

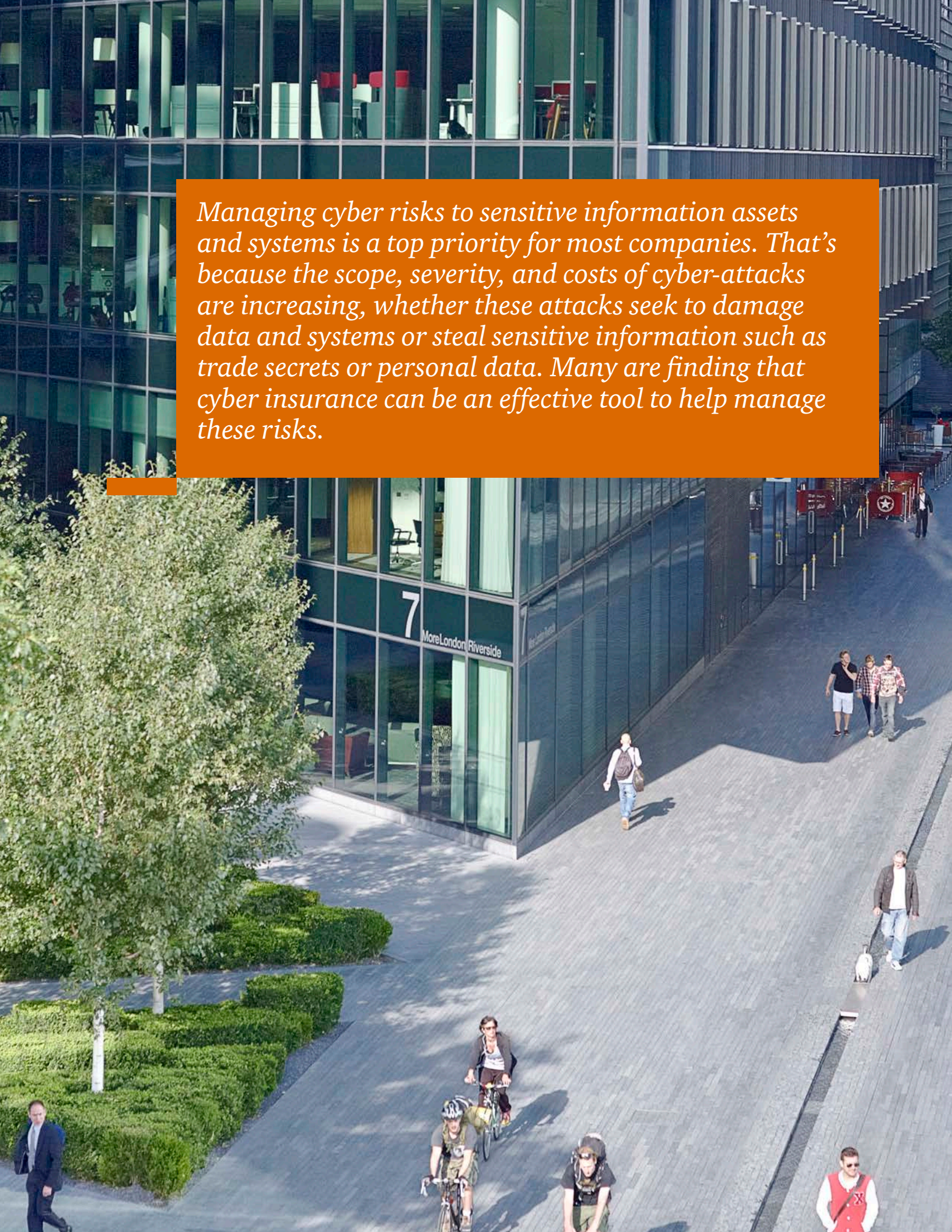
# ***Managing cyber risks with insurance***

Key factors to consider  
when evaluating how cyber  
insurance can enhance your  
security program

