MARSH & McLENNAN COMPANIES | THE CHERTOFF GROUP

NOVEMBER 2014

A CYBERSECURITY CALL TO ACTION

CONTENT:

MARSH GUY CARPENTER MERCER OLIVER WYMAN

EXECUTIVE SUMMARY

Cyber-attacks are a present and growing danger. Massive data breaches and a steady stream of reports about vulnerability have put boardrooms on high alert and spurred companies to dedicate more resources to cyber-breach preparedness, response, and recovery.

In 2013, the US budget for cybersecurity products and services exceeded US$67 billion. In addition, cyber-insurance premiums reached US$1.3 billion, and Marsh data indicates that take-up rates are climbing for a wide range of industries. With hackers constantly refining techniques and succeeding in their efforts, are we closing the gap on the cyber threat or falling farther behind?

The following report seeks to describe progress US companies have made in addressing the cyber threat. Using data compiled by Marsh, and analyzed in cooperation with The Chertoff Group, this report profiles how US companies prepare for cyber incidents and recover from events. Specifically, the report focuses on:

- Benchmarking data that demonstrates the buying trends of US companies in select industry sectors.
- Analysis from Marsh proprietary modeling tools that projects ranges of severity for potential data breaches.
- A survey of information-security practices implemented by Marsh clients.

Two key findings emerged:

1. More organizations are buying cyber insurance, and the limits purchased are also rising. However, Marsh data-breach modeling demonstrates that purchasing trends may fall short of the largest cyber exposures.
2. Many companies still have lapses in basic security practices recommended by internally accepted information security standards.

The question that remains is whether companies are undertaking data-driven analyses of cyber-risk exposure and information-security assessments to identify vulnerable practices.

Cyber risk is a complex exposure for companies to address. No security strategy is bulletproof. At some point, each company must decide how much cyber risk it will accept, what resources it will devote to mitigating the risk, and how much risk it will transfer. Prior to making those decisions, companies should take care to use the right tools and collect the data needed to drive their choices.

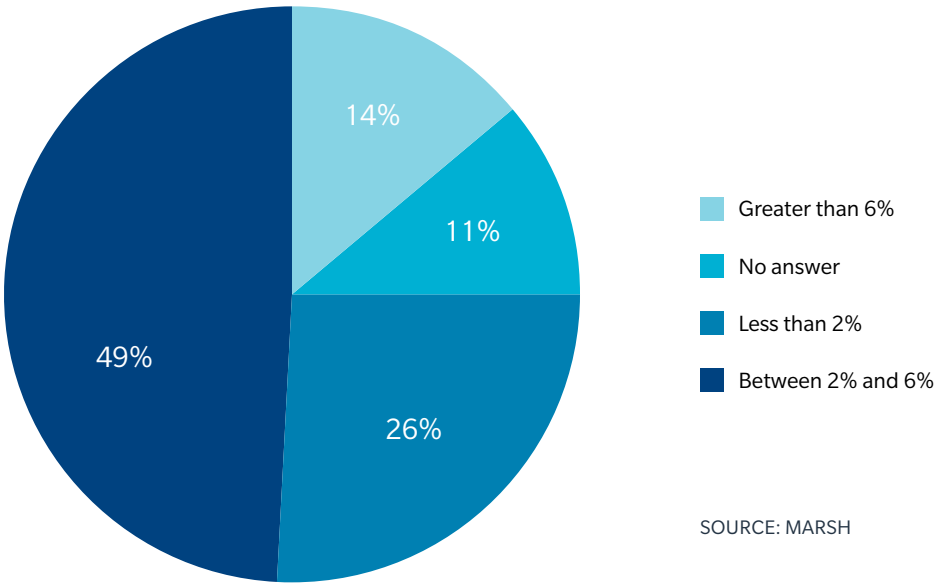
INTRODUCTION

Hackers persistently target US computer networks. Sophisticated companies fall victim to theft of customer data, network disruptions, stolen intellectual property, and attacks targeting physical infrastructure. Yet while those exploits raise attention for the need to prepare and defend against cyber-attacks, many companies still underestimate the potential impact of the cyber threat and remain exposed.

The following report undertaken by Marsh & McLennan Companies, and performed in cooperation with The Chertoff Group, uses a data-driven approach to examine two issues: (1) Are companies adequately preparing for the consequences of cyber breaches? (2) Are they maximizing their ability to reduce vulnerabilities? Using Marsh proprietary data and analytical tools, we review current trends for using risk transfer to address potential exposures, as well as the ability to mitigate risk by aligning basic cyber controls to the threat. Our findings indicate growing efforts to combat the threat, but also a greater need for adoption of best practices and preparation for the inevitability of breaches.

Every organization must respond to this pervasive threat with finite resources. According to Marsh, of clients that purchase cybersecurity, more than a quarter dedicate less than 2% of their information-technology budgets to information security, while nearly half dedicate somewhere between 2% and 6% (see FIGURE 1).

