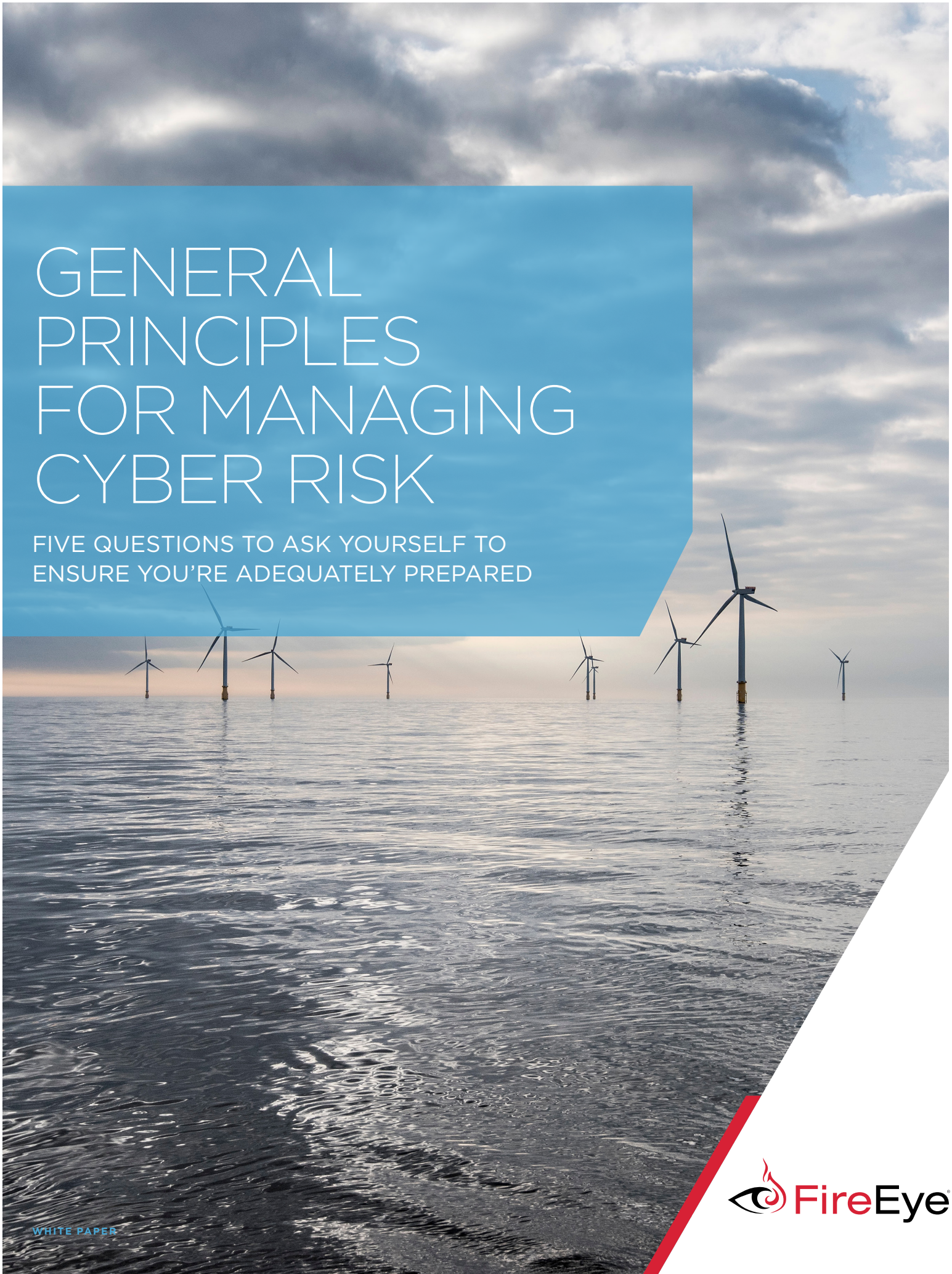


GENERAL PRINCIPLES FOR MANAGING CYBER RISK

FIVE QUESTIONS TO ASK YOURSELF TO ENSURE YOU'RE ADEQUATELY PREPARED

WHITE PAPER

FireEye

EXECUTIVE SUMMARY

OVER THE LAST DECADE, CYBER SECURITY HAS EVOLVED FROM A NICHE CONCERN OF IT PROFESSIONALS TO A MAJOR PRIORITY FOR CEOs AND BOARDS OF DIRECTORS. COMPANY LEADERS ARE NOW CHARGED WITH MANAGING CYBER RISK WITH THE SAME URGENCY THAT THEY HAVE TREATED TRADITIONAL BUSINESS RISK IN THE PAST.

The emergence of cyber risk as a cornerstone of risk management is being driven by new and increasingly complex threats. Organizations must deal with an evolving set of risks to their information systems and data. Many of these threats were unimaginable just a few years ago.