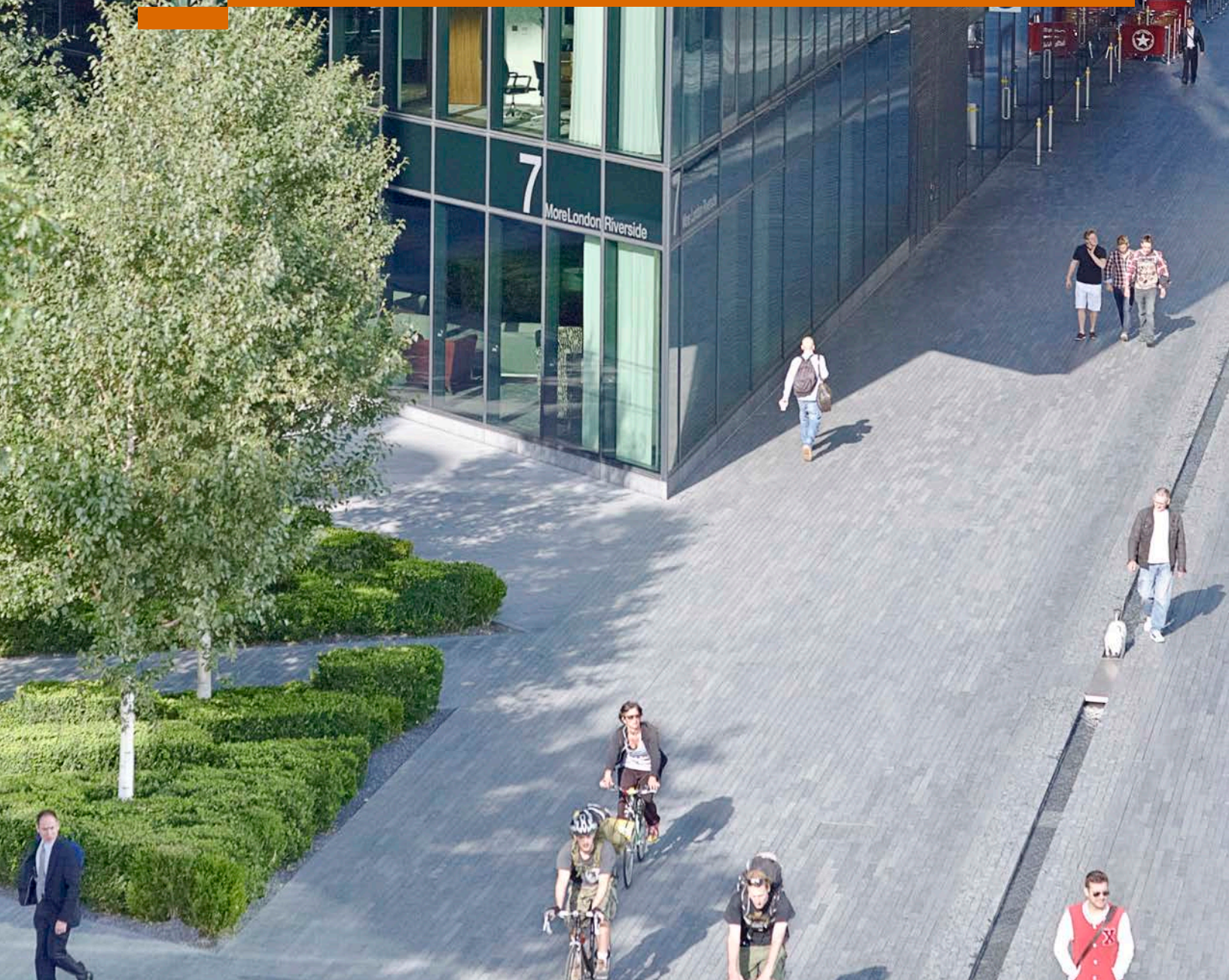
June 2014







*Managing cyber risks to sensitive information assets and systems is a top priority for most companies. That's because the scope, severity, and costs of cyber-attacks are increasing, whether these attacks seek to damage data and systems or steal sensitive information such as trade secrets or personal data. Many are finding that cyber insurance can be an effective tool to help manage these risks.*







*A lack of historical data loss attributed to cyber-attacks makes it difficult for insurance companies to determine premiums.*

In *The Global State of Information Security*® Survey 2014, an annual study co-sponsored by PwC, respondents said the number of detected security incidents in 2013 increased by 25% over the year before. At the same time, the number of respondents unaware of how many incidents they experienced doubled over the previous two years.

These results demonstrate that cyber security is no longer a technical problem for the IT department, but rather it is a risk the Board and C-suite must understand and properly manage. Doing so will require corporate executives and Boards to adopt a new mind-set and develop new tools to manage risk.

The complexities of modern business ecosystems and increasingly global interconnectivities create often-obscured pools of risk that can compound the challenges of risk management. Systemic cyber risk can stem from internal enterprise vulnerabilities and lack of controls, but it can also emanate from upstream infrastructure, disruptive technology, supply-chain providers, trusted partners, outsourcing contractors, and external sources such as hacktivist attacks or geopolitical actors. Many of these risks are outside the purview or controls of the typical corporate risk officer.

