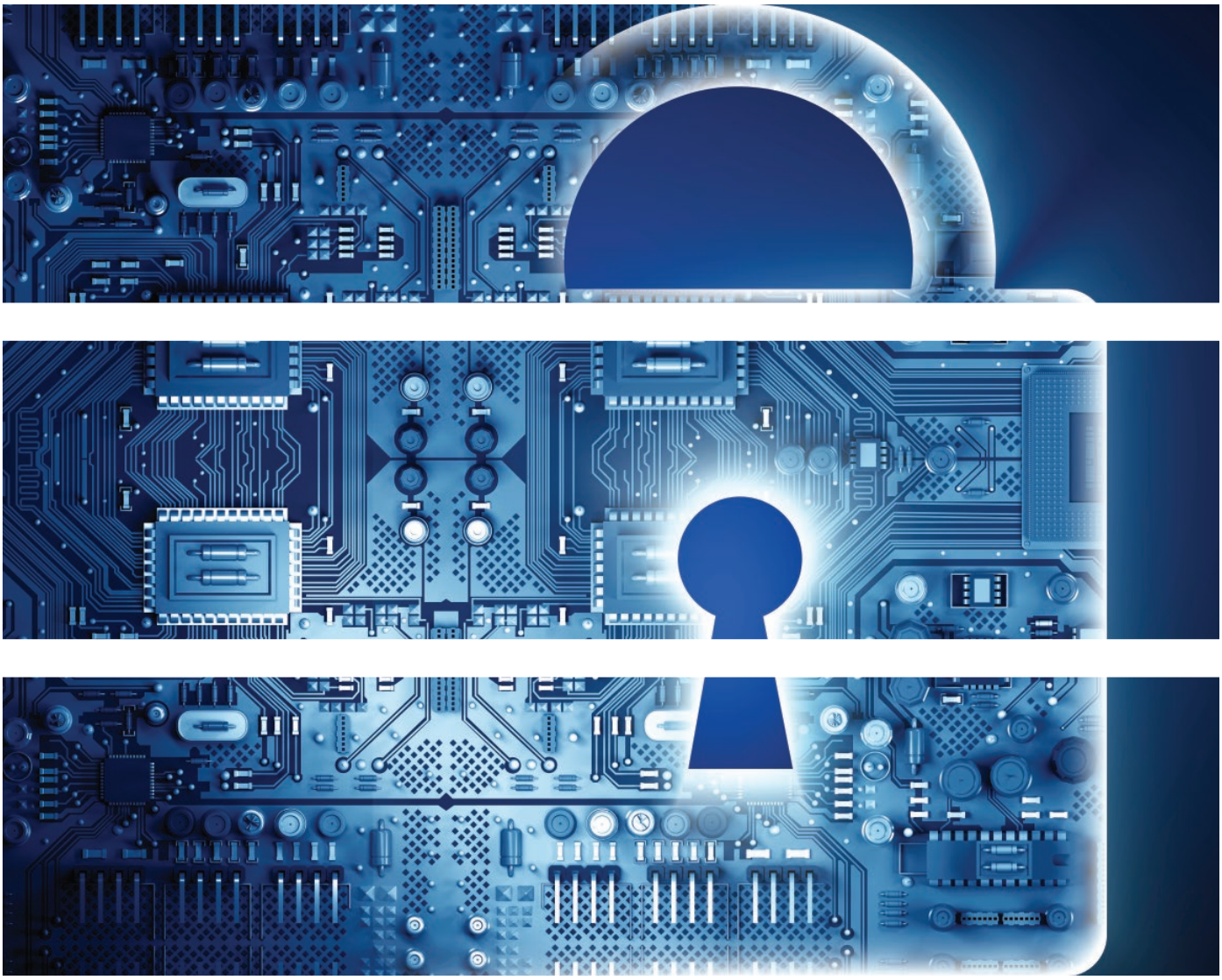
Hewlett Packard Enterprise | FireEye | MARSH & McLENNAN COMPANIES

Special report

Cyber resiliency in the Fourth Industrial Revolution

A roadmap for global leaders facing emerging cyber threats



4th

Industrial Revolution—
complexity increases over time

1784

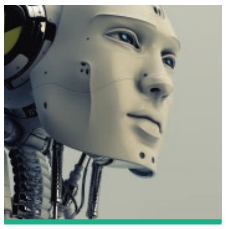
Steam engine

1870

Mass production

1969

Information technology



2020

Cyber-physical systems

Fourth Industrial Revolution cyber-physical systems

- 100 billion connected devices
- Digital industrial control systems
- Machine-to-machine
- Mass customization
- Global sensor-net overlay
- Autonomous vehicles/homes
- Digital service avatars (iConcierge)

Breaches are inevitable; resilience is necessary

The First Industrial Revolution, in the late 18th century, was driven largely by steam engines. The second, in the late 19th century, introduced mass production and the division of labor. The third, in the late 20th century, involved digital automation and information technology.