This paper explains the different forms of cyber risk and shows how the threat level has risen in recent years. It provides a basic framework for managing cyber risk. It also poses five key questions that business leaders should ask themselves to ensure their cyber risk stance is sufficiently robust and resilient to meet evolving threats.

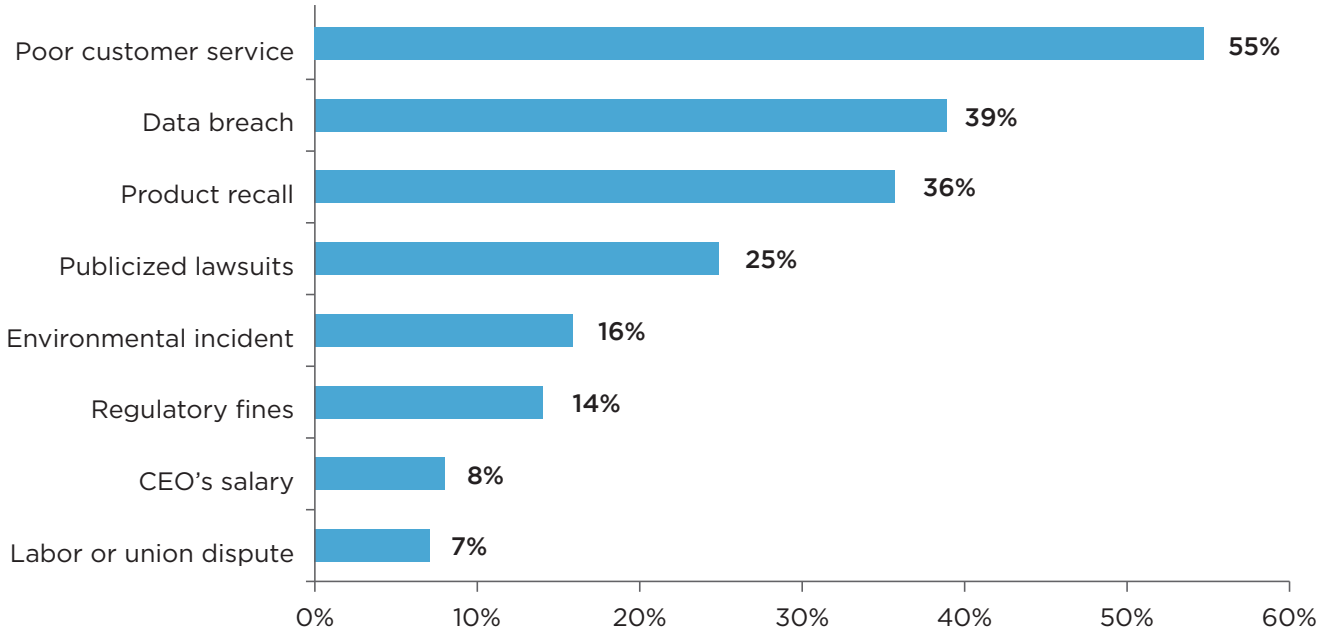
EVOLUTION OF CYBER THREATS

Over the last five years, cyber threats have changed. Previously, attackers typically sought personally identifiable information (PII) or credit card data today for quick financial gain. Today, however, sensitive business negotiations and high-value research and development (R&D) data are increasingly at risk of exposure. Meanwhile, business resiliency and data integrity are increasingly threatened by destructive attacks.