In response to this complex risk environment, the market for insurance products is evolving as companies seek new opportunities to gain insight into and better manage cyber risk. A significant third-party market currently exists to cover losses suffered by a company's customers in the wake of a cyber-related loss. The insurance industry, however, is trying to expand into new cyber-risk areas, such as first-party policies to cover the value of lost intellectual property, reputation, and brand, as well as products to cover cyber-related infrastructure failures. One challenge is a lack of historical loss data attributed to cyber-attacks that can be used to estimate probabilities of loss and calculate loss values. This absence of data makes it difficult to determine appropriate premiums.

Companies should understand the evolving market of cyber-insurance products and position themselves to take advantage of the most appropriate products given their risk profiles. It is equally important that businesses collaborate with both the insurance industry and government agencies to participate in the maturation of cyber insurance and potentially develop a more effective tool for managing cyber risk.



### Consider coverage beyond the breach

Cyber-insurance products cover both damage and liability stemming from attacks that could damage, corrupt, or disclose specific classes of data assets or technical infrastructure—risks that are typically excluded from traditional commercial liability coverage. These emerging insurance

*Many organizations invest in security as a technology initiative rather than a risk-reduction investment. As a result, they may not understand cyber-specific exposures, costs of response, post-breach liabilities, and potential for brand damage.*

products cover damages such as data destruction, denial of service, theft, and extortion; they also may include incident response and remediation, investigation, and security-audit expenses. Policies also may cover losses to others arising from errors and omissions, regulatory failures (e.g., individuals are not notified about breach of personally identifiable information), and inadequate data-security safeguards.

Given today's elevated threat environment and the rising financial impact of cybercrime, protecting against financial losses from cyber risks should rank as high as other insurable risks. *The Global State of Information Security® Survey 2014* found that average financial losses attributed to security incidents were up 18% in 2013 over the previous year, and big

liabilities are increasing faster than smaller losses. Respondents reporting losses exceeding \$10 million, for instance, increased 51% from 2011.

The annual security survey also found that when companies quantified losses for cyber breaches, a majority failed to factor in the full costs: Just 35% considered legal-defense services and only 29% included forensics and investigations. Also lacking were consideration of the costs of deploying detection software, services, and polices, as well as court settlements. This is key because PwC's experience investigating cybercrime in regulated industries indicates that the costs of remediating and investigating a cyber breach can be several times that of the actual first-order losses, such as cash theft in ATM cyber fraud.

### Using cyber insurance as a risk-management tool

Businesses should consider cyber insurance as an effective component of a cyber-risk management strategy. To do so, they should view cyber security within the context of information risk management to help understand and mitigate cyber threats specific to their enterprise. Companies should not relegate cyber security to an isolated technology function that is detached from enterprise risk management.

As a first step, businesses should proactively evaluate available cyber-insurance products and understand pricing. Many insurers are actively working to define offerings, and companies may have the opportunity to be involved in their development.

Many corporations frequently invest in IT security as a technology initiative, rather than a strategic investment in risk reduction at the corporate level. Consequently, they might not understand or appreciate cyber-specific legal and regulatory exposures, costs of response, possible post-breach exposures and liability, and brand damage. More importantly, they might not have a risk-based understanding of cyber threats and vulnerabilities to the company's key data assets, or "crown jewels," that support the primary value drivers. As a result, potential business consequences—financial, legal, reputational, and regulatory—resulting from loss of high-value data may not be factored into risk assessments. Given today's elevated level of cyber threats, corporate executives should regularly review periodic cyber-security assessments, including tool and process evaluation, incident-response readiness tools and training, and forensics capabilities. Doing so can help manage cyber risk at the enterprise level and help understand the potential value of cyber insurance.

When weighing decisions on cyber insurance, businesses should include Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs) in the discussion. Decisions regarding the purchase of cyber insurance typically fall to risk managers, lawyers, Chief Financial Officers (CFOs), and compliance officers. Given the current state of cyber threats, however, CIOs and CISOs should be key players in assessing risks to determine

appropriate coverage as well as evaluating and selecting cyber-insurance providers.

For many companies, the predominant challenge in effective cyber security is anticipating future sources of risk and finding and measuring hidden threats. Such sources and threats can be introduced in networks through exposure to insecure third-party systems and insiders in the business ecosystem. CIOs and CISOs manage sensitive data and are the executives most likely to be aware of the sources of cyber risk. Therefore, close involvement of security leaders in selecting and purchasing cyber-insurance products can help to more efficiently allocate corporate resources to manage risk over time.