Only decades later, the world is now on the cusp of a Fourth Industrial Revolution. This new world revolves around cyber-physical systems, the Internet of Things, and the Internet of Services. Our hyper-connectivity in this new digital world has been a boon for productivity—connecting and executing tasks with a speed that was inconceivable even five years ago.

With that hyper-connectivity, however, comes the risk of significant disruption through a cyberattack—the potential consequences of which have escalated dramatically. Until recently, cybersecurity largely meant defending against website defacements, denial of service attacks, and data breaches. The threat posed by them, however, is now morphing into the realm of physical assets and critical infrastructure.

While this risk intensifies, businesses, governments, customers, and individuals around the world demand even more from the new economy. Engaged in a repeating loop, the world is more dependent on technology, even as the risk posed by that dependence increases exponentially.

It's like running in a race without a finish line. As organizations bolster their defenses, adversaries adjust their strategies and methods of attack. New "zero day" attacks are conceived and launched. Organizations scramble to respond. This dynamic will continue—from our vantage point—for decades to come.

Our three companies—each a leader in its space—have come together to offer a roadmap for global leaders to respond to this threat. As it's become all too clear, there is no panacea or silver bullet. So, accepting the premise that breaches are inevitable, we set forth an approach for building cyber resilience. The critical objective is to enable organizations to withstand significant cyberattacks and continue core operations.

Mike Nefkens
Executive Vice President &
General Manager
Hewlett Packard Enterprise

Kevin Mandia
President
FireEye

Peter J. Beshar
Executive Vice President &
General Counsel
Marsh & McLennan Companies

The path to cyber resilience

Cyber breaches happen. That is the new reality. However, with cyber resilience, organizations can respond with agility to cyberattacks. So, despite an attack, the organization carries on—patients are treated, power is generated, commerce flows.

This new approach emphasizes five fundamental steps:

1. Identify your most critical assets—What do you have that is most valuable to others?
2. Gather intelligence on cyber threats—Who are the bad actors?
3. Understand your digital profile—What does your online activity signal to others?
4. Build a resilient system—What are the most critical elements of defense?
5. Plan for a breach—What can you do now to prepare for a crisis?

Building a moat around your organization has proven ineffective. In a dynamic threat environment, it is simply not possible to construct an impenetrable firewall. Instead, these five steps are designed to enhance your organization's ability to anticipate attacks, respond with agility, and maintain core operations.

Perfection is not the goal of this methodology, and not every organization will have equal need or resources to implement each step. Rather, this approach is intended to guide you on how to identify cyber priorities and develop a risk-based response.

1. Identify your most critical assets

All data is not created equal. Yet, the traditional approach to cyber defense is to construct a perimeter and treat all assets in a similar fashion. This method can lead to inefficiencies and misalignment of resources.

A better approach begins with a simple question: Why should my organization be concerned about cybersecurity? Answering this question with precision requires identifying which data, applications, and systems are essential for your organization to conduct operations, and then developing a cyber strategy that is driven by protecting core business functions—and not merely responding to threats.

So, what do you have to lose? What are your most critical assets? Intellectual property? Turbines? Customer data? Medical histories? Trade secrets? Proprietary financial data? Industrial control systems?

2. Gather intelligence on cyber threats

Evolution in the nature and sophistication of cyber threats has been stunning. And, it is only beginning.

In just the past few years, hackers have grown far more sophisticated, their attacks more complex, targets more encompassing, and the impact of those attacks more damaging. There is now a highly advanced underground online economy where hacker tools and illicitly obtained data are readily available. Companies must now confront the specter of data manipulation, extortion, and potential acts of terrorism. Understanding the ever-changing threat landscape plays an essential role in cyber resiliency.