FIGURE 1: PERCENTAGE OF INFORMATION-TECHNOLOGY BUDGET DEVOTED TO INFORMATION SECURITY



SOURCE: MARSH

Many organizations perceive a distinction between investing in assessments or technology versus insuring against the consequences of a breach. However, strengthening cybersecurity defenses and risk transfer through cyber insurance should not be viewed as an "either-or" proposition. Instead, these two elements of risk management complement one another. Cyber-insurance products can lead organizations toward implementing stronger security.

First, the very exercise of evaluating whether cyber insurance fits a corporate risk strategy often leads an organization to evaluate its defenses and identify weaknesses. By conducting reviews of their own practices against widely recognized standards, such as those leveraged by the Framework for Improving Critical Infrastructure Cybersecurity released by the National Institute of Standards and Technologies (the "NIST Framework"), organizations can gauge their performance and find areas for improvement.

Second, many of our clients have found that the insurance underwriting process gives them an additional reference to evaluate their cyber security. By comparing their processes and controls with the view offered by the insurance community, companies can identify areas of improvement based on real-world cyber-event experience. Those that receive external validation may stand to benefit from lower premiums.

Third, if a cyber insurance program is implemented, organizations can benefit from services that meet the goals of the core functions set forth under the NIST Framework — identify, protect, detect, respond, and recover. Under some coverages, cyber insurance vendors perform assessments of practices, scan systems for threats, offer ongoing consultancy for mitigating threats, and assist in responding to incidents. In short, the cyber insurance industry has developed into an engine that drives the improvement of cybersecurity.

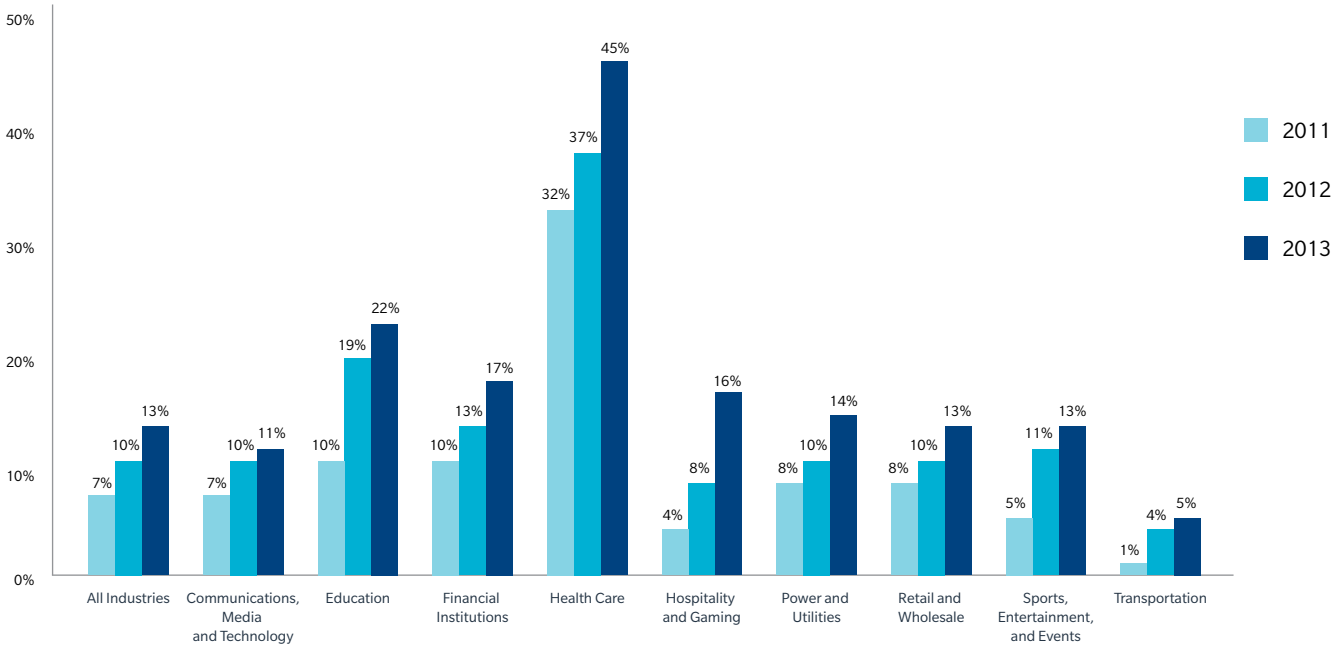
Although cyber insurance provides an additional incentive for bettering cyber practices, widespread adoption of best practices, like those promoted by the NIST Framework, will require more coordinated efforts. Collaboration among government agencies, security companies, the insurance industry, and the companies under attack will be essential to assess vulnerabilities and confront the risk head on.