Business executives should understand how security priorities differ among decision makers and managers, based on their individual perspectives and responsibilities. For example, *PwC's 2013 US State of Cybercrime survey* found that Chief Technology Officers (CTOs) and Chief Security Officers (CSOs) do not agree on the most significant cyber threats facing their organization. CSOs and CISOs pointed the finger at hackers and foreign nation-states as the top threats, while CIOs and CTOs were more concerned about insider threats. An effective risk assessment should comprehensively analyze the current security landscape to reach a consensus on cybersecurity risks and needs.

As companies evaluate and select products, they should discuss with insurers the fundamentals of good

security that drive risk-control elements and how adoption of these practices can affect coverage and premiums. These fundamentals are articulated in the Cybersecurity Framework released in February by the *National Institute of Standards and Technology (NIST)*, a set of guidelines we recommend organizations adopt.<sup>1</sup> Beyond the fundamentals, leading security practices include identification and encryption of sensitive data; strong authentication controls and privileged access management; application and device controls; reliability controls; insider-threat programs; security operations with perimeter, network, and host monitoring; regular breach-indicator assessments; and solid breach-response and forensic-investigative capabilities. Also key are integrated threat-intelligence and analytics capabilities. Our experience shows many companies lack threat knowledge and often under-invest in resources necessary for responding to threats. This is especially true for critical asset identification, monitoring and detection, incident and crisis management, process and technology fundamentals, and instilling an enterprise-wide culture of security.

These shortfalls can result in heightened risk of data loss, damage, or liability. They also can impair the success of cyber-insurance claims. That's why it is critical to review investments against threat intelligence and these key security capabilities. Doing so can help companies prevent and detect breaches, and also help remediate and respond to legal, regulatory, and market demands in the wake of an incident.

Finally, companies should conduct regular risk assessments that include threat analysis and vulnerability/controls analysis to maintain an up-to-date risk profile. Residual risk should be compared against management's risk tolerance before selection and procurement of cyber insurance. Businesses should work with insurers to identify the appropriate policy based on cyber risks, overall security posture and controls of the insured, and the anticipated costs of response and remediation.

---

<sup>1</sup> PwC, Why you should adopt the NIST Cybersecurity Framework.



*Posing the right questions can clarify how cyber insurance can protect the business, what kind of insurance product or coverage is optimal, and how to prioritize resources.*

### **11 key questions to consider in managing cyber risk**

Before engaging insurers in conversations, business executives should first ask risk-based questions about how insurance can meet the company's unique needs. Posing the right questions can clarify how cyber insurance can protect the business, what kind of insurance product or coverage is optimal, and how to prioritize resources. We recommend considering the following questions to evaluate the strength of a company's toolkit for managing cyber risk, as well as the role of insurance in that toolkit:

1. How does the company's risk-management process evaluate cyber risks? Does it understand cyber-related business, brand, and regulatory risks from an ecosystem-wide perspective (e.g., the transitive risk introduced outside a company's firewall by suppliers, contractors, and customers)?
2. What tools, processes, and controls does the company employ to prevent, detect, and respond to cyber-security incidents?
3. What are the priorities and investments in prevention, detection, and response? For instance, does the business prioritize prevention of attacks, and how does the investment in prevention compare with the company's spending on detection, response, and computer forensics?
4. Does the company integrate threat intelligence and assessments into proactive cyber-defense programs? Does it assess vulnerabilities against known tactics and tools used by threat actors who might target it? Does it understand potential threats?
5. Which data assets are most valuable to specific adversaries? Are security investments aligned with the threat actor's capabilities to steal or compromise those assets?
6. Do the firm's stakeholders (e.g., its Board, regulators, and customers) understand the threats that target the business?
7. How do corporate executives communicate with cyber-security leadership concerning threats, attacks, defensive technologies, and risk-mitigation strategies?
8. Do corporate executives understand the factors that increase their digital attack surface for a specific threat, either through technology decisions (e.g., adaptation of social networking or mobile devices) or business strategy (e.g., acquisition of a business line or a shift in geographic operations)?
9. Has the company integrated cyber risk into its information-security strategy?
10. What is the company's strategy for effectively using and updating

cyber-security technology (e.g., implementation of new versions and security patches to existing technology or employing data-analytics platforms to leverage data generated by IT security tools)?

11. Does the business understand which data assets and systems are most important to its key value drivers? Are security investments prioritized to protect the most valuable assets?

