security model are applicable when assessing the maturity of security from a cyber risk perspective as defined and requested by the client (“cyber risk is defined as any risk that results from criminal threats towards data and/or applications”).

Our model is based on security principles that combine the process, people and technology an organization uses to establish, implement, operate, monitor, review, maintain and improve its cybersecurity program within the context of its overall business objectives and activities.

The cyber risk maturity model is proprietary and is based upon the experience gained from undertaking multiple cyber risk maturity assessments with a range of clients across multiple sectors. The overarching framework used for the maturity model is depicted on the right.

The model makes use of standards such as ISO and ISF, but is flexible and can be adjusted to the client’s specific requirements.
## EY POV
### Our information security services for internal audits

- Information security services for internal audits include security data analytics and other services from our Advanced Security Centers (ASC) providing additional value to the client.
- Advanced Security Centers are EY-controlled environments based in the Americas, EMEIA and Asia-Pacific that host application/infrastructure testing facilities including hardware devices and simulators.
- Our center-based approach allows us to perform these services rapidly and cost-effectively.
- Globally, we conduct more than 600 vulnerability assessments a year and routinely serve multinational clients.
- We provide security testing during the pilot internal audits for applications/mobile devices and data privacy and security practices.

### EY’s information security services

<table>
<thead>
<tr>
<th>Service benefits</th>
<th>Advanced security centers</th>
<th>Large professional service firms</th>
<th>Security firms</th>
<th>Boutique firms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Focus in business risk</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Brand confidence</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Diverse industry knowledge combined with technical expertise</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategic national and global locations, resources and knowledge</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full range of security and risk advisory services available with the firm</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proprietary tools</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Dedicated team specializing the testing</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack and penetration team critical mass and ability to scale</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Establishes security training offering</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Collaborative environment for knowledge sharing</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure physical center meeting Department of Defense standards and dedicated to testing</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### ASC services

- **Application assessments**
  - (Black box, gray box and SDLC assessments)
  - Identify and manage risks
  - Validate security design and configurations
  - Data loss prevention and vulnerability assessments
  - Protect the availability and confidentiality of corporate, customer and personally identifiable information
## Cybersecurity case studies

### Information security transformation for a large health care company

<table>
<thead>
<tr>
<th>Business need</th>
<th>The client required external assistance on cyber threat preparedness and incident management process.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project scope</td>
<td>EY was engaged by the client to recommend measures to enhance its cyber threat readiness program and assist in the implementation of leading practices for its incident management process.</td>
</tr>
</tbody>
</table>
| Services provided | Performed cyber threat readiness assessments and penetration testing over areas such as research computing clusters, high risk/classified network areas, high-priority patients and domain trusts.  
  - Launched a security operations center (SOC) to investigate and respond to security incidents.  
  - Developed formal processes with defined incident response procedures, malware investigation handbook and incident escalation criteria.  
  - Implemented privileged credential partitioning via new hardened architecture to impede domain administrator compromise and theft of user domain password credentials. |

### Enterprise attack and penetration testing for a global oil and gas company

<table>
<thead>
<tr>
<th>Business need</th>
<th>The client required external help in identifying vulnerabilities through attack and penetration testing.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project scope</td>
<td>EY was engaged by the client to assess the security of its applications, networks and related infrastructure through the performance of attack and penetration services. The project included several assessment areas including web applications, wireless and IP telephony networks, physical security and phone social engineering.</td>
</tr>
</tbody>
</table>
| Services provided | Assisted the client’s security team on a daily basis in communicating and explaining the identified vulnerabilities and risks to application owners.  
  - Identified high-risk vulnerabilities in the client’s key information systems.  
  - Provided tactical and strategic recommendations to remediate vulnerabilities and address root cause. |
EY has made numerous contributions to public thought leadership in the areas of cybersecurity. Please feel free to view our electronic resources online at www.ey.com.

"Concerns about cybersecurity," BoardMatters Quarterly, April 2013

As the pace of technology evolution accelerates, so do cyber risks. Are you being proactive when addressing current threats – and those on the horizon?

Cybersecurity: considerations for the audit committee
Audit committee members increasingly list cybersecurity as a top concern. This EY report explores the issue and provides questions for the audit committee to consider.

Cybersecurity: how safe is your smart grid?
Power and utility companies face increased risk of cyber attack through convergence of real-time operational technology (OT) and enterprise IT environments, and initiatives such as the smart grid and advanced metering (AMI) technology. The article describes measures to secure operational environments from attack.

CFO: need to know
Cybersecurity demands the attention of more than just the CIO, because it's more than “just a technology issue.” The company is not impervious to attack – it probably already has been hacked. The article explains that cybersecurity poses broad risks, and countering it requires a broad perspective.
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

About EY’s Advisory Services

Improving business performance while managing risk is an increasingly complex business challenge. Whether your focus is on broad business transformation or more specifically on achieving growth, optimizing or protecting your business having the right advisors on your side can make all the difference. Our 30,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and exceptional client service. We use proven, integrated methodologies to help you solve your most challenging business problems, deliver a strong performance in complex market conditions and build sustainable stakeholder confidence for the longer term. We understand that you need services that are adapted to your industry issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where your strategy and change initiatives are delivering the value your business needs.

© 2014 Ernst & Young LLP. All Rights Reserved.

BSC no. 1311-1162097

ED None

ey.com