POTENTIAL BUSINESS IMPACT OF CYBER INCIDENTS

Companies have increasingly gravitated to the benefits of insuring against cyber risk. The number of Marsh clients purchasing cyber insurance increased 21% from 2012 to 2013. Data-rich sectors that already experienced widespread purchasing, including financial institutions, retail/wholesale, and professional services, increased more than 13%. Adding to that trend, new industries emerged as sectors that routinely purchased cyber coverage, such as manufacturing, energy and utilities, and hospitality (see FIGURE 2).

Although that growth reflects that more companies recognize cybersecurity risk, it remains less clear whether organizations appreciate the potential business impact of a cyber incident.

FIGURE 2: CYBER INSURANCE PURCHASING BY INDUSTRY, 2011-2013



SOURCE: MARSH

The following analysis addresses that question using two distinct pieces of data. First, using a proprietary Marsh statistical model, the Cyber IDEAL, we develop profiles of hypothetical companies based on three industry sectors (retail, higher education, and health care), with assumptions made for annual revenues and number of records being protected[1]. After that profile is developed, we compare the potential exposure with the actual trends of Marsh clients — from the same industry and with similar revenues — for placing risk-transfer programs. Based on those comparisons, the data and analysis indicate that the exposure facing many organizations eclipses the risk-transfer programs those organizations have implemented. Those organizations may have accepted the potential for those larger losses because they view those incidents as remote and unlikely.

1 The Cyber IDEAL model provides analysis for a company's data-privacy exposure. However, there are many perils that companies face from a network security perspective. Some of those perils can be addressed through cyber insurance, such as lost revenues from business interruption, expenses to restore a network, the expense to recreate corrupted or damaged data, and extortion threats against cyber assets. Others, such as theft of trade secrets or patents or loss of speculative profits, would not be covered by a typical cyber insurance program. The Cyber IDEAL model focuses on data privacy exposure because, unlike other events, sufficient loss information exists upon which a statistical analysis may be performed.

RETAIL

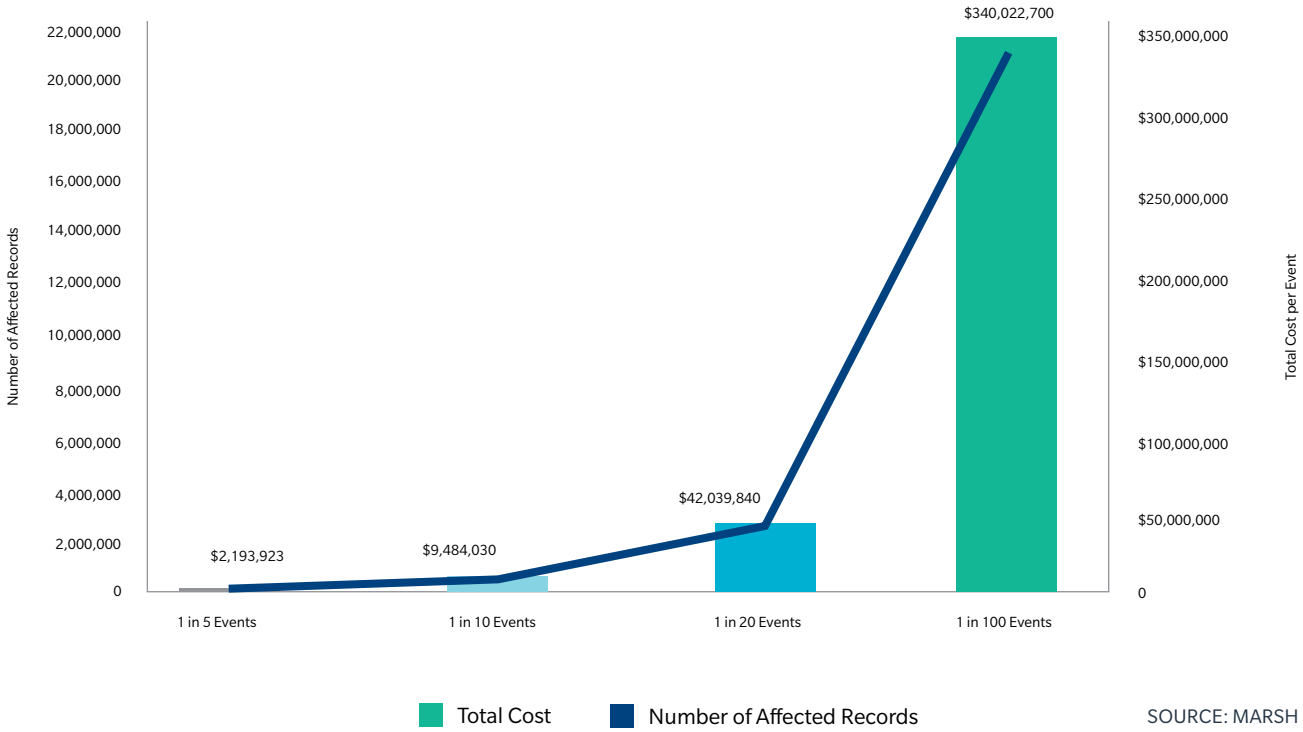
According to Marsh data, retailers with revenues between US$5 billion and US$20 billion on average will buy an aggregate limit of US$23 million. However, a hypothetical retailer in that bracket may have a much higher exposure than that average limit. To calculate the impact of a potential data-breach event for a retailer of this size, the following parameters were assumed:

ASSUMPTIONS FOR RETAIL EXPOSURE

Industry	Retail
Revenue	US$12 billion
Record Type	Credit and debit card
Maximum Records Held	75 million

Based on that profile, Cyber IDEAL indicates that the organization's data-breach exposure for a one-in-twenty event could likely result in costs that exceed US$42 million (see FIGURE 3). However, a less frequent but more severe event, occurring once in every 100 data breaches, could result in the exposure of more than 21 million records. Should that severe incident occur, costs could exceed US$340 million, or nearly 12 times the average limits purchased. Such an event could potentially create an enterprise-threatening risk, before even accounting for the risk to reputation.

FIGURE 3: RETAIL EXPOSURE FOR A 1-IN-100 EVENT (US$)



SOURCE: MARSH

HIGHER EDUCATION

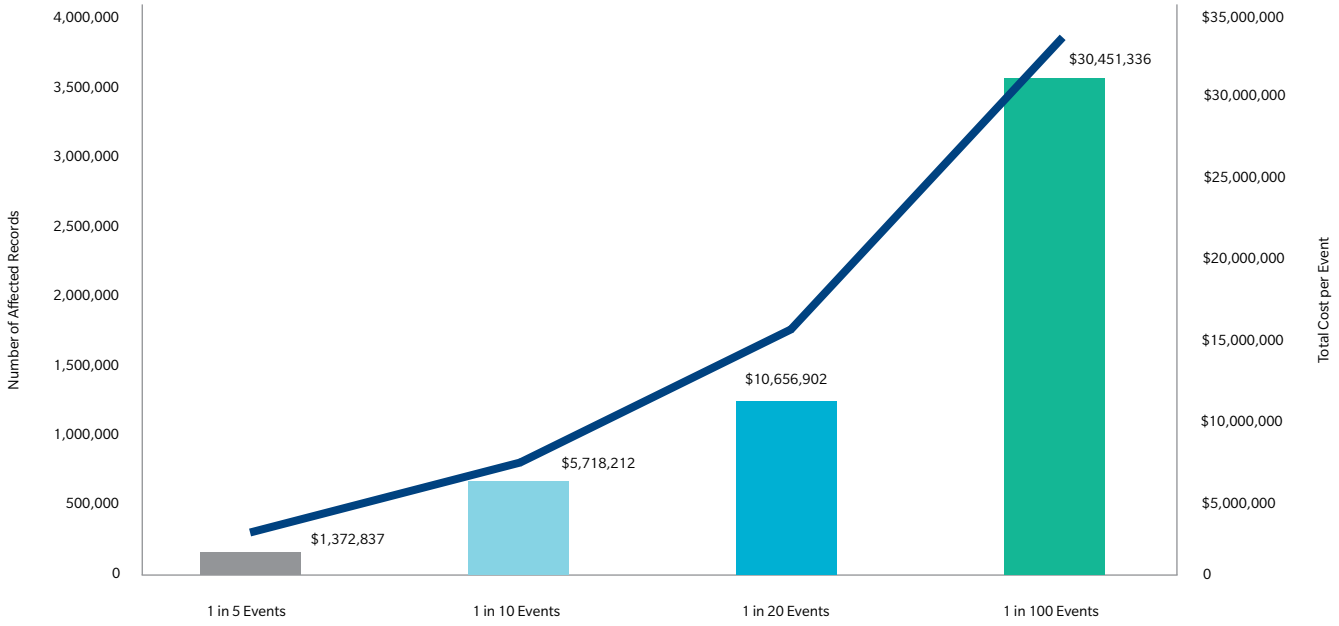
Marsh data indicates that a university with an operating budget of US$1 billion on average purchases cyber insurance with a limit of US$5 million. However, the exposure faced by that university could easily surpass that aggregate limit. To calculate the impact of a potential data breach event for a university of this size, the following parameters were assumed:

ASSUMPTIONS FOR HIGHER EDUCATION EXPOSURE

Industry	Higher education
Operating Budget	US$1 billion
Record Type	Personally Identifying Information (PII)
Maximum Records Held	5 million

According to the Marsh Cyber IDEAL model, a breach for a university of this profile could result in costs of more than US$10 million (see FIGURE 4). A less frequent but more severe event, occurring once in every 100 data breaches, could result in the exposure of more than four million records and incur costs of more than US$30 million, or more than six times the average coverage amount.

