Cybersecurity and internal audit

August 15, 2014
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
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.

---

Experimentation → Monetization → Attack risk and sophistication

Corporate espionage

State-sponsored espionage

APT life cycle

- Intelligence gathering
- Initial exploitation
- Data exfiltration
- Privilege escalation
- Command and control

---

Initial

Exploitation
Key risks associated with cybersecurity

- **High risk**
  - 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.
  - Vendors do not support security policies, leading to compromise of security controls or poor service levels.

- **Moderate risk**
  - Tangible benefits are not defined, resulting in non-profitable security projects being delivered.
  - Service levels are not defined or not aligned to business requirements.
  - 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.
  - Users are provided with inappropriate access to systems and data.
  - Attacks and malicious activity may not be detected.
  - The extent of damage from an attack may not be identified, contained or remediated.

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).

Unprotected systems may not be detected.

The extent of damage from an attack may not be identified, contained or remediated.
What can organizations 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.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Identifying and quantifying the real risks</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>2. Protecting what matters most</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>3. Sustaining an enterprise-wide program</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>4. Optimizing for business performance</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>5. Enabling business performance</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
# How can internal audit help?

<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?

<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 |
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 or 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. 1404-1239678

ey.com