A potential inventory of assets

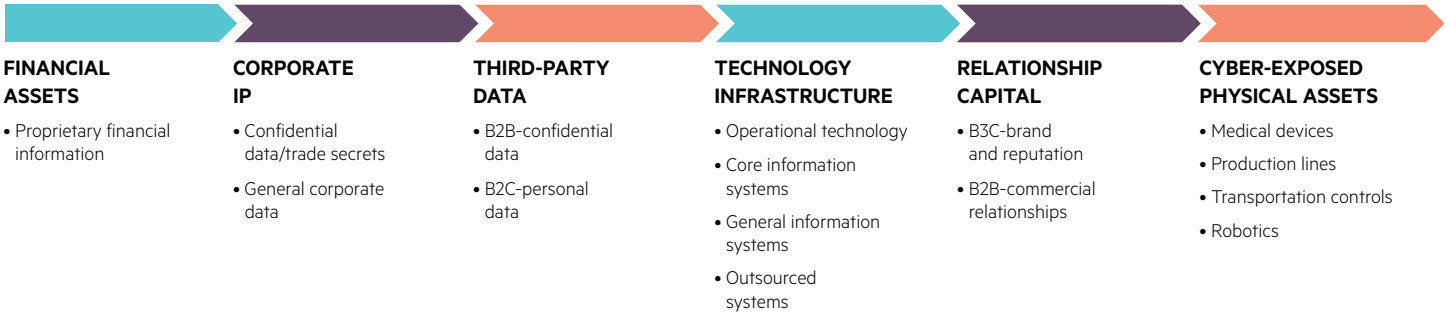


Figure 1: Sample inventory of assets[1]

The cyber-threat landscape

Two other factors accentuate the threat posed by cyberattacks. First, on average, it takes an organization more than 200 days to realize that its systems have been breached.[2] Indeed, in multiple instances, breaches have been undetected for years. Second, in more than 65 percent of cyberattacks, it is a third party, and not the organization itself, which discovers that a breach occurred. For an organization to adopt cyber resilience, mature cyber threat intelligence is essential to identify threats and reduce the period of exposure.

Attacks on physical assets and critical infrastructure

Over the past several years, most publicly reported breaches have concerned data theft—such as credit cards, Social Security numbers, and patient records. Attacks are now morphing into the realm of physical assets that threaten the critical infrastructure—including electric grids, transportation systems, satellites, civilian nuclear facilities, and telecommunications networks. By exploiting industrial control systems and critical infrastructure, cyberattacks now pose a threat to public safety and economic security.

FireEye identified a series of advanced threat actors who possess a high-cyber capability to conduct network attacks and use a range of tactics and target critical industries worldwide. Recent threats to operational technology included:

- A new type of malware, discovered by FireEye in 2015, which creates a "loop" that sends instructions to hardware to alter its operations while appearing, on the surface, to be working properly.
- A malware discovered by Norwegian law enforcement in 2014 that compromised 50 Norwegian energy companies.
- The leaking of partial blueprints of a South Korean nuclear reactor by hacktivists linked to state actors.

[1] Source: Marsh

[2] M-Trends 2015: A View from the Front Lines, Feb. 2015, Madiant

	NUISANCE	DATA THEFT	CYBER CRIME	HACKTIVISM	NETWORK ATTACK	MALICIOUS INSIDER
Objective	Access and propagation	Economic, political advantage	Financial gain	Defamation, press and policy	Escalation, destruction	Financial gain, defamation, whistleblowing
Example	Botnets and spam	Advanced persistent threat	Credit card theft	Website defacements	Destroy critical infrastructure	Theft of IP
Targeted	No	Yes	Yes	Yes	Yes	Yes
Character	Automated	Persistent	Opportunistic	Conspicuous	Conflict driven	Informed and trusted

Figure 2: Actors on the cyber-threat landscape[3]

Within the energy sector in particular, potential targets include offshore drilling rigs, power generation plants, and pipelines exposed by direct connectivity to the Internet and enterprise IT networks.[4]

Compromise assessments and penetration testing—the "inside-out" approach
With increasing frequency, organizations rely on two tools to identify critical vulnerabilities: compromise assessments and penetration "pen" tests. Compromise assessments evaluate network end points for indicators of compromise or other anomalous activity. Experts use this tool, and pen tests, which analyze your internal security protocols, to assess your vulnerability.