According to a PricewaterhouseCoopers 2016 report on cyber risk, the number of detected cyber attacks skyrocketed in 2015 — up 36% from 2014. This number is expected to rise even further in subsequent years, with businesses around the world already enduring more than 117,000 attacks each day.[1] Computer crime emerged for the first time as a top 10 risk in the AON 2015 Global Risk Survey.[2] Although getting known for poor customer service is still considered the most serious threat to businesses, data breaches have risen to second place, with 39% of companies saying it would have the "greatest impact" on their reputation (Fig. 1.)[3]

FIGURE 1: ISSUES THAT AFFECT COMPANY REPUTATION

Which of the following issues would have the greatest impact on your organization's reputation? Two responses permitted.



Source: Advisen. "Fifth Annual Report on Risk." 2015.

1 Advisen. "Fifth Annual Report on Risk." 2015.
2 AON. "Global Risk Survey." 2015.
3 Advisen. "Fifth Annual Report on Risk." 2015

For cyber attackers, the risks are low and the rewards high. A cyber criminal can conduct a network intrusion anonymously from hundreds or thousands of miles away and gain access to data — credit card numbers, industrial designs or business plans — that allows them to reap significant rewards (see "Network Breaches: A Low-Risk, High-Reward Proposition for Cyber Criminals").

The motivations for cyber threat activity are diverse: they range from fraud and extortion for financial gain to industrial or political spying. Threat actors may even conduct an attack to gain attention for a political cause or to gain an advantage in a military conflict. These threats can be divided into four major categories: cyber espionage, cyber crime, hacktivism and destructive attacks. These categories are summarized in Table 1.

TABLE 1. CYBER THREATS AND THE RISK THEY POSE

TABLE 1. CYBER THREATS AND THE RISK THEY POSE		
ATTACK TYPE	**MOTIVATION**	**GOALS**
Cyber Espionage	Cyber espionage actors seek access to sensitive confidential information that they can wield to their advantage. They may work for a national government or could be industrial spies.	• Steal intellectual property and confidential business information • Monitor intelligence targets for military or strategic insights • Collect information on strategic business developments for a competitive advantage
Cyber Crime	Cyber criminals seek to monetize the data they steal, whether it is credit card data, PII or insider data to game capital markets. These attackers also seek to extort their victims by threatening to disrupt the integrity of key systems.	• Use malware and targeted intrusions to steal money, personal information or credit card data from individuals and businesses • Steal non-public information for an advantage in stock trading • Hold targets hostage by using tools such as ransomware or distributed denial of service (DDoS) attacks to threaten the confidentiality, integrity or availability of critical data and systems
Hacktivism	Hacktivist actors seek to make a political or social statement.	• Protest social, economic or political causes • Harm the reputation of their targets by publicizing their attacks • Act as cover for cyber threat groups backed by a national government
Destructive Attacks	Destructive attacks are often conflict driven and seek to disable or destroy target systems.	• Disrupt critical systems to degrade enemy capability in a conflict • Attack industrial control systems • Degrade public trust in critical services

Network Breaches: A Low-Risk, High-Reward Proposition for Cyber Criminals

Over the last year, many incidents have illustrated the rewards that threat actors can reap with very little risk:

Advanced persistent threat (APT) actors and cyber criminals have been behind massive thefts of PII. Many of these thefts involve millions of records. Detailed personal information can be used for fraud or to help espionage attackers better understand their targets. Such cyber criminals are rarely caught, or if caught, successfully prosecuted for their crimes.