FIGURE 4: HIGHER EDUCATION EXPOSURE FOR A 1-IN-100 EVENT (US$)



SOURCE: MARSH

HEALTH CARE

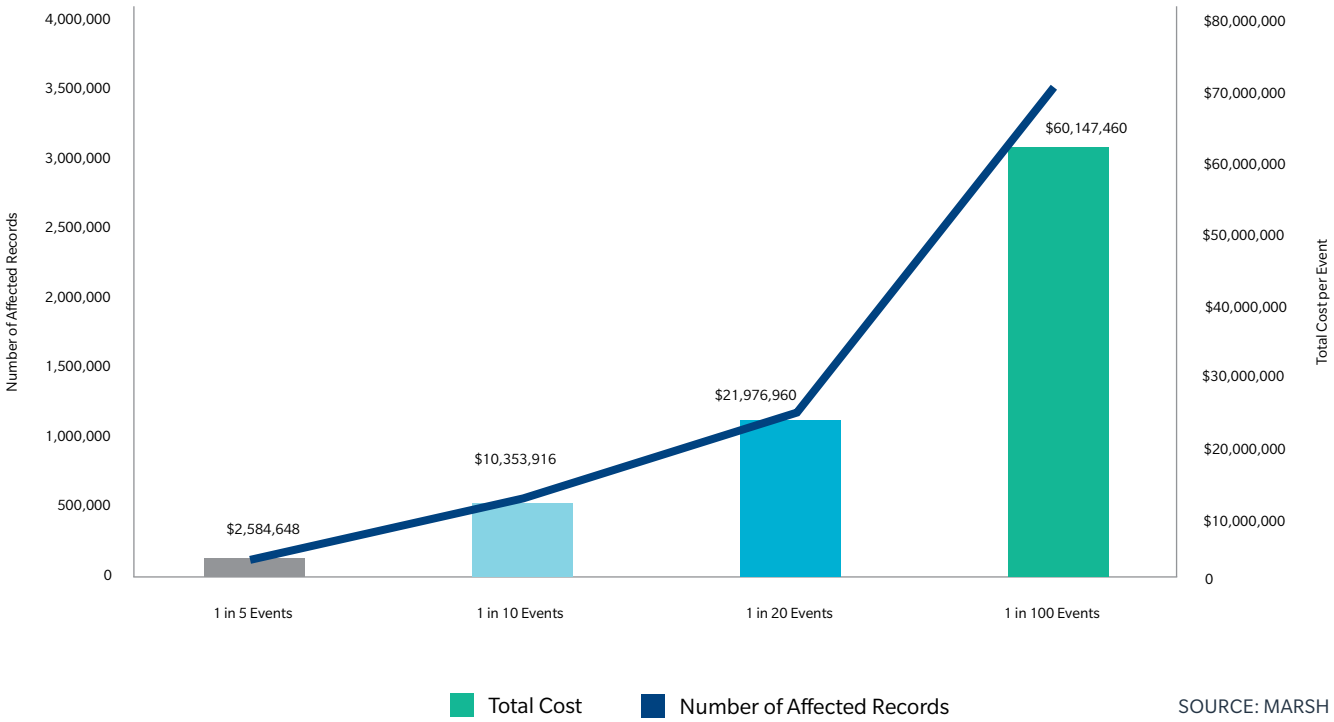
Marsh data indicates that a US$3-billion health care company on average buys US$11 million in cyber insurance limits. Although many health-care-sector institutions may surpass that figure, the average demonstrates that many more run the risk of being significantly underinsured against large data breaches. To assess the adequacy of those limits, we prepared a Cyber IDEAL analysis of the following profile:

ASSUMPTIONS FOR HEALTH CARE PROVIDER AND SERVICES

Industry	Health care providers and services
Revenue	US$3 billion
Record Type	Personal Health Information (PHI)
Maximum Records Held	5 million

A health care company with this profile can expect costs amounting to nearly US$22 million for the one-in-twenty event (see FIGURE 5). In the event of a more severe breach occurring one in every 100 events, costs could top US$60 million, leaving almost US$50 million in uninsured costs. Accordingly, while many health care companies have increased their protections against data breaches in recent years, many may be carrying exposures with significant risk to their balance sheets and reputation. That risk could grow should cyber-attacks continue to increase in frequency or sophistication.

FIGURE 5: HEALTH CARE EXPOSURE FOR A 1-IN-100 EVENT (US$)

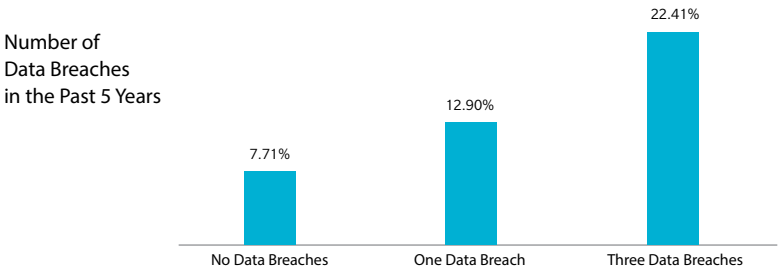


SOURCE: MARSH

REPEATED BREACHES

One might assume that once an organization experiences a data breach, the response is to secure defenses to make sure that history does not repeat itself. However, an analysis of prior data breaches indicates that the statistical likelihood that an organization will suffer a data breach[2] (see FIGURE 6).