Based on hundreds of tests carried out by FireEye, it is clear that the vast majority of systems are susceptible to attacks—despite traditional security controls in place. Consistently, indicators of compromise are discovered by forensic imaging, malware analysis, and review of incident log activity. Implementing a continuous state of testing, however, builds cyber resilience by finding and fixing critical weakness more quickly.

3. Understand your digital profile

Big Data approach to analyzing cyber risk—the "outside-in" perspective
Hackers look for opportunity and probe for weakness—a combination of the value of your assets and vulnerability of your systems. Big Data can now be harnessed to assess the likely motivation for and potential susceptibility to cyber events by relying exclusively on data points beyond an organization's perimeter. This is the outside-in approach.

In the digital era, each organization creates a footprint through its online activity. Your business, just like an individual, leaves a trail of digital breadcrumbs behind.

For example, do your servers share web hosting platforms with others, or worse, with highly targeted companies? Can hackers spot instances of unpatched software by monitoring browsers used by employees to access the Internet? Is your organization subject to activity on the so-called "dark web?" What do your job postings for IT positions reveal about your operations? Will poor employee morale, as reflected in external surveys, correlate to insider attacks? What is your web presence and how strong is it?

Aggregating these and hundreds of other data points over time yields susceptibility and motivation scores that can be used to benchmark your organization against past performance and the performance of your peers. The susceptibility of an organization is defined by its technology, people, and processes; motivation describes why an outside actor would attack your organization. If a hacker probes two companies with similar networks and one has user credentials available on the dark web, which is the hacker more likely to attack?

[3] Source: FireEye-Mandiant

[4] In fiscal year 2014, the energy sector led all industries for the number of cyberattacks reported to the Industrial Control Systems Cyber Emergency Response Team at the U.S. Department of Homeland Security, with 79 reported attacks accounting for 32 percent of reported attacks. ICS-CERT Monitor, Sept. 2014 to Feb. 2015, **https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf**.

As an example, Figure 3 is a scatter graph of 212 companies in the power industry ranked by susceptibility and motivation. This same analysis can be conducted on any sector or industry.

