Insights on
governance, risk
and compliance

October 2014

Cyber program management

Identifying ways to get ahead of cybercrime

EY
Building a better
working world

> “We fight off 50,000 cyber attacks every day.”
>
> *CEO, global energy organization*

Contents

An existential threat

Business depends on technology. Digital systems are now the lifeblood of an organization: but they also have the potential to bring about its demise.

Reported breaches of information security are rising annually by 50%. This isn't sensationalism. Government security experts have coined the term "cyber fatality" to mean a digital breach that puts a company out of business.

It's not hard to see why cybercrime is accelerating and expanding. From the hacker or cyber criminal's point of view, the risks are limited, the potential rewards high: and in some territories, government sponsorship of cybercrime means hackers get paid for just trying. Turning to digital crime is an easy calculation.

This is scarcely news to any business leader today. But as our latest *Global Information Security Survey*[1] makes clear, organizations are still struggling to deliver the right response to the mounting risks.

The best-prepared businesses now recognize that responsibility for deflecting cyber attacks is no longer just the responsibility of their IT departments; it is an enterprise-wide boardroom issue. The only sure way to counter the threat is with an approach that roots the organization's cybersecurity strategy in the real world of its business strategy.

One of the most common questions we hear regarding security is "is this really necessary for us?" That's why we have we prepared this report to help board members and C-level decision makers understand the relationship between your responsibility, the scale of cyber threat, and a suggested approach that's sharply focused on your business structure, culture and risks.

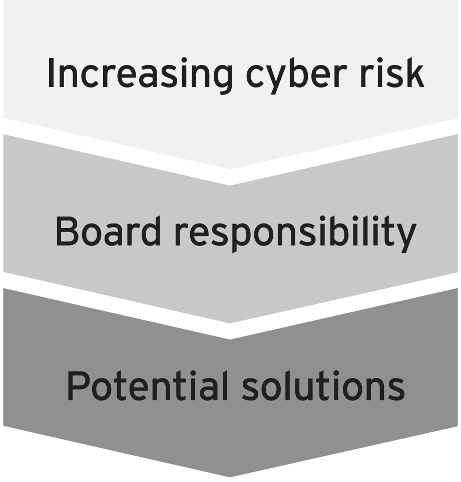
> The question is not "if" your company will be breached, or even when. It has already happened. The real questions are: is your organization aware of it, and how well are you protected for the future?

This report covers:

Increasing cyber risk
The growing complexity and speed of cybersecurity risks, what they mean to the organization and the response gap.

Board responsibility
The current state of C-level engagement in cybersecurity, and the challenges of integrating risk management into strategic planning.

Potential solutions
The advantages of adopting a holistic cyber program management approach to information security, based on meaningful analytics.



Increasing cyber risk

Board responsibility

Potential solutions

[1] *Get ahead of cybercrime: EY's Global Information Security Survey 2014*

The exponential rise in attacks

The importance of staying ahead of cybercrime

As cybersecurity threats evolve with unparalleled speed, complexity and impact, organizations are no longer asking "are we secure?" but "how can we ensure that the information most important to our business will be secure enough?"

In today's connected, information-heavy world, a startling new way of viewing the global business landscape is emerging. Given the mission-critical nature of data in nearly every aspect of modern enterprise – and the astonishing growth in the cyber criminals who seek to undermine it – organizations across all sectors are facing not simply escalating risk, but the near-certainty that they will suffer an information security breach.

In fact, the harsh reality of today's security environment means that they are likely to have experienced it already and that, therefore, there are only two kinds of organization: those that have been breached and know it, and those that remain dangerously oblivious.

This radical redrawing of the business landscape is a powerful wake-up call that should resonate around the boardroom table. With so much at stake – intellectual property; customer, operational and financial data; organizational reputation – informed leaders are realizing that it is time for a fundamental rethink of how information security is understood and positioned within their organizations.

It is no longer sufficient to treat it as a function of IT or other technical administration.

The historical focus of the cybersecurity team on operations and compliance still rings true. Two of the top four frameworks are ITIL (IT ops framework) and COBIT (audit framework), showing many companies are still taking the "doing what we're required" approach vs. "doing what we should" to protect the company.

While systems expertise remains an essential ingredient of preparedness, it is only when cybersecurity is understood within the organization's overall risk management structure that executive leadership can have confidence that their single most important business asset – information – is sufficiently protected against today's threats, and tomorrow's.

In a world of ever-evolving threats that can cause potentially catastrophic damage and may even one day lead to an organizational cyber fatality, better protection enables effective business performance and enhances a company's ability to operate day-to-day, while providing heightened resilience in the face of continually evolving threats.

Areas of focus for an organization's cybersecurity

- Architecture
- Asset management
- Awareness
- Business continuity management
- Data infrastructure
- Data protection
- Governance and organization
- Host security
- Identity and access management
- Incident management
- Metrics and reporting
- Network security
- Operations
- Policy and standards framework
- Privacy
- Security monitoring
- Software security
- Strategy
- Third-party management
- Threat and vulnerability management

The threat spectrum

The nature of digital security today is best understood from two perspectives: internal and external.

Internal threats

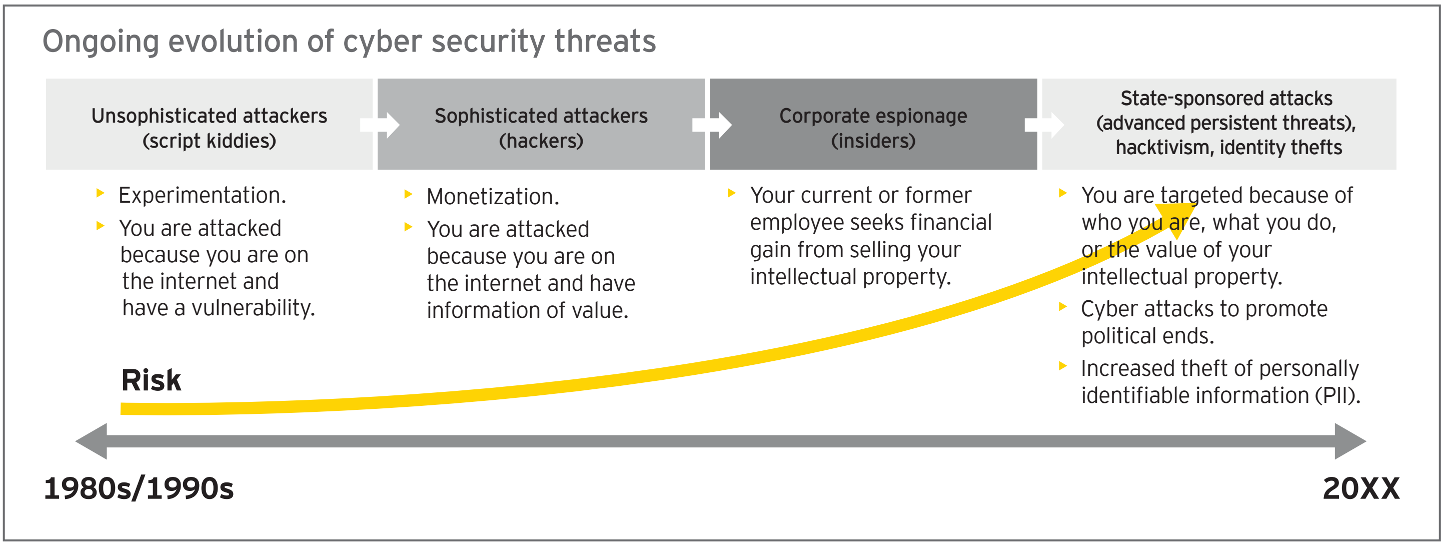
Internal threats to information security run from the inadvertent (simple user error, loss of mobile devices) to the malicious (internal fraud, data theft). As companies support productivity through the rapid integration of bring your own device (BYOD), cloud computing and other aspects of total mobility, there is a corresponding increase in the risk to which the information located on or accessed via these channels is exposed. Not only does the inherent accessibility of these systems breed vulnerabilities, but they also demand more and more complex processes of integration. As IT teams are forced to hang new systems on inadequate or insufficiently compatible existing frameworks, information security may be compromised – albeit unwittingly.

External threats

Hackers today are well-funded, persistent and sophisticated. People and processes are increasingly as much of a target as technology. Cyber criminals are motivated to evolve as quickly as possible; responses must be equally agile to keep pace.

56%

of respondents say that it is "unlikely or highly unlikely" that their organization would be able to detect a sophisticated attack.



Ongoing evolution of cyber security threats

Unsophisticated attackers (script kiddies)

- Experimentation.
- You are attacked because you are on the internet and have a vulnerability.

Sophisticated attackers (hackers)

- Monetization.
- You are attacked because you are on the internet and have information of value.

Corporate espionage (insiders)

- Your current or former employee seeks financial gain from selling your intellectual property.

State-sponsored attacks (advanced persistent threats), hacktivism, identity thefts

- You are targeted because of who you are, what you do, or the value of your intellectual property.
- Cyber attacks to promote political ends.
- Increased theft of personally identifiable information (PII).

Fast-evolving, multidimensional threats exist across all sectors

The exact risk spectrum varies by industry. A more strategic understanding of the value of data to the organization's ability to thrive is required, rather than just a focus on the performance of the network or platform.

Rapid consolidation through mergers and acquisitions means that many companies now operate across multiple industries and locations. An organization's security framework may be sufficient for its original sector or geography, but expansion calls for security measures to be reviewed in step.

It is not simply that the pace and complexity of change are accelerating, but that the severity of the impact is spiraling upward. The gap in an organization's ability to manage the pace of change is one problem, but the dangers of not doing so are more serious than ever before.

The response gap

Companies are increasingly reliant on digital data to drive their growth. The "bad guys" have recognized this, have fortified their techniques and are enjoying significant success; while the "good guys" are still trying to fight a modern war with bayonets! Having a well-defined security program can help management make an informed choice about how to invest in security. At a minimum, they need better insight about how key information assets are being protected, which is a role the information security function is well positioned to provide, better than internal audit and other risk/compliance-driven functions.

Investments in IT and related areas to address digital security may be misdirected. Companies have not adapted their view of security, as they are still identifying system availability as the top priority. Denial of service attacks are inconvenient, but theft of sensitive data can be crippling to leadership and costly to shareholders. The best controls to contain the damage of a cyber attack are often far down the priority list – i.e., high-value IP, managing privileged access and strong monitoring capability.

Organizations tend to overinvest in protecting IT assets while underinvesting in a full and strategic understanding of the nature of the threats most likely to derail their business objectives. One in four respondents (25%) to our *Global Information Security Survey 2014* (GISS)* said they had no program in place to identify vulnerabilities.

Even among those organizations that do understand and acknowledge the true nature of the threats that stand to cause them most harm, responses are often inadequate.

The weaknesses that expose organizations to increased risk fall into broad categories:

- Cybersecurity is misaligned within organizational priorities.
- Response frameworks are outdated or incomplete and remain too focused on IT.
- Solutions have traditionally relied on "bolt-on" upgrades and a multitude of heterogeneous security software products.
- Lines of accountability within organizations are unclear.
- Analytics are underutilized.

Many companies are reacting to what's being discussed in the media vs. the controls the attackers are focusing on. Companies need to identify where they're at risk and secure those areas before they move to emerging technologies that aren't being fully adopted by their business counterparts; for example, few companies are not using cloud or mobile for mission-critical data, just productivity apps and CRM. Over one third of companies aren't even looking at their internet-facing security posture – often the lowest hanging fruit for attackers – with 60% of companies not knowing the risk to their cloud-based internet-facing systems, as fewer than 10% of these systems have been tested in the last 12 months.*

Global organizations have the added complexity of managing cybersecurity across regions or sectors with different standards, leading to conflict and inconsistencies. Similarly, different enterprise units may also have security frameworks that collide or compete, as is so often the case in entities created through mergers and acquisitions.

The potential for cybercrime to strike a fatal blow has never been greater. Fast-growing and increasingly complex threats driven by external or internal adversaries are only exacerbated by systemic gaps. An entirely new approach to understanding organizational cybersecurity is needed to stay ahead of today's hackers.

**All survey statistics in this report refer to EY's 17th Global Information Security Survey 2014 which captures the responses of 1,825 C-suite leaders and information security and IT executives/managers, representing most of the world's largest and most-recognized global companies. Responses were received from 60 countries and across nearly all industries. For further information, please access: www.ey.com/GISS2014.*

The risk is increasing

Businesses across all sectors and geographies are dependent on an ever-increasing array of information systems – and on the technologies that enable them. Yet every technological advancement is as full of peril as it is of promise.

All the while that technological change gathers momentum and information becomes more critical to bottom-line activities, the speed and severity of security threats intensifies. The vast amount of global research on the prevalence of cybercrime reveals that almost every company has already suffered some form of information security breach – though by no means are all aware of it. What's more, the risk of a cyber attack is on the rise, as hackers become increasingly sophisticated, agile and well-funded.

Key findings in our GISS reveal an ominous concern among information security executives:

- 67% of responders see an increase in risk from external threats, while 53% report an increase in internal vulnerabilities.
- 31% report an increase of at least 5% in the number of security incidents experienced year over year.
- A little over a third of respondents (36%) report having no threat intelligence program to detect where cyber attacks are or may be coming from. Just under a third (32%) have only an informal program.

None of these trends should be news to most business leaders. Though some have made good inroads even in the last 12 months, many remain troublingly slow to see information security as a risk deserving the full engagement of senior level executives.

67%

have seen threats increasing in the last 12 months.

25%

of respondents said they have no program in place to identify vulnerabilities.

Report from the field: top-level engagement in cybersecurity

Each year, EY surveys information security executives around the world to uncover the key trends and emerging issues dominating their focus. Although our research reveals great strides in the highest organizational level taking ownership of information security, much more needs to be done:

- Less than half of respondents (49%) align their information security strategy with the organization's overall business strategy; more than half still align it with the IT strategy.
- Just 39% of respondents have aligned their information security strategy with their organization's risk appetite or tolerance.
- While 49% of respondents indicate that their information security budget has remained approximately the same over the last 12 months, 5% report a decrease in budget.

Get ahead of cybercrime: EY's Global Information Security Survey 2014

Why security gets sidelined by the Board

Cybercrime impact: stopping business in its tracks

The risks and vulnerabilities associated with today's technologies and information flows go well beyond conventional IT thinking. A cyber attack can affect the very ability of an organization to fulfill its mandate.

At best, security breaches are a costly distraction from core business activities; at worst, they can lead to catastrophic failure. In between lies a broad range of business impacts that threaten operations, production capabilities, customer and/or employee data, liability exposure and intellectual property, any one of which could jeopardize business continuity and integrity.

The potential for reputational damage – in the market, among shareholders and with partners – cannot be overstated. Yet when boards and senior leadership are unaware of the wider context of risk exposure, they remain recklessly oblivious to the very hazards they should be identifying and mitigating. Rather than let risks escalate, the matter of cybersecurity must be propelled to the boardroom: only here can it take its rightful place as an essential part of the organization's overall risk management strategy.

Competing demands, and an outdated understanding of the threats, crowd out the security discussion.

With so much at risk, why are C-level executives and their boards reluctant to tackle cyber-security? Reasons vary by organization, but most are rooted in these significant obstacles:

- **A crowded agenda**
  Cybersecurity is just one of many pressing issues demanding board-level engagement, particularly in a time of ongoing economic volatility.
- **The IT silo**
  Cybersecurity has traditionally been thought of as an IT issue that focuses on protecting the IT systems that process and store information, rather than on the strategic value of the information itself.
- **"Not our problem"**
  Cybersecurity has been seen as a significant problem only in select sectors such as the military or financial services. But if your sector relies on digital data to operate and compete, your information and IT systems are worthy of appropriate risk management.
- **Difficult to gauge**
  Unlike many types of organizational risk, cyber threats are hard to predict, making the risks and potential impact difficult to gauge. Senior leaders may feel they lack the expertise necessary to make enterprise-wide decisions or may be wary of being pulled too deeply into technical processes.
- **Invisible pay-off**
  In the face of competing demands for scarce resources, it can be hard for executive leadership to invest money, people and time in the unknown and unpredictable rather than in shareholder deliverables or more obvious needs.
- **Wrong priorities**
  Organizations have overinvested in preventative controls at the expense of detect/response capability.

What business leaders are asking about their cybersecurity readiness

The success of a sophisticated, effective cybersecurity strategy lies in the ability to look ahead to future opportunities and threats.

Executive leadership should consider whether the organization's security framework could respond to these issues:

Regulatory risk

- How will governments and regulators respond to the increasing threat of information risk?

Geopolitical shocks

- What is our organization's exposure to these shocks? How responsive is our IT organization?

Reputation risk

- How would a cyber attack affect our reputation and brand?

Control failures

- Could gaps or weaknesses in our IT controls and security be contributing factors?

Information risk

- How will our organization address the key risk areas of security, resilience and data leakage?

Expansion in emerging markets

- Does increasing our company's footprint add to the challenge of business continuity?

Reshaping the business

- How much would our information risk profile change?

Regulatory risk

- How will governments and regulators respond to the increasing threat of information risk?

Shared service centers

- Would using third parties or shared service centers increase risks to our security and IT sourcing?

IP and data security

- Is our organization covered against data leakage, loss and rogue employees?

Acquisitions and integration

- How successful are our organization's investments if we're unable to integrate the information belonging to an acquired company?

Hitting the headlines

- Hacktivists are ideological by nature. How might issues such as tax policy, pay and environmental management result in our company becoming a cyber target?

> Exhaustively trying to stop breaches is a waste of resources. Companies need to balance appropriate preventative controls with strong detective capabilities.

Success demands a holistic solution

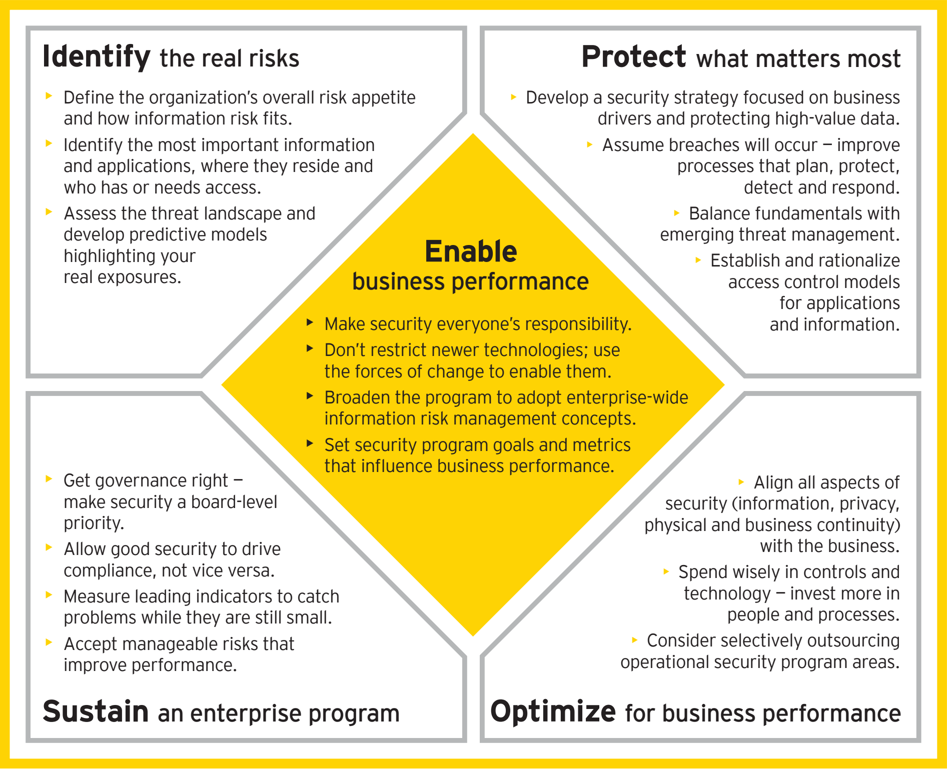
Leaders need to take a holistic approach to cybersecurity planning and management.

A sharp focus on your business structure, culture and risks will let you better safeguard the data essential to your organization's survival and success. For many, this requires a fundamental transformation in how information security is understood within the business. Creating a security program around intelligence on threats and also business risks will support resilience in a constantly shifting landscape of risk.

EY sees the advantages of a multi-tiered approach that ties security management to business performance:

- Better alignment to business objectives
- Increased readiness, scalability and flexibility
- Global cross-standard application
- Rigorous cycle of risk identification and management
- Future-focus to anticipate emerging challenges

Let business performance be your driver. These four goals connect your security strategy to business performance: **identify** the real risks; **protect** what matters most; **sustain** an enterprise program; **optimize** for business performance.



Identify the real risks

- Define the organization's overall risk appetite and how information risk fits.
- Identify the most important information and applications, where they reside and who has or needs access.
- Assess the threat landscape and develop predictive models highlighting your real exposures.

Protect what matters most

- Develop a security strategy focused on business drivers and protecting high-value data.
- Assume breaches will occur – improve processes that plan, protect, detect and respond.
- Balance fundamentals with emerging threat management.
- Establish and rationalize access control models for applications and information.

Enable business performance

- Make security everyone's responsibility.
- Don't restrict newer technologies; use the forces of change to enable them.
- Broaden the program to adopt enterprise-wide information risk management concepts.
- Set security program goals and metrics that influence business performance.

- Get governance right – make security a board-level priority.
- Allow good security to drive compliance, not vice versa.
- Measure leading indicators to catch problems while they are still small.
- Accept manageable risks that improve performance.

Sustain an enterprise program

- Align all aspects of security (information, privacy, physical and business continuity) with the business.
- Spend wisely in controls and technology – invest more in people and processes.
- Consider selectively outsourcing operational security program areas.

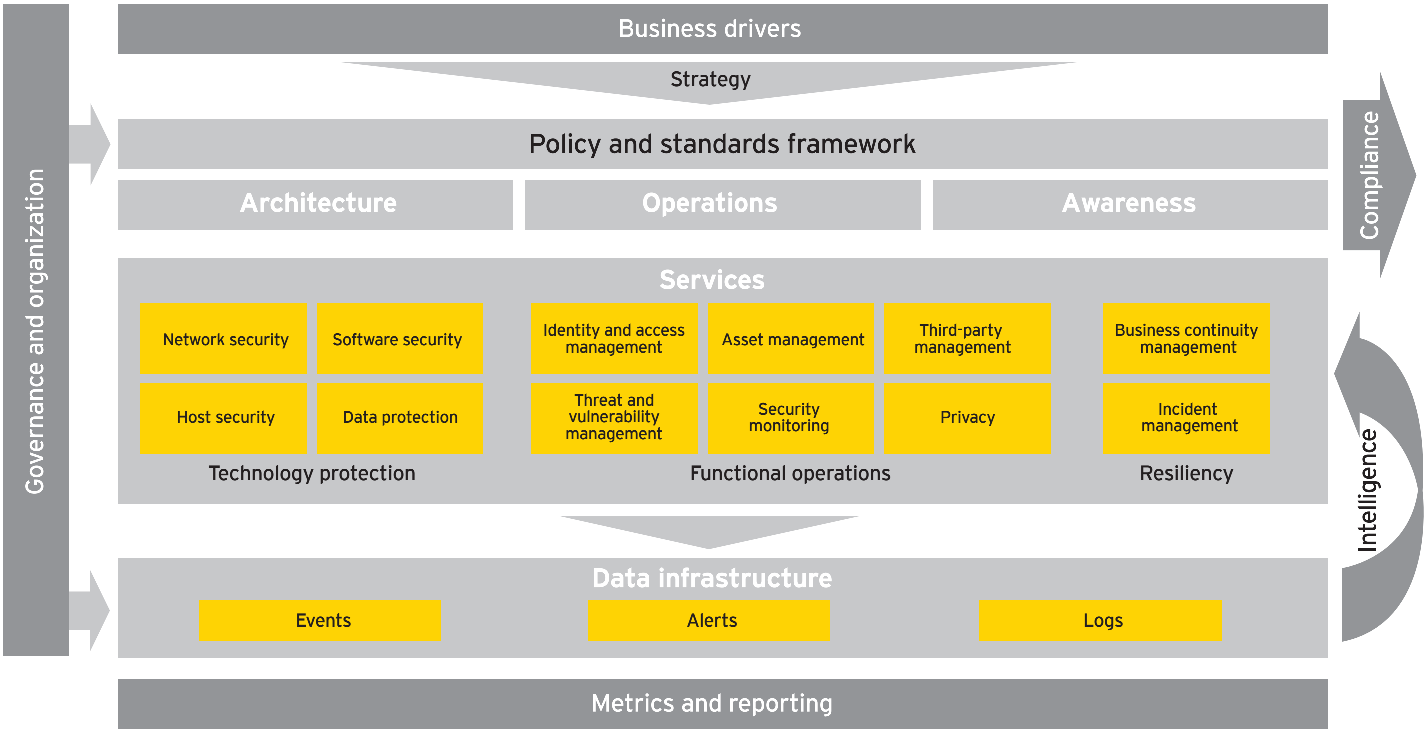
Optimize for business performance

A holistic approach based on meaningful analytics

Few companies today have the appropriate skills and resources in-house to effectively secure their information assets and at the same time optimize business performance. Organizations in all sectors can benefit from an objective assessment of their information security programs and structures.

EY's Cyber Program Management (CPM) framework is built upon a meaningful analysis of how information security shapes and fits into an organization's overall risk management structure. At its foundation is a clear focus on the organization's strategic priorities and business objectives *(see figure below)*.

EY's Cyber Program Management (CPM) framework



A CPM assessment assists with:

- Understanding your organization's risk exposure
- Assessing the maturity of your current cybersecurity program and identifying areas for improvement
- Building a prioritized road map for project investments and organizational change initiatives
- Collecting information to create benchmarks against other organizations
- Validating that your security investments have improved your security posture

Evaluating your cybersecurity program

EY's Cybersecurity Program Assessment has been developed by our Cybersecurity Advisory practice as a means of objectively evaluating any organization's security program.

Developed in conjunction with global leaders operating across multiple sectors and regions, and based on the domains of the CPM framework, the model will measure your program against 300 maturity assessment data points. You'll be able to see the "surface area" coverage of your program, how it compares to that of your peers and how much work is still left to do.

EY's proprietary, multi-tiered approach is tailored to your specific business environment. Consideration is given to your organization's structure, business objectives and the nature of the industry and region(s) in which it exists: this allows for a broad, high-level analysis as well as total immersion in specific areas and components.

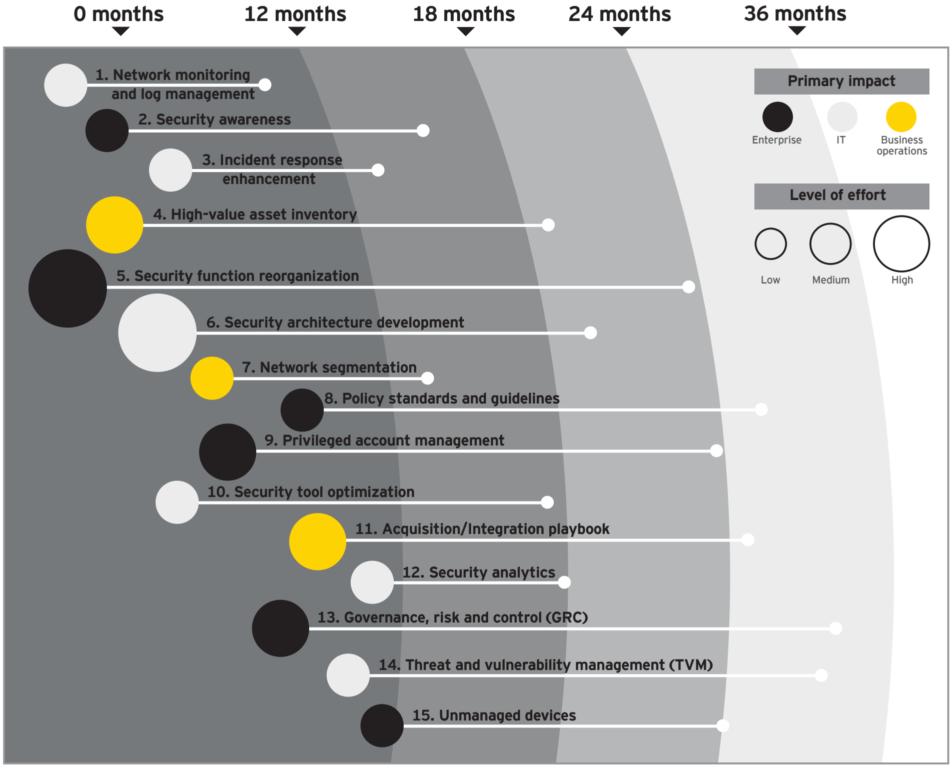
Dashboard metrics let you see at a glance what's needed to support the ongoing assessment, transformation and sustainability of the information security strategy. For example, maturity ratings *(see figure below)* help to position the organization along the relevant spectrum for its current, competitive and future states.

This and other assessment tools and benchmarking are designed to trigger meaningful analysis and actionable recommendations that can move your organization from its current state to the desired readiness. At the same time, you will better equip your organization to limit its exposure to unpredictable and ever-changing cyber threats.

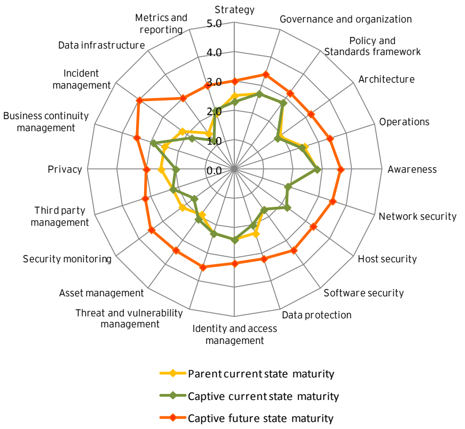
According to our GISS 2014 respondents:

- 36% do not have a threat intelligence program
- 25% do not have a vulnerability program
- 16% do not have a breach detection program
- 13% do not have an incident response capability
- 12% do not have an identity and access management program
- 8% do not have a data protection program

Cybersecurity Program Assessment



0 months
12 months
18 months
24 months
36 months
1. Network monitoring and log management
2. Security awareness
3. Incident response enhancement
4. High-value asset inventory
5. Security function reorganization
6. Security architecture development
7. Network segmentation
8. Policy standards and guidelines
9. Privileged account management
10. Security tool optimization
11. Acquisition/Integration playbook
12. Security analytics
13. Governance, risk and control (GRC)
14. Threat and vulnerability management (TVM)
15. Unmanaged devices
Primary impact
Enterprise
IT
Business operations
Level of effort
Low
Medium
High



An example of a maturity "spider graph" rating the cybersecurity requirements in an organization *(see page 2)*

Aligning security management to business performance

> CPM is the framework for the processes, people and technology that an organization uses to establish, implement, operate, monitor, review, maintain and improve a security program within the context of an organization's overall business objectives and activities.

CPM is a global cross-standard application, created with all the advantages of a multi-tiered approach, offering a rigorous cycle of risk identification and management. It provides your organization with a practical future-focused outlook to help you anticipate new challenges from emerging technologies and business trends.

CPM ties security management to business performance through better alignment to your strategic objectives by helping organizations to:

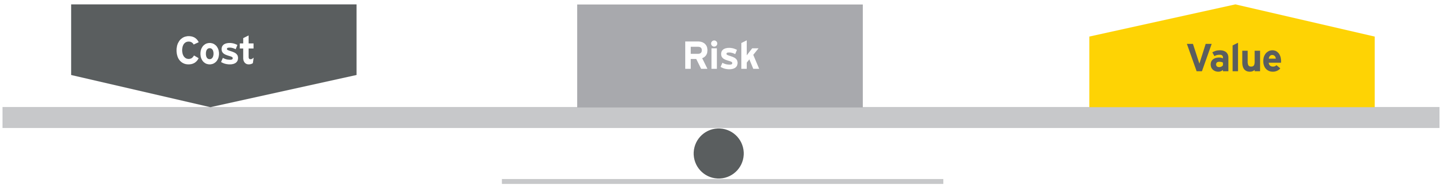
- Identify the real risks
- Protect what matters most
- Sustain an enterprise program
- Optimize for business performance
- Increase readiness, scalability and flexibility

CPM assessments are of special interest to the C-suite and audit committees of companies that: are unsure of their current risk exposure; are growing their cybersecurity team and are interested in a fresh perspective on how their current capabilities compare to others in their peer group; and are interested in investing in cybersecurity but are in need of project and spend prioritization. It can also provide invaluable insights to organizations that have recently experienced a public or private breach resulting in data loss, reputational damage and brand impairment.

CPM helps you balance cost, risk and value

A CPM assessment enables you to perform the balancing act of reducing costs while identifying gaps in existing security capabilities; the findings can help you make strategic prioritized investments to address business needs, increase company value and keep your organization secure.

Balancing cost, risk and value



Are our cybersecurity capabilities efficient and effective? Do we have the:

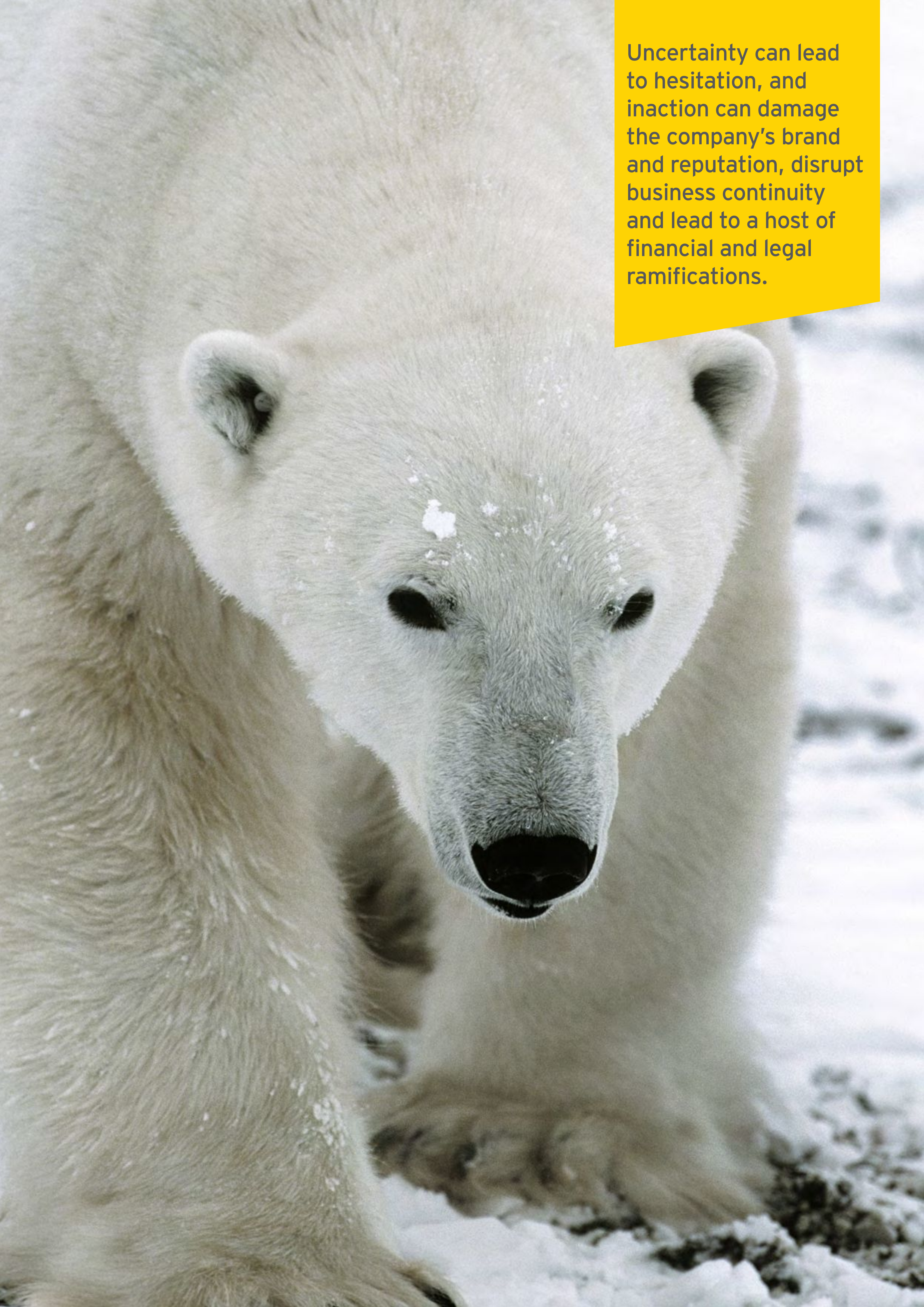
- Right resources?
- Right initiatives, processes and technologies?
- Right investments?

Does our cybersecurity program currently:

- Manage enterprise security risk?
- Adequately protect us from new and emerging threats?
- Identify gaps and remediate root cause security issues?
- Proactively respond to changes in the business and regulatory environment?

Will our cybersecurity program:

- Keep us competitive?
- Protect brand image and value?
- Protect assets of most importance to the organization?
- Enable new business initiatives?



Uncertainty can lead to hesitation, and inaction can damage the company's brand and reputation, disrupt business continuity and lead to a host of financial and legal ramifications.

Conclusion

Cybersecurity must be a board priority

Inadvertent loss of data or deliberate attack — either way, the security breach is an inevitable and recurring feature of today's global business landscape.

As traditional and digital worlds converge, security threats to business operations become increasingly complex. Emerging technologies, user mobility and the sheer volume of data exchanged daily all represent opportunities for hackers to target the digital assets that drive modern enterprise. One attack is all it takes to jeopardize an organization's stability, if not its very existence.

Most organizations struggle to keep pace with the breakneck speed at which technologies and threats evolve, giving rise to hazardous gaps emerging between risk and response. This leaves organizations wide open — not only to competitive disadvantage and potential collapse, but also to market, regulatory and stakeholder pressure to improve security governance.

In the face of such high stakes, successful business leaders will be those who transform their cybersecurity strategy by giving it due consideration and aligning it with core business objectives. A deeper understanding of known and unknown threats, business-critical information and how to cascade digital security effectively throughout the enterprise will be instrumental in improving and protecting business performance.

Elevating responsibility for shaping information security to the board level is imperative. Business leaders are best placed to mitigate cyber threats, downgrade breaches and ensure prosperity in today's borderless, data-driven business environment when cybersecurity runs throughout the risk management strategy of the entire organization, rather than intermittently alongside.

What role should the board play?

Informed leaders are realizing that it is time for a fundamental rethink of how cybersecurity is understood and positioned within their organizations. Cybersecurity should not be viewed as a prohibitor to fast-paced emerging technology and go-to-market strategies — when done right, it gives you a competitive advantage.

The company's board should set the tone for enhancing security and determine whether the full board or a committee should have oversight responsibility. In some cases, a risk committee, executive/operating committee or the audit committee will be given the oversight charge. These committees should be well informed about the company's processes, and they should leverage that information to understand whether management has the right people and processes in place.

Companies need to shift their mindset from being the hunted to being the hunters. Every company should establish a "red team" focused on identifying security weaknesses before the bad guys are able to do so. Companies should also establish a formal "team" that takes a diligent/regimented approach to detecting malicious activity. The goal: smart people supported by well-tuned technology following clearly defined processes.

Questions for the board

Is our cybersecurity focused on protecting the assets that make money for our company?

How well do we protect high-value information, especially given today's increasingly mobile workforce?

Is our cybersecurity strategy aligned with our business objectives?

How do we measure the effectiveness of our cybersecurity program?

Are we spending on the right security area priorities?

Would we know if we were the victim of a breach?

Is our cybersecurity function appropriately organized, trained, equipped, staffed and funded?

How does our program compare to industry peers?

Understanding the problems

Most board members are financially savvy, but they may lack a deep knowledge of technological issues and they therefore rely more heavily on the technology officers within the company to provide them with perspectives on IT risk management. Depending on the circumstances, some directors may want to consider bringing someone with a deep understanding of IT issues onto the board or audit committee.

While technology officers are able to provide data, such as the number of attempted breaches, it can be difficult to convert the data into meaningful information that could help leadership better understand the possible risks facing the organization. On top of that, board and audit committee members may not know how to evaluate the quality of the information they receive or ask the right follow-up questions. Cybersecurity should be discussed in the boardroom quarterly or more frequently.

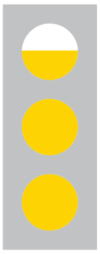
The historic approach of prevention is no longer valid. The board's approach needs to change to a posture of preparedness and proactive response: balancing focus on people, process and tools to help them get ahead of cybercrime.

Key considerations for the audit committee

It's important to gauge the pulse of the company's tolerance for risk and evaluate the decisions made by management over which gaps are tolerable.

Questions should include:

- Has the company experienced an increase in the number of cybersecurity breaches?
- What has the company done to bolster its cybersecurity program?
- Is information security an IT function within the company? If so, to whom does it report?
- Is there anyone on the board or audit committee with an IT background?
- Is the audit committee involved in planning to enable the better management of cybersecurity risks?
- How often does the committee discuss cybersecurity? Who presents that information to the board? Are they communicating the issues in ways that are understood?
- Does the audit committee seek or receive routine updates on risks and advancements in cybersecurity?



87%

of organizations feel that their cybersecurity function does not fully meet the organization's needs.

61%

of organizations have not aligned their cybersecurity strategy to their risk appetite or tolerance.

Want to learn more?

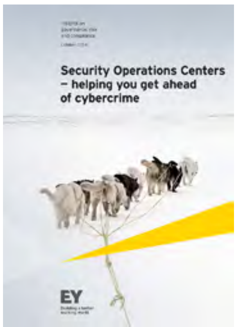
Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective.

Please visit our ***Insights on governance, risk and compliance*** series at ey.com/GRCinsights

Get ahead of cybercrime: EY's Global Information Security Survey 2014.
www.ey.com/GISS2014

Achieving resilience in the cyber ecosystem.
www.ey.com/cyberecosystem

Reducing risk with Cyber Threat Intelligence.
www.ey.com/CTI


Security Operations Centers – helping you get ahead of cybercrime
EY

Security Operations Centers – helping you get ahead of cybercrime.
www.ey.com/SOC

Privacy trends 2014: privacy protection in the age of technology.
www.ey.com/privacy2014

Maximizing the value of a data protection program.
www.ey.com/dataprotect

Identity and access management: beyond compliance.
www.ey.com/iam

Building trust in the cloud
Creating confidence in your cloud ecosystem
EY

Building trust in the cloud: creating confidence in your cloud ecosystem.
www.ey.com/cloudtrust

Big data: changing the way businesses compete and operate.
www.ey.com/bigdatachange

At EY, we have an integrated perspective on all aspects of organizational risk. We are the market leaders in internal audit and financial risk and controls, and we continue to expand our capabilities in other areas of risk, including governance, risk and compliance, as well as enterprise risk management.

We innovate in areas such as risk consulting, risk analytics and risk technologies to stay ahead of our competition. We draw on in-depth industry-leading technical and IT-related risk management knowledge to deliver IT controls services focused on the design, implementation and rationalization of controls that potentially reduce the risks in our clients' applications, infrastructure and data. Information security is a key area of focus where EY is an acknowledged leader in the current landscape of mobile technology, social media and cloud computing.

EY | Assurance | Tax | Transactions | Advisory

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.

EYG no. AU2699
ED none

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com/GRCinsights

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.

To find out more about how our Risk Advisory services could help your organization, speak to your local EY professional or a member of our global team, or view: ey.com/advisory.

Our Risk Advisory Leaders are:

Global Risk Leader		
Paul van Kessel	+31 88 40 71271	paul.van.kessel@nl.ey.com
Area Risk Leaders		
Americas		
Amy Brachio	+1 612 371 8537	amy.brachio@ey.com
EMEIA		
Jonathan Blackmore	+971 4 312 9921	jonathan.blackmore@ae.ey.com
Asia-Pacific		
Iain Burnet	+61 8 9429 2486	iain.burnet@au.ey.com
Japan		
Yoshihiro Azuma	+81 3 3503 1100	azuma-yshhr@shinnihon.or.jp

Our Cybersecurity Leaders are:

Global Cybersecurity Leader		
Ken Allan	+44 20 795 15769	kallan@uk.ey.com
Area Cybersecurity Leaders		
Americas		
Bob Sydow	+1 513 612 1591	bob.sydow@ey.com
EMEIA		
Ken Allan	+44 20 795 15769	kallan@uk.ey.com
Asia-Pacific		
Paul O'Rourke	+65 6309 8890	paul.orourke@sg.ey.com
Japan		
Shinichiro Nagao	+81 3 3503 1100	nagao-shnchr@shinnihon.or.jp