Answers to these questions can help guide a company to identify gaps in its ability to manage cyber risk, and consequently help it choose and qualify for the most appropriate cyber-insurance product. More importantly, these answers can provide important guideposts for effective corporate cybersecurity governance, strategy, resource prioritization, and risk mitigation.



*Today, cyber risks, technologies, and vulnerabilities evolve at lightning speed, and sharing information among public and private entities regarding cyber threats and responses has become central to a strong cybersecurity program.*

### **Identifying the right policy**

The relatively new cyber-insurance market is evolving as a number of companies compete to elbow their way onto the playing field. A full cyber-risk assessment should be conducted before a company implements a risk-management strategy, including the use of cyber insurance.

Buyers of cyber insurance must carefully consider insurance conditions, exclusions, and limitations: What costs and risks are covered, and under what conditions. Of specific concern is due diligence concerning past breaches, and to what extent a cyber attacker might have been already present in a corporate network before the policy was purchased. Policies will require various levels of due diligence, although coverage of losses due to breaches occurring before the purchase of insurance (if the breach is undetected at the time of purchase) will differ by policy. Conducting a breach-indicator analysis can be useful in helping identify specific indications of known attackers.

Additional actions to take when evaluating cyber-insurance providers and policies include:

- Mandate compliance with reasonable security standards
- Require threat- and breach-indicator assessments to determine whether specific threats are present in the buyer's environment
- Require periodic reviews and assessments for both security posture and possible breaches
- Provide a list of qualified providers of incident response and forensics services
- Factor in coverage for business interruption and lost revenue
- Consider the cost of forensic investigations and regulatory responses



It's also important to note that the insurance industry currently has difficulty covering losses resulting from stolen intellectual property and trade secrets. These losses may include damage to revenue streams, future growth potential, market presence, and brand or reputation. First-party loss coverage is still difficult to obtain due to the difficulty of calculating future losses from a lack of data on cyber theft and economic espionage. As the cyber-insurance market matures, however, more data on threats and consequences will become available, and as more IP and trade-secret theft cases are litigated, insured companies will be better positioned to recover losses across the spectrum of damage from cyber-attacks.

### **Collaborate to better manage cyber risks**

The nascent cyber-insurance market can help strengthen corporate cyber security, and stronger cyber security can benefit a wide variety of stakeholders, both public and private. Specifically, it can help prevent the non-financial damage of cyber-attacks. Note, however, that damages due to theft of intellectual property and impairment of corporate brands and consumer trust are less tangible—but potentially more destructive in the long term. Theft of trade secrets can be compared with theft of a priceless painting—a potentially irreplaceable loss. The check from the insurance settlement may be welcome, but prevention of IP theft is decidedly preferable.

Today, cyber risks, technologies, and vulnerabilities evolve at lightning speed, and sharing information among public and private entities regarding cyber threats and responses has become central to a strong cybersecurity program. Indeed, the data and insight into threat actors are now in the hands of corporate forensics investigators and security providers. Collaborating with the insurance industry represents a new way to better manage cyber risks.

---

***To have a deeper conversation, please contact:***

**David Burg**

Principal, US and Global  
Cybersecurity Leader  
david.b.burg@us.pwc.com

**Michael Compton**

Principal, Cybersecurity Strategy  
and Operations  
michael.d.compton@us.pwc.com

**Peter Harries**

Principal, Health Industries  
peter.harries@us.pwc.com

**John Hunt**

Principal, Public Sector  
john.d.hunt@us.pwc.com

**Mark Lobel**

Principal, Technology, Information,  
Communications and Entertainment  
mark.a.lobel@us.pwc.com

**Gary Loveland**

Principal, Consumer and Industrial  
Products and Services  
gary.loveland@us.pwc.com

**Joe Nocera**

Principal, Financial Services  
joseph.nocera@us.pwc.com

**Dave Roath**

Partner, Risk Assurance  
david.roath@us.pwc.com

**Paul McDonnell**

Principal, Financial Services  
paul.h.mcdonnell@us.pwc.com

**Jamie Yoder**

Principal, Financial Services  
jamie.yoder@us.pwc.com

***Contributing authors***

**Joe Calandro**

Managing Director  
joseph.calandro@us.pwc.com

**Eric Matrejek**

Managing Director  
eric.matrejek@us.pwc.com

**Neal Pollard**

Director  
neal.a.pollard@us.pwc.com







***[www.pwc.com/cybersecurity](http://www.pwc.com/cybersecurity)***