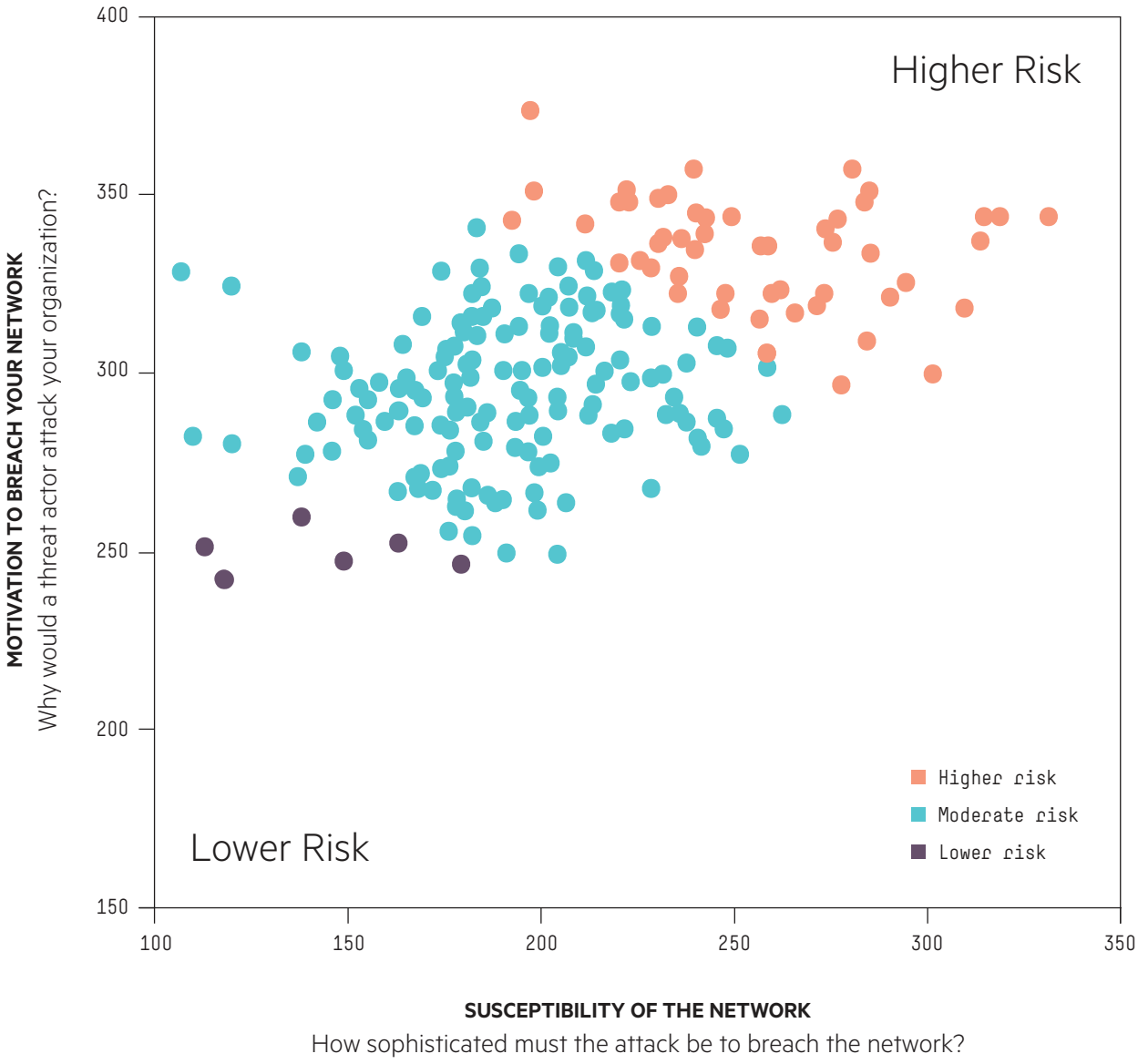


Figure 3: U.S. power, oil, and gas companies with $1 billion or more in annual revenue[5]

[5] Source: Marsh Global Analytics

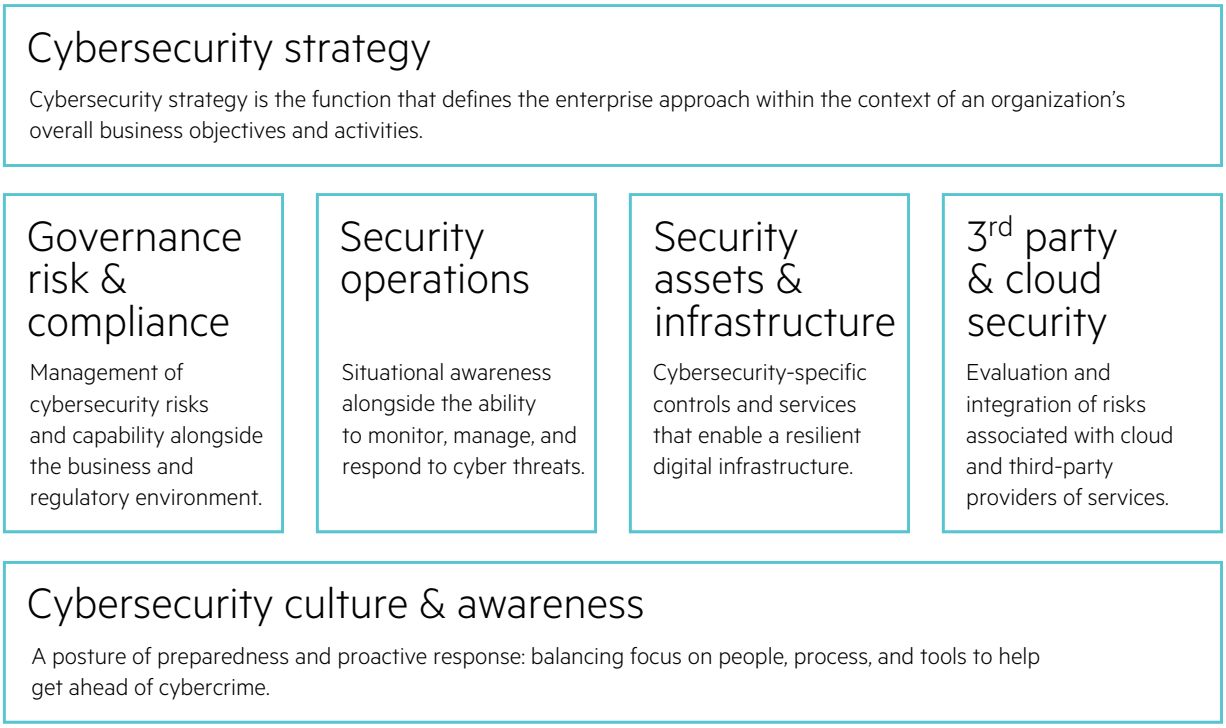


Figure 4: Six core elements of cybsersecurity[6]

