Beating cybercrime

Security Program Management from the board’s perspective

Insights on governance, risk and compliance

October 2013
An existential threat

Business depends on technology. Digital systems are now the lifeblood of your company. But they also have the potential to bring about its demise.

This isn’t sensationalism. Reported breaches of information security are rising annually by 50%. Government security experts have coined the term “cyber fatality” – meaning a digital breach that puts a company out of business.

It’s not hard to see why cybercrime is surging. Put yourself in the hacker’s shoes for a second. 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 makes clear, organizations are still struggling to deliver the right response to the mounting risks. In particular, they find it hard to align their security strategies with their real-world business strategies.

The best-prepared businesses now recognize that responsibility for deflecting cyber attacks can no longer be shunted off to their IT departments. This is a boardroom issue. The only sure way to counter the threat is with a strategic approach that roots your digital security in the real world of your business.

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 report covers:

**Increasing cyber risk**
The emerging cyber security risks, what they mean to your organization and the response gap (pages 2-5)

**Board responsibility**
The current state of senior engagement in cyber security, and the challenges of integrating risk management into strategic planning (pages 6-7)

**Potential solutions**
The advantages of adopting a holistic Security Program Management approach to information security, based on meaningful analytics (pages 8-12)
Increasing cyber risk

The exponential rise of risk

The importance of staying ahead of cybercrime

As cyber security 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 already have experienced it, and there may be only two kinds of organizations: those that have been breached and know it, and those that remain dangerously oblivious to it.

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; and organizational reputation – informed leaders are realizing that it is time for a fundamental rethink of how information security is understood and positioned within their organization.

It is no longer sufficient to treat it as a function of IT or other technical administration. While systems expertise remains an essential ingredient of preparedness, it is only when cyber security 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, as well as provides heightened resilience in the face of continually evolving threats.

Information security requirements in an organization:

- 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; defenses must be equally agile to keep pace.

---

### Ongoing evolution of cyber security threats

<table>
<thead>
<tr>
<th>Unsophisticated attackers (script kiddies)</th>
<th>Sophisticated attackers (hackers)</th>
<th>Corporate espionage (insiders)</th>
<th>State-sponsored attacks (advanced persistent threats), hacktivism, identity thefts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1980s/1990s</td>
<td></td>
<td></td>
<td>20XX</td>
</tr>
<tr>
<td>➤ Experimentation</td>
<td>➤ Monetization</td>
<td>➤ You are attacked because of who you are, what you do, or the value of your intellectual property</td>
<td></td>
</tr>
<tr>
<td>➤ You are attacked because you are on the internet and have a vulnerability</td>
<td>➤ You are attacked because you are on the internet and have information of value</td>
<td>➤ Cyber attacks to promote political ends</td>
<td></td>
</tr>
<tr>
<td>➤ Your current or former employee seeks financial gain from selling your intellectual property</td>
<td>➤ Increased theft of personally identifiable information (PII)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

### Fast-evolving, multidimensional threats exist across all sectors

The exact risk spectrum varies by industry. What is required is a more strategic understanding of the value of data in the ability of the organization to thrive, rather than the performance of the network or platform.

Rapid consolidation through mergers and acquisitions means that many companies now operate across multiple industries. 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.
The response gap

Investments in IT and related areas to address digital security may be misdirected. Organizations tend to over invest in protecting IT assets while under investing in a full and strategic understanding of the nature of the threats most likely to derail their business objectives. Almost one in four respondents (23%) surveyed 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:

- Digital security is misaligned within organizational priorities.
- Response frameworks are outdated, 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.

Global organizations have the added complexity of managing digital security 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 digital security is needed to stay ahead of today’s hackers.

Mike Trovato, EY Asia-Pacific Security Practice Leader

“It is not simply that the velocity and complexity of change is 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 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 EY’s Global Information Security Survey 2013 reveal an ominous concern among information security executives:

- 59% of the respondents cite an increase in risk from external threats while 9% report a risk in internal threats.
- 31% report an increase of at least 5% in the number of security incidents experienced year over year.
- Yet nearly a third of respondents (31%) report having no threat intelligence program to detect where cyber attacks are or may be coming from. A little over a third of respondents 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.