FIGURE 6: LIKELIHOOD THAT ORGANIZATION WILL EXPERIENCE A DATA BREACH IN THE NEXT 12 MONTHS



SOURCE: MARSH

While at first counterintuitive, the analysis highlights that data breaches are a frequent event. Organizations face incessant intrusions, and previous experience may not reduce or eliminate the threat.

AN ADAPTIVE THREAT

Malicious actors consistently improve their skills and create new exploits. These hackers benefit from state-sponsored outsourcing (which has created a class of contract hackers), financial resources of organized crime groups, and the increasing availability of user-friendly hacking tools. The borderless nature of the internet often enables these actors to operate with relative impunity, often beyond the reach of law enforcement in the victim's jurisdiction. Moreover, some of the most significant risks stem from disgruntled or corrupt insiders.

Organizations face several basic challenges in confronting this threat. Adversaries remain able to bypass perimeter-based defenses by exploiting vulnerabilities originating with the user, such as through exploiting weak passwords or bypassing controls through malware delivered in a "phishing" campaign or via a "watering-hole" campaign. In addition, organizations continue to struggle with maintaining secure system configurations that prevent lateral movement inside a network as well as leaving vulnerabilities unpatched and thus open to exploitation by malware. Moreover, because controls have historically been perimeter-based, organizations lack visibility and situational awareness for harm being done inside the network, particularly by insiders. The ease of compromise also allows malicious actors to hide their tracks by leveraging compromised systems as intermediate points along their attack pathway.

---

2 In the context of Cyber IDEAL, not every cyber incident constitutes a breach. Rather, a data breach is an incident of sufficient significance that it triggered a regulatory reporting requirement or could otherwise be confirmed for its occurrence and magnitude. Thus, the many events that organizations experience but remain unreported are not considered by the model.

To address these challenges and respond to the morphing threat, an effective security risk management program should include a regular risk-assessment process that anchors the organization with strong cyber practices. Security programs should be evaluated for their flexibility and defense-in-depth (including against insider threats), consideration of risk aggregation, and overall resiliency. In February 2014, NIST paved the road for this process with the release of its Framework, which organizations can use to evaluate and strengthen their programs. The NIST Framework guides organizations in mapping their controls to five core functions that: (i) identify the assets that support critical business functions and the related cyber risks; (ii) protect assets using appropriate safeguards; (iii) detect cybersecurity events; (iv) respond to cybersecurity events; and (v) recover from events by restoring services and capabilities.

Marsh recently conducted an examination of the information security and data-privacy controls of more than 400 US clients. The results demonstrate that, while a number of institutions have implemented cybersecurity programs, many of these programs are not yet fully risk based.

INFORMATION-SECURITY PRACTICES IN PLACE

FOCUS ON INFORMATION ASSETS THAT MATTER MOST

Given the adaptive nature of the threat, a foundation for risk response is appreciating an organization's underlying business objectives, and how information assets align to those objectives. Marsh survey data indicates that, while most companies apply some form of role-based access control, these access controls do not necessarily reflect the underlying value of the information assets and systems these controls are intended to protect — the starting point for the NIST Framework (see FIGURE 7). This data is consistent with The Chertoff Group's risk-assessment findings across multiple industries.

FIGURE 7: PROTECTING INFORMATION ASSETS

Is access to the network based upon a data user's role?	85%
Are data-protection requirements defined and documented?	50%
Are data-classification policies based on risk assessments?	43%

SOURCE: MARSH

More specifically, as noted in the above table, less than half the companies surveyed classify their information based on an actual assessment of risk. Asset categorization as a risk management starting point is a common concept reflected not only in the NIST Framework, but also in numerous NIST information-security guidelines, the Board of Directors cybersecurity handbook released by the National Association of Corporate Directors, and The Chertoff Group's own security risk management methodology. By identifying and classifying high-value information assets, graduated levels of security can be applied based on risk.

ORGANIZATIONS NEED STRONGER DATA PRIVACY TRAINING

The free-flow of electronic information means more data is being collected and used by a growing number of organizations. Without a strong data-protection program, the sprawl of data can make it difficult to adhere to privacy compliance mandates and best practices around collection, use, sharing, retention, and protection of personally identifying information (PII). Many companies, even those that aggregate data, lack formal privacy controls and training programs. Many may not fully appreciate data-protection mandates and the related impact of a violation on the organization (see FIGURE 8).