4. Build a resilient system

With a deeper understanding of your critical assets and overall threat environment, the next step is to develop a strategic framework for deploying your resources. This process should address six core elements:

- Cybersecurity strategy
- Governance, risk, and compliance
- Security operations
- Security assets and infrastructure
- Third party and cloud security
- Cybersecurity culture and awareness

[6] Source: HPE

- **Cybersecurity strategy**
  An organization's overarching strategy determines its risk management goals. Objectives may be as basic as safeguarding data and ensuring confidentiality, integrity, and availability or improving security by reducing vulnerabilities. More complex priorities include benchmarking progress against an established industry standard.

  Challenge: Stove-piping
  Poor communication, lack of management engagement, and an absence of board oversight are barriers to effective development of a cyber strategy. Cyber-risk management is an enterprise concern, not simply a technology issue. However, even organizations that accept this notion can struggle to embrace sound enterprise risk management practices unless senior management takes ownership of this issue, and the board provides necessary oversight.

- **Governance, risk, and compliance**
  Almost more than any other risk a company faces, are the myriad of stakeholders involved in building cyber resilience. The board of directors. Multiple members of the senior management team, including the CEO, CFO, general counsel, CIO, head of HR, and chief information security officer (CISO). Your employees. Your vendors. The role of the board and each member of senior management, in particular, should be clearly articulated in order to enhance your organization's agility to respond to a dynamic threat and avoid conflict.

  Challenge: An avalanche of new laws
  Cybersecurity laws, regulations, and policies are fragmented and in a constant state of flux. It is estimated that more than 140 new pieces of security or privacy legislation will be passed globally in the next two years. There is almost no commonly accepted framework that an enterprise can use across industry, and national and regional environments. Organizations must strive to adopt enterprise standards and protocols to guide the appropriate allocation of resources.

- **Security operations**
  A company's security operations identify threats to the organization and direct real-time responses to mitigate damage and business disruption. A key responsibility of security operations is to implement tactical controls that keep pace with evolving threats. For example, as social engineering attacks like spear phishing prove to be distressingly effective, detonation or "sandbox" software may mitigate this risk. As organizations struggle to protect personally identifiable information, data loss prevention (DLP) software is an important component of an organization's security toolkit.

  A security operations center (SOC) forms the core of the security operations function, providing situational awareness alongside the ability to monitor, manage, and respond to cyber threats. In its 2015 Enterprise Report on the State of Security Operations, Hewlett Packard Enterprise (HPE) found that 20 percent of SOCs were not providing minimum security monitoring capabilities, while 87 percent were not meeting recommended levels of security.

  Challenge: Attribution
  The inability of companies to identify the sources of attacks provides hackers with a significant advantage. Advanced attackers acting with impunity rapidly change tactics to bypass traditional defenses. Industry and government leaders must accelerate their commitment to gathering and sharing threat intelligence to improve attribution.

- **Security assets and infrastructure**

  These include data centers, servers, software, and personal devices, which should employ controls that protect data, users, applications, and networks from threats. Legacy systems create inherent vulnerabilities for many reasons, including the challenge of patching known software vulnerabilities.

  A multi-layered defense protects all forms of infrastructure, from conventional networks to emerging cloud and mobile platforms. The first line begins with firewalls at the perimeter. Next, systems are segmented to isolate and protect critical operations. Within a system, applications are protected through tight controls around access privileges, including two-factor authentication. At the most granular level, data at rest or in transit is protected through encryption.

  Challenge: Shrinking the attack surface

  The rapid development of the Internet of Things and proliferation of mobile devices create an ever-expanding set of entry points for hackers. For many organizations, data sprawl is the top cyber vulnerability. To shrink your attack surface, your organization should review its network architectures to eliminate unneeded Internet connections and avoid accumulating data for no reason. Limiting your attackers' opportunities is as important as any investment in technology.

- **Third party and cloud security**

  A key lesson of prominent data breaches over the past two years is that any organization is only as cyber resilient as the weakest of its third-party vendors. Regulators, focused on third-party vulnerabilities, are introducing cybersecurity mandates related to vendors. An organization must now actively manage its network supply chain ecosystem, and align controls with the vendor's network activities. At the same time, moving data and applications to the cloud—with the right safeguards—can *increase* security and resilience.