Report from the field: Top-level engagement in cyber security

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 (70%), much more needs to be done:

- Less than half of respondents (46%) align their information security strategy with the organization’s overall business strategy; more than half still align it with the IT strategy.
- Just 38% of respondents have aligned their information security strategy with their organization’s risk appetite or tolerance.
- While 43% of respondents indicate that their information security budget has increased, 65% of information security departments are still feeling the pinch.

---

1 Under cyber attack: EY’s Global Information Security Survey 2013
2 Ibid
Why security gets sidelined by the board

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**
  Information security is just one of many pressing issues demanding board-level engagement, particularly in a time of ongoing economic volatility.

- **The IT silo**
  Information security 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”**
  Cyber security 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.

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 digital security 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.
What leaders are asking about their cyber security readiness

The success of a sophisticated, effective cyber security 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?

**Shared services 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?

“In a mobile, borderless environment, the human is the new perimeter when it comes to protecting data. The approach to protecting the organization needs to combine people, processes and technology.”

Jose Granado, EY Americas Security Practice Leader
Potential Solutions
Success demands a holistic solution

Leaders need to take a holistic approach to information security 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.
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 innovative Security Program Management (SPM) 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 Security Program Management (SPM) framework

An SPM assessment assists with:

- Understanding your organization’s risk exposure
- Assessing the maturity of your current information security 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 security program

EY’s Security Program Assessment has been developed by our Information Security 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 SPM 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 functions. 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.

Security Program Assessment

<table>
<thead>
<tr>
<th>0 months</th>
<th>12 months</th>
<th>18 months</th>
<th>24 months</th>
<th>36 months</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Network monitoring and log management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Security awareness</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Incident response enhancement</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. High-value asset inventory</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Security function reorganization</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Security architecture development</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Network segmentation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Policy standards and guidelines</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Privileged account management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Security tool optimization</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11. Acquisition/Integration playbook</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12. Security analytics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13. Governance, risk and control (GRC)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14. Threat and vulnerability management (TVM)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15. Unmanaged devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Potential solutions

An example of a maturity “spider graph” rating the information security requirements in an organization (see page 2)
SPM — aligning security management to business performance

SPM 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.

SPM 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

SPM assessments are of special interest to the C-suite and audit committees of companies that: are unsure of their current information security risk exposure; are growing their Information Security 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 information security 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.

SPM helps you balance cost, risk and value

An SPM 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

<table>
<thead>
<tr>
<th>Cost</th>
<th>Risk</th>
<th>Value</th>
</tr>
</thead>
</table>

**Are our information security capabilities efficient and effective? And do we have:**
- Right resources?
- Right initiatives, processes and technologies?
- Right investments?

**Does our information security 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 information security 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.

Cyber security must be a board priority
Conclusion

Cyber security 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 information security 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 information security runs throughout the risk management strategy rather than intermittently alongside.

What role should the board play?

Informed leaders are realizing that it is time for a fundamental rethink of how information security is understood and positioned within their organization. Information security 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.

“With so much at stake – intellectual property, customer, operations and financial data, and organizational reputation – informed leaders are realizing it's time for a fundamental rethink of how information security is understood and positioned within their organization.”

Ken Allan, EY Global Leader, Information Security
Understanding the problems

Cyber security is not just a technology issue; it’s a business risk that requires an enterprise-wide response. Yet 62% of organizations who responded to the recent GISS said they have not aligned their information security strategy to the organization’s risk appetite and risk tolerance.

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 boards of 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. Still, only 34% of survey respondents said they discuss information security in the boardroom quarterly or more frequently.

Key considerations for the audit committee

Audit committees should ask questions about the state of specific security programs and then ask for benchmarks: how is the company doing relative to its competitors and the industry?