The last year has also seen an explosion of ransomware attacks. In addition to attacking individuals, cyber extortionists have turned their sights to businesses such as hospitals and financial services firms that rely on data for critical operations. After accessing and locking the files of their victims, cyber extortionists then charge them to decrypt the files. For business targets, the ransom can be quite high — again, offering cyber criminals a big return for very little risk.

For cyber attackers, the risks are low and the rewards high.

Cyber attacks evolve quickly and can be difficult to predict. Yet the damage from failing to take them seriously can be immense. A Washington D.C. think tank, the Center for Strategic and International Studies, claims that the annual cost of cyber crime and economic espionage to the world economy runs as high as $445 billion — or almost one percent of global income.[4] It is also important to note that this doesn't include the intangible damage to organizations, such as damage to brand and reputation.[5]

The Ponemon Institute found that the mean cost of a breach is rising, reaching $7.7 million in 2015.[6] Business disruption accounts for 39% of total costs, which include expenses related to business process failures and lost employee productivity. Detection and recovery costs combined account for 53% of the total cost, with productivity loss and direct labor representing the majority of these costs.[7]

Risk from third parties — contractors, suppliers, or partners — is growing. One of the most widely publicized and costly breaches of the past several years was due to a single phishing email sent to a supplier's employee. Yet only 42% of companies consider supplier risks.[8] In fact, most companies do not have a process for assessing the security of third-party partners before they do business with them.[9] And only 12% of businesses in 2015 looked beyond their suppliers to their suppliers' suppliers (fourth parties).[10]

As organizations rely more on complex information systems to conduct business intelligently, their operations are increasingly exposed to cyber risk. Business leaders must therefore implement a robust risk management program that prioritizes cyber risk.

GENERAL PRINCIPLES FOR MANAGING CYBER RISK

The National Association of Corporate Directors published the following principles for managing cyber risk in its *Cyber-Risk Oversight Executive Summary, Director's Handbook Series, 2014 Edition:*

- **Understand and approach cyber security as an enterprise-risk management issue.** It can no longer be relegated to the IT director, but must be a multi-disciplinary concern managed at the highest levels of your organization. This already appears to be changing for the better. In 2014, only 29% of respondents said their senior leaders were involved in data breach preparedness. This year, possibly due to the publicity over recent breaches, 39% of respondents say their boards are involved in data breach preparedness.[11]
- **Comprehend the legal implication of cyber risks.** In case of a breach, litigation is almost inevitable. Depending on the kind of information your organization generates, collects, processes or stores, you could face millions in legal fees. If regulatory mandates like Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI DDS) have been violated, you must include the hefty penalties associated with them in your calculations. You should even anticipate claims against individual board members and executives from shareholders and class action suits, with charges including breach of fiduciary duty, corporate waste and mismanagement. The key allegation is typically that directors or officers did not take sufficient steps to prevent a cyber attack that resulted in monetary or reputational harm to the company.[12]

4 Center for Strategic and International Studies. "The Economic Impact Of Cybercrime And Cyber Espionage." 2013.
5 Ibid.
6 Ponemon Institute. "Cost of Cyber Crime." 2015.
7 Ibid.
8 PriceWaterhouseCoopers. "2015 US State of Cybercrime Survey." 2015.
9 Ibid.
10 Ernst & Young. "Global Information Security Survey. 2015.
11 Ponemon Institute. "Third Annual Study: Is Your Company Ready for a Big Data Breach?" October 2015.
12 The Business Litigation Reporter. "Breaches in the Boardroom: What Directors and Officers Can Do to Reduce the Risk of Personal Liability for Data Security Breaches." February 6, 2015.

Prioritize and protect the most critical information assets and systems, based on the business strategy of the organization and the current risk picture.