FIGURE 8: PRIVACY CONTROLS AND TRAINING PROGRAMS

A chief privacy officer is responsible for management and compliance with your privacy policy.	36%
Does your organization leverage an e-training platform for employee training in order to provide privacy awareness training to your employees?	62%
Is privacy training a separate component of training?	37%
Is privacy training offered annually?	46%

SOURCE: MARSH

ACCESS AND IDENTITY MANAGEMENT

The security of user-access controls is a leading risk for many organizations. Compromised credentials are often at the heart of extensive network infiltration. Thus, the implementation of advanced authentication controls, such as two-factor authentication from remote access, can be a critical practice in preventing unauthorized access. While nearly all respondents to the Marsh assessment reported that they implemented security controls for remote users, almost half of respondents answered that they did not use advanced controls for remote users (see FIGURE 9). Accordingly, many organizations may be missing a critical security component to deter hackers.

FIGURE 9: ACCESS AND IDENTITY MANAGEMENT

Are controls in place to secure remote network access?	96%
Do you use advanced authentication controls (such as two-factor authentication or certificates) for remote access?	54%
Do you require firewalls to restrict VPN users from concurrently accessing the internet ("split tunneling")?	53%

SOURCE: MARSH

CYBER-INCIDENT RESPONSE

When responding to a cyber-incident, costs and liabilities can be substantially reduced by doing so on a timely and agile basis. Effective response plans will help companies manage a cyber-incident in a manner that minimizes damage, preserves organizational reputation, and reduces recovery time and costs. Yet according to self-assessments provided by Marsh clients, one-quarter of organizations did not have an incident-response plan and the majority of organizations did not routinely test the plan for its effectiveness (see FIGURE 10).

FIGURE 10: CYBER-INCIDENT RESPONSE

Does your organization have an incident-management program?	76%
Is the incident-response program tested annually?	37%
Does the incident program include trained personnel?	60%

SOURCE: MARSH

Incidents should also inform ongoing risk assessment and prioritization of controls. One of the most common forms of data breach is lost and stolen laptops. Whole-disk encryption of laptops can be a straightforward way of limiting business impact to a victim organization and its customers; yet half of respondents still do not implement hard-disk encryption on mobile devices and laptops (see FIGURE 11).

FIGURE 11: HARD-DISK ENCRYPTION ON MOBILE DEVICES AND LAPTOPS

Do your mobile devices and laptops have hard-disk encryption enabled?	50%

SOURCE: MARSH

Timely and agile response is much less achievable when relevant plans are not exercised beforehand. Companies should ideally incorporate a "when, not if" culture to prepare for cyber-incidents, and start planning and exercising response strategy in advance.

THIRD-PARTY RISK MANAGEMENT

As network systems become increasingly dependent upon outsourced service providers, and business operations grow interdependent with the technology of business partners, organizations sacrifice control over their technical infrastructure for increased efficiency. To avoid increased exposure due to these interdependent relationships, companies should monitor the cyber practices of the vendors and business partners connected with their networks, and should seek contractual obligations requiring strong security practices. However, while most organizations indicated on their self-assessments that that they enforce third-party security standards, only a small number monitor access and authorization on an assessment of the risk profile of the third party in question, or monitor a third party after authorization for recurrent risk (see FIGURE 12).

FIGURE 12: THIRD-PARTY RISK MANAGEMENT AND MONITORING

Does your company enforce security standards for third parties that connect to your network?	92%
Are risk assessments of network security practices performed on third parties prior to approval?	48%
Are third-party connections monitored for security events	59%

SOURCE: MARSH

SECURITY CONTROLS FOR DEPLOYING CRITICAL SYSTEMS

When a company rolls out a new critical system, design and development can often focus on operational functionality, reliability, and speed to market, but ignore security. Companies should recognize that an ounce of prevention is often worth more than a pound of cure. Attackers are adept at exploiting poor network hygiene — for example, known configuration and code-related vulnerabilities that remain unpatched — to move laterally within a network.

By integrating security planning at the requirements-identification phase of the system development lifecycle, organizations can (a) reduce the cost of complexity of building security into a system after-the-fact; and (b) align security and underlying business processes up front to make for a more seamless user experience and identify opportunities to promote adoption. Despite the importance of configuration management, nearly one in three organizations responded that they do not remove unnecessary services, ports, or protocols from their information assets, which increases the points of vulnerability and vectors of potential attack (see FIGURE 13). In addition, one out of four critical systems does not undergo security testing before being deployed into a production environment, where users will access live data.

FIGURE 13: SECURITY CONTROLS FOR DEPLOYING CRITICAL SYSTEMS

Do critical systems get full security testing before deployment?	73%
Do you harden production systems by removing unnecessary services?	66%
Is security testing performed using a defined and documented methodology?	56%
Is availability testing conducted on redundant systems?	57%
Is penetration testing performed by an independent third party?	52%

SOURCE: MARSH

GOVERNANCE AND PROGRAM MANAGEMENT

Although most organizations reported having strong information-security policies, many lack the basic practices and procedures necessary to educate their users, including the executive team, about cyber risks. These structures enable organizations to prioritize their responses and to permeate organizational culture with safe cyber practices. For example, a chief information security officer (CISO) serves as a bridge between management and security, but almost half of the assessed companies had not appointed a CISO or comparable position (see FIGURE 14). In addition, more than one of every four organizations lacked a centralized IT security team.

