5 Insights for executives

Technology risk management in a cyber world
A C-suite responsibility

Of special interest to
Chief information security officer
Chief risk officer
“Our IT systems are as safe as Fort Knox,” an oil and gas company executive stated with absolute confidence. He firmly believed that his company’s data was secure and beyond the reach of would-be hackers. However, based on a cyber breach at several peers, the company decided to engage EY to examine its information security program – just to be sure.

Two days into an assessment of the organization’s network, the EY team discovered that an attacker from a foreign jurisdiction was stealing intellectual property. There was no logical reason for the information to be flowing in that direction. The executive who had so firmly attested to the security of the company’s network was not the only one surprised by the findings. The Board of Directors and Audit Committee were so taken aback by the breach that they mandated that the company completely rethink its approach to information security.

Senior executives acknowledge that information security and cyber threats exist, but often are in denial that it can happen to them. And worse, they often leave managing those threats to just the IT security department. Beyond the fear of a cyber breach is the emerging importance of effective technology risk management functions as an enabler to business performance by speeding product introductions and empowering employees to be able to safely use the latest IT trends, such as mobile and social media.

Cyber risks can impact shareholder value, tarnish the brand and expose the company to litigation. You can turn risk into results and enhance business performance, speed new product launches and provide more reliable business decision information through an enterprise technology risk management program. These are issues of importance to the C-suite, elevating the need for boards of directors, general counsels, chief risk officers and chief information security officers to understand and talk about their organization’s level of due care, approach and preparedness to address cyber risks.
What’s the issue?

Most companies don’t think that they are targets for cyber attackers. As the threat landscape rapidly changes and risks increase, companies need to change their mindset 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 IT environment on a daily basis – to assume “they’re in.” Cyber breaches can impact shareholder value, tarnish the brand and expose the company to litigation. These are issues of importance to the C-suite, elevating the need for boards of directors, audit committees, general counsels and chief risk officers to work alongside information security and privacy officers to fully address their organization’s risk management level of due care, approach and preparedness, and implement an Information Technology Risk Management (ITRM) program that is adequate and effective in managing cyber risks.

The US Government estimates American businesses suffered losses of intellectual property totaling more than $1 trillion from cyber attacks.

Why now?

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. Executives are realizing, sometimes painfully, that cyber risk needs to be addressed in the boardroom and become a more mainstream part of the enterprise risk management discussion.

As executives are becoming more aware, so too are governments. Unimpressed by the lack of reasonable care that organizations are exercising when it comes to protecting intellectual property and personally identifiable information, governments are introducing a wave of legislation at the federal and state level that will have an impact on business. The C-suite needs to be prepared, sooner rather than later, to respond to avoid costly errors made in times of crisis.

Now is the time to broadly address IT risk management at the C-suite, to proactively address business risks and maintain compliance, be prepared for cyber breaches and enable technology to enhance business performance.
How does it affect you?

Implementing an effective ITRM program that addresses cyber risk begins with understanding the roles that each member of the C-suite needs to play.

- **Board of Directors/Audit Committee.** The Board is responsible for setting an adequate standard of due care and ensuring its execution through its oversight mandate. The Board, through an Audit, Risk and/or Technology Committee, should review the IT risk posture of the organization at least annually. In keeping with recent SEC guidance, the Board and Audit Committee should determine the nature and extent of the requested cyber risk and incident disclosures, if any.

- **Chief risk officer (CRO).** Responsibilities range from overseeing the development and implementation of an ITRM program to monitoring and measuring its performance and effectiveness against the standard of due care set by the Board. An effective ITRM program is broader than cyber risks and information security, addressing the entire IT risk universe (e.g., business risk, cloud, social, mobile, change management).

- **General counsel (GC).** In the event of a cyber compromise, the GC needs to act quickly to minimize the impact of the breach. The GC’s office should be part of a breach response plan in place that includes an external communications plan that has been tested to ensure effective execution in a time of crisis. The GC will need to be prepared to respond carefully to authorities such as the FBI, and to draft responses to subpoenas for evidence that demonstrate a reliable forensic chain of custody.

- **Chief information officer (CIO) and Chief information security officer (CISO).** The CISO function is typically responsible for developing and testing a cyber incident response program, and should oversee a company-specific threat assessment that analyzes the potential targeted assets and the resulting business impact. The CIO and CISO should work with the CRO to ensure that tactics are effectively mitigating the broader IT risk landscape. CISOs should be transitioning traditional information security functions to be IT risk management functions.

<table>
<thead>
<tr>
<th>Function (stakeholder)</th>
<th>Technology risk management for cyber threats</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Govern (ongoing)</strong></td>
<td>Respond (incident and breach)</td>
</tr>
<tr>
<td>Board/ Audit Committee</td>
<td>• Set standard of due care</td>
</tr>
<tr>
<td></td>
<td>• Periodically evaluate cyber risk governance and review annual cyber risk assessment</td>
</tr>
<tr>
<td></td>
<td>• Issue cyber risk disclosures as per SEC guidance</td>
</tr>
<tr>
<td>Risk management (e.g., CRO)</td>
<td>• Oversee ongoing ITRM program for cyber risks</td>
</tr>
<tr>
<td>Legal (e.g., GC)</td>
<td>• Develop cyber risk legal response strategy</td>
</tr>
<tr>
<td></td>
<td>• Approve cyber breach response program</td>
</tr>
<tr>
<td>Information security (including incident response team) (e.g., CISO)</td>
<td>• Build threat mitigation program to plan/ protect most critical assets</td>
</tr>
<tr>
<td></td>
<td>• Establish incident, investigation and forensics response program; conduct tests</td>
</tr>
</tbody>
</table>
What's the fix?

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.

Actions the C-suite will need to consider include:

Identifying and quantifying the real risks.
The technology risk management lifecycle is a process that: defines how the external threats specifically 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.

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.

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.

Optimizing for business performance.
Aligning all aspects of technology risks with the business, including information/cyber security, privacy, and physical and business continuity/resiliency, will not only protect the bottom line, it will also generate cost efficiencies and improve performance.

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.
What's the bottom line?

Cyber attacks, incidents and breaches are not on the decline; they are on the rise. Hackers’ motives for targeting a company are expanding and might surprise you. The threats are internal and external, and they impact disclosure obligations, regulatory compliance and business performance. You should develop strategies and tactics as if unauthorized users are in your IT environment — assume “they’re in.” Now is the time for all senior executives at the highest levels of the organization to work together to establish a new mindset and approach toward an enterprise-wide ITRM program, including processes before, during and after a cyber breach. Effective IT risk management processes and technologies can enhance business performance, empowering employees and improving customer connections.
Want to learn more?

The answers in this issue are supplied by:

Bernie Wedge
Americas ITRA Leader
Ernst & Young LLP
+1 404 817 5120
bernard.wedge@ey.com

Dan Casciano
Americas IT Risk Management Leader
Ernst & Young LLP
+1 336 605 7801
daniel.casciano@ey.com

Jose Granado
Americas Information Security Leader
Ernst & Young LLP
+1 713 750 8671
jose.granado@ey.com

For related thought leadership, visit www.ey.com
We want to hear from you!
Please let us know if there are subjects you would like insights for executives to cover.
You can contact us at:
fiveseries.team@ey.com