- **Possess adequate access to cyber security expertise.** A full 57% of IT managers say that lack of skilled resources is challenging their ability to contribute value to the organization.[13] Organizations that don't have security expertise in house should turn to third-party experts to act as trusted advisors to assist with their security programs and help frame the issues when briefing the their executives.

- **Discuss cyber risk management regularly on the board meeting agenda.** No news isn't necessarily good news. The median number of days an organization was compromised in 2015 before the organization discovered or was notified of a breach was 146.[14] Although this was 50 days fewer than 2014, it is still far too long.

  A case in point: the Mandiant Red Team simulates attacks on companies to determine the strength of their cyber defenses. It is typically able to obtain access to domain administrator credentials within just three days of gaining initial access to an environment.[15] That would theoretically leave more than four months for an attacker to enjoy free reign inside an environment – plenty of time to cause considerable damage.

- **Involve cyber security professionals in business strategy discussions and vice versa.** Security professionals should advise the heads of lines of business on cyber security risk as they determine new sales channels, business strategies, capabilities and merger and acquisition decisions. Additionally, cyber security risk decisions are not just security teams' responsibilities — they should be a part of a holistic business strategy with business line executives playing a significant role in the decision-making process.

- **Ensure that management establishes an enterprise-wide risk-management framework with sufficient staffing and budget.** Make sure to fund cyber security initiatives well. Worldwide spending on information security increased just 4.7% in 2015, with many businesses actually cutting back on security as part of cost-saving measures, according to Gartner.[16] But what businesses are spending might not be enough. A survey of high-level IT executives by Ernst & Young found that 49% believe their security budgets should increase at least 25% to align with the business' tolerance for risk.[17]

- **Clearly identify which cyber risks to avoid, mitigate, accept or insure with specific plans for each category.** Organizations can't protect themselves against every threat. Prioritize and protect the most critical information assets and systems, based on the business strategy of the organization and the current risk picture. Because a breach is inevitable, you must carefully plan how to respond to it. Finally, consider transferring a portion of the risk your organization is assuming to a cyber insurance provider. This creates a financial buffer should you suffer a large breach. There is ample choice in the market place. Demand for cyber insurance has grown considerably in recent years. Last year, the insurance industry reaped $2.5 billion in premiums on policies to protect companies from losses resulting from attacks. That was up from around $2 billion a year before, and less than $1 billion two years before that.[18]

13 Ernst & Young. Global Information Security Survey. 2015.
14 Mandiant, a FireEye company. "MTrends 2016." February 2016.
15 Ibid.
16 Gartner. "Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach $75.4 Billion in 2015." September 23, 2015.
17 Ernst & Young. Global Information Security Survey. 2015.
18 Stephen Gandel (Fortune). "Lloyd's CEO: Cyber attacks cost companies $400 billion every year." January 23, 2015.

Questions to Ask About Cyber Risk

1. Is cyber security part of your enterprise risk management activities, and not simply an IT / technology concern? Who has the authority to accept risk in your organization and do you possess transparency on aggregated risk?
2. Who conducts risks analyses and assessments and how often?
3. What is your organization doing to manage/minimize the legal risks/exposures?
4. Do you adequately monitor third-party risks?
5. Are you keeping abreast of the latest threat intelligence and applying additional protection to your assets? How?

ELEVATE CYBER RISK RESPONSIBILITY TO THE TOP OF THE ORGANIZATION

The threat landscape is constantly changing. Attackers can creatively target information assets using evasive techniques. Business leaders need to take note of their changing risks in a way that encompasses the current threat landscape, and keep their breach response plans current.

Businesses must create an enterprise-wide robust risk framework based on today's best practices and principles. They also have to invest adequately in the right security tools and services, get access to up-to-the-minute security intelligence, and hire people with advanced security knowledge and expertise. Most importantly, cyber risk transparency should be elevated to the highest organizational levels. Accountability must start at the top.

For more information on FireEye, visit:
www.FireEye.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com