FIGURE 14: GOVERNANCE AND PROGRAM MANAGEMENT

Does your company have information security and privacy policies?	84%
There is a centralized information security team or equivalent in place.	74%
Has your company dedicated a security officer (CISO or CSO) either within or outside the IT organization?	53%
Have you communicated the name and contact information for your information security team to users?	61%

SOURCE: MARSH

A CALL TO ACTION

A healthy risk management program depends on focused engagement at the board and senior leadership level — the only place where enterprise risk management consistently comes together. Boards are uniquely equipped to push organizations to bring together their organizations' chief security officer (CSO), chief information officer (CIO), CISO, enterprise risk management (ERM) team, and leaders of individual lines of business. As consensus grows on the importance of active board engagement and oversight over cybersecurity risks, board-level input on information and network security issues will increasingly become the expectation of state and federal regulators[3].

However, the board alone cannot address this problem. Cybersecurity is a complex risk and collaboration within the organization and among partnering stakeholders, including government agencies, security professionals, and the risk management industry, is critical. Companies rely on government support to clarify the threat and set expectations for best practices, such as those announced in the NIST Framework. The insurance sector can drive the adoption of best practices through underwriting standards and leverage security expertise to strengthen individual organizations. Lastly, companies, federal regulators, and underwriters will depend on the security community to define the standards that will best protect networks.

3 See SEC Cybersecurity Roundtable, comments of Mary Jo White, March 26, 2014, available at http://www.sec.gov/spotlight/cybersecurity-roundtable.shtml.

Accordingly, as we move forward with greater efforts to address the risk, each step should emphasize greater cooperation.

- Boards should consider engaging cyber-savvy advisors to provide an independent perspective on the organization's current level of risk management maturity, and seek risk assessments that will compare those practices with federally recognized best practices. Often, the risk-assessment process can be informed and implemented by the placement of cyber insurance coverage.
- Risk-assessment experts should help companies develop a systematic understanding of the potential threats, related vulnerabilities, and possible attack paths, as well as the consequences that could result from an intrusion. Recognizing that no network is impregnable, companies should consult with risk management professionals on the best approach for insuring against those consequences.
- Insurance carriers should embrace and drive best practices, like those announced in the NIST Framework, by rewarding insureds who demonstrate their implementation following an independent assessment.
- Federal agencies should closely coordinate with insurance and security communities to achieve a critical mass of support for implementation. The recent effort of the collaborative process that yielded the first version of the NIST Framework serves as a model for such collaboration; future efforts should replicate that effort and avoid a splintering of priorities.
- While cyber insurance is already an element in a risk strategy that many companies implement, it can serve also as a vehicle for improving cyber hygiene across the nation. Federal policy makers can help drive private-sector adoption of best practices with stronger incentives, such as protecting organizations that demonstrate implementation of best practices against punitive litigation. In turn, liability protections could help insurers quantify exposures, especially for the largest risks, and further develop the risk transfer market.

Our nation is at a crossroads. There is a persistent drumbeat of attacks targeting all industries, which aim to steal customer data and intellectual property, disrupt networks and business operations, and destroy critical infrastructure. Unless confronted, these exploits could erode the stability of critical sectors of our economy and potentially threaten our security.

At the same time, awareness, preparedness, and detection of cyber threats has grown, along with an unprecedented level of collaboration among industry, government agencies, security professionals, and risk management experts. By embracing this greater collaboration, our nation will better identify vulnerabilities through risk assessments, share threat information among stakeholders, implement and monitor defenses, and create the solutions to respond to the exposure of cyber risk.

MARSH & McLENNAN COMPANIES

ABOUT THE CHERTOFF GROUP

The Chertoff Group is a premier global advisory firm focused exclusively on the security and risk management sector. The Chertoff Group helps clients grow and secure their enterprises through business strategy, risk management, and merger and acquisition services. The Chertoff Group, and its investment banking subsidiary Chertoff Capital, have advised on multiple M&A transactions totaling more than $6 billion in deal value. Headquartered in Washington DC, the firm maintains offices in Austin, Houston, London, New York, and San Francisco. For more information about The Chertoff Group, visit www.chertoffgroup.com.

ABOUT MARSH & MCLENNAN COMPANIES

MARSH & McLENNAN COMPANIES (NYSE:MMC) is a global professional services firm offering clients advice and solutions in the areas of risk, strategy, and human capital. Marsh is a global leader in insurance broking and risk management; Guy Carpenter is a global leader in providing risk and reinsurance intermediary services; Mercer is a global leader in talent, health, retirement, and investment consulting; and Oliver Wyman is a global leader in management consulting. With annual revenue exceeding $12 billion, Marsh & McLennan Companies' 55,000 colleagues worldwide provide analysis, advice, and transactional capabilities to clients in more than 130 countries. The Company prides itself on being a responsible corporate citizen and making a positive impact in the communities in which it operates. Visit www.mmc.com for more information.

USDG7808