You could be under cyber attack – now!
Addressing the threats you know isn’t enough. Information security needs to focus on the risks on the far horizon.

Of special interest to
Chief information officers
Chief information security officers
Chief technology officers
In the time it takes you to read this article, a significant percentage of you will suffer a cyber attack that breaches your organization’s security perimeter. It could be weeks before you find out and even longer before you can assess the extent of it. The attacker has probably been roaming around your network for months — undetected. And the associated costs of the breach may be staggering.

In Under cyber attack: EY’s Global Information Security Survey 2013, we find that many organizations have made significant progress in the last 12 months to improve their defenses against cyber attacks. However, their positions remain reactive. They are addressing only the risks they know without seeking to understand the risks that are lurking around the corner.

Leading organizations appear to be more proactive and expansive in their efforts to combat cyber threats. However, to be a cybersecurity innovator, organizations must set their sights on the far horizon. Innovating requires a fundamental transformation of the information security program to proactively fortify against both the known and the unknown risks in the cyber risk environment.
What’s the issue?

According to our survey, more organizations recognize the extent and depth of the threats they face — from the top of the organization to the shop floor. Information security is now seen as vital to the ongoing health of the organization. This is exemplified by the 70% of organizations whose information security policies are now owned at the highest organizational level.

Driven by board-level leadership or by fear, organizations seem to be making improvements in a number of areas:

Yet, for every step organizations are taking in the right direction, there remain miles to go:

- 68% of respondents state business continuity and disaster recovery as their top two priorities.
- 46% of organizations indicate that information security budgets are on the rise.
- 46% of spend will be directed toward security improvement, expansion and innovation in the next 12 months.
- 50% of organizations align their information security strategy to the organization’s business strategy.
- 65% of respondents cite budget constraints as their number one obstacle to delivering value to the business.
- 31% still do not have a threat intelligence program; 34% have an informal program.
- 62% of organizations have not aligned their information security strategy to their risk appetite or tolerance.
- 50% of respondents cite a lack of skilled resources as a barrier to value creation.

As the rate and complexity of cyber attacks continue to increase, organizations need to act quickly to avoid leaving themselves exposed to a costly and brand-damaging security incident that shakes the confidence of consumers and shareholders.
Why now?

Although organizations are making good progress in improving how they manage the risks that they already know, with only 17% of respondents indicating that their information security function fully meets the needs of the company, they still have a long way to go.

And time is running out. The volume of cyber risks that organizations don’t know about, particularly when it comes to emerging technologies that are just around the corner or appearing on the horizon, is growing at a rate too fast for many organizations to keep up.

How does it affect you?

As new technologies drive marketing and customer-oriented initiatives, information security chases associated cyber threats from behind. Mergers and acquisitions, structural changes within the organization and entrance into new markets all place additional stress on the information security function to provide adequate protection.

These pressures will only increase as the pace of emerging technologies continues to accelerate – as will the cyber risks. Not considering these risks until they arise gives cyber attackers an advantage that can be disastrous for the organization. To understand the impact, we need only to think of recent high-profile attacks on well-known brands that have had serious negative financial and reputational consequences.

“If you have fallen behind, have two-way discussions with the business and IT – not to roadblock, or own or control, but to get things moving and make things happen.”

— Retail and wholesale organization
What's the fix?

Where average organizations are making improvements in the risk areas they know, leading organizations are doing more. We have grouped 10 risk areas into four categories where we see leading organizations expanding improvement opportunities.

Acting on these opportunities for improvement will enable organizations to more proactively respond to know cyber risks and anticipate unknown ones. However, to be a cyber threat innovator, organizations need to reach well beyond these leading practices. Innovators must constantly scan the horizon, searching for the vulnerabilities in each opportunity emerging technology brings.

<table>
<thead>
<tr>
<th>1. Commitment from the top</th>
<th>Board support. Organizations need executive support to establish a clear charter for the information security function and a long-term strategy for its growth.</th>
</tr>
</thead>
</table>
| 2. Organizational alignment | Strategy. Information security must develop strong, clearly defined relationships with a wide range of stakeholders across the business and establish a clearly defined and formalized governance and operating model.  
Investment. Organizations need to be willing to invest in cybersecurity. |
| 3. People, processes and technology to implement | People. Today’s information security function requires a broad range of capabilities with a diversity of experiences. Technical IT skills alone are no longer enough.  
Processes. Processes need to be documented and communicated, but information security functions also need to develop change management mechanisms to quickly update processes when opportunities for improvement arise.  
Technology. To gain the most value from a technology solution, information security functions must supplement their technology deployment efforts with strategic initiatives that address proper governance, process, training and awareness. |
| 4. Operational enablement | Continuous improvement. Organizations must establish a framework for continuously monitoring performance and improving their information security programs in the areas of people, process and technology.  
Physical security. Organizations should ensure that all their information security technology is physically secure, especially with consideration for access to Wi-Fi. A security operations center can enable information security functions to respond faster, work more collaboratively and share knowledge more effectively.  
Analytics and reporting. Signature and rule-based tools are no longer as effective in today’s environment. Instead, information security functions may wish to consider using behavior-based analytics against environmental baselines.  
Environment. Information security requires an environment with a well-maintained enterprise asset management system (which includes criticality of supported business processes) to manage events associated with business priorities and assess the true risk or impact to the organization. |
What's the bottom line?

As our 2013 Global Information Security Survey suggests, organizations are improving their response to known cyber threats.

Unfortunately, too often information security continues to be viewed as a compliance exercise. To be a leader in information security, organizations need to place more emphasis on improving employee awareness, increasing budgets and devoting more resources to innovating security solutions. They need to look at the leading practices and consider how they can be applied to their business.

However, to be an information security innovator — a pioneer that sets its sights on the risks they are only just appearing on the far horizon — organizations have to do much more. They need to be prepared to fundamentally transform their information security programs where necessary.

In all instances, leadership is the key. After all, when it comes to cracking the information security code, 80% of the solution is not technical – it’s a case of good governance.
“New technologies will create new issues you have to think about in advance.”

— Professional services organization

Want to learn more?

For related thought leadership, visit ey.com/5.
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

Are you under cyber attack?
You could be right now and not even know it. Learn more about the steps you should take at ey.com/giss.