  Challenge: Assessment of cloud performance

  While outsourcing offers great advantages and, at times, improved security, it also adds complexity. Organizations should establish controls that:

  – Limit vendor access within your network.

  – Avoid overreliance on any specific outsourced vendor.

  – Impose an obligation on vendors to provide notice before transferring your data to other jurisdictions.

- **Cybersecurity culture and awareness**

  Evolving culture to meet threats—Technology solutions, including end-to-end encryption, cannot eliminate cyber risk. More than 90 percent of successful cyberattacks are launched via spear phishing campaigns. Accordingly, creating a cyber-aware culture and providing training for employees are critical elements of cyber resilience. Many, if not most, cyber breaches trace back to human error. Accordingly, organizations must focus on their people and processes for addressing cyber risk. Cyber resilience must reside in the organization's DNA, so it becomes an organizational imperative to protect and enable digital interactions.

  Challenge: Lack of focus on the user

  Training should never grow stale or formulaic. Employees can be an organization's greatest vulnerability. A key challenge is to convert this vulnerability into an asset by training employees to become the first responders—who recognize incidents and protect the organization.

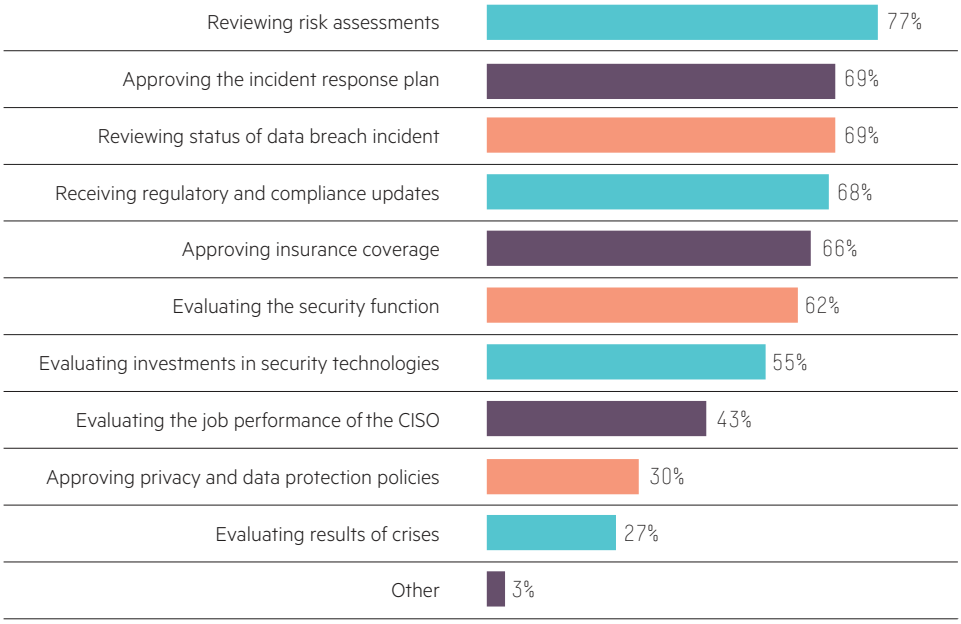


Figure 5: Role of senior executives in incident response[7]

5. Plan for a breach

Cyber resilience through response and recovery
Almost inevitably, an organization's efforts to prevent attacks will eventually fail. Cyber resilience depends on an organization's ability to respond to a significant breach and continue operating effectively. In this regard, there are two important steps to consider: contingency planning and the mitigation and transfer of financial risk.

Contingency planning
Operating on the premise that every institution will ultimately be breached, contingency planning is critical. For example:

- Does your organization have a written incident response plan?
- Which executive will lead your incident response?
- Have you engaged in a simulated exercise to test your plan?
- Which outside advisors will you depend on? Have you engaged them on retainer?
- Have you developed relationships with key government officials?

To the extent that an organization has taken these steps, many will have limited their preparations to a data breach. With the looming threat posed to critical infrastructure, it is important that organizations conduct contingency planning against threats to physical assets as well.

Bottom line—in the absence of adequate preparation, organizations that are victimized by a cyberattack rapidly become, in the eyes of regulators, customers, and consumers, the perpetrator of the offense.

[7] *The Importance of Senior Executive Involvement in Breach Response*, Ponemon Institute LLC, sponsored by HPE Security Service, October 2014