They should also ask for an explanation of the measures that are in place to prevent or detect attacks. 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 information security breaches? ?
- What has the company done to bolster its information security 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 information security risks? ?
- How often does the committee discuss cyber security? 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 information security? ?

62% of organizations have not aligned their information security strategy to their risk appetite or tolerance.

34% of information security professionals surveyed present information security to the board on each quarter or more frequently.
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

**Under cyber attack**: EY’s Global Information Security Survey 2013

**Security Operations Centers against cybercrime**: top 10 considerations for success
[www.ey.com/soc](http://www.ey.com/soc)

**Privacy Trends 2013**: the uphill climb continues

**Mobile device security**: understanding vulnerabilities and managing risk
[www.ey.com/mobiledevicesecurity](http://www.ey.com/mobiledevicesecurity)

**Protecting and strengthening your brand**: social media governance and strategy
[www.ey.com/protectingbrand](http://www.ey.com/protectingbrand)

**Information security in a borderless world**: time for a rethink
[www.ey.com/infosec_borderless](http://www.ey.com/infosec_borderless)

**Identity and access management (IAM)**: beyond compliance
[www.ey.com/iam](http://www.ey.com/iam)

**Bring your own device**: security and risk considerations for your mobile device program
[www.ey.com/byod](http://www.ey.com/byod)

**Key considerations for your internal audit plan**: enhancing the risk assessment and addressing emerging risks
[www.ey.com/iaplan](http://www.ey.com/iaplan)
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.
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 our IT Risk Advisory services could help your organization, speak to your local EY professional, or a member of our team.

The leaders of our RISK practice are:

**Global RISK Leader**

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paul van Kessel</td>
<td>+31 88 40 71271</td>
<td><a href="mailto:paul.van.kessel@nl.ey.com">paul.van.kessel@nl.ey.com</a></td>
</tr>
</tbody>
</table>

**Area RISK Leaders**

**Americas**

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jay Layman</td>
<td>+1 312 879 5071</td>
<td><a href="mailto:jay.layman@ey.com">jay.layman@ey.com</a></td>
</tr>
</tbody>
</table>

**EMEIA**

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jonathan Blackmore</td>
<td>+44 20 795 11616</td>
<td><a href="mailto:jblackmore@uk.ey.com">jblackmore@uk.ey.com</a></td>
</tr>
</tbody>
</table>

**Asia-Pacific**

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iain Burnet</td>
<td>+61 8 9429 2486</td>
<td><a href="mailto:iain.burnet@au.ey.com">iain.burnet@au.ey.com</a></td>
</tr>
</tbody>
</table>

**Japan**

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shohei Harada</td>
<td>+81 3 3503 1100</td>
<td><a href="mailto:harada-shh@shinnihon.or.jp">harada-shh@shinnihon.or.jp</a></td>
</tr>
</tbody>
</table>

The information security leaders within our RISK practice are:

**Global Information Security Leader**

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ken Allan</td>
<td>+44 20 795 15769</td>
<td><a href="mailto:kallan@uk.ey.com">kallan@uk.ey.com</a></td>
</tr>
</tbody>
</table>

**Area Information Security Leaders**

**Americas**

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jose Granado</td>
<td>+1 713 750 8671</td>
<td><a href="mailto:jose.granado@ey.com">jose.granado@ey.com</a></td>
</tr>
</tbody>
</table>

**EMEIA**

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ken Allan</td>
<td>+44 20 795 15769</td>
<td><a href="mailto:kallan@uk.ey.com">kallan@uk.ey.com</a></td>
</tr>
</tbody>
</table>

**Asia-Pacific**

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mike Trovato</td>
<td>+61 3 9288 8287</td>
<td><a href="mailto:mike.trovato@au.ey.com">mike.trovato@au.ey.com</a></td>
</tr>
</tbody>
</table>

**Japan**

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shinichiro Nagao</td>
<td>+81 3 3503 1100</td>
<td><a href="mailto:nagao-shnchr@shinnihon.or.jp">nagao-shnchr@shinnihon.or.jp</a></td>
</tr>
</tbody>
</table>

ey.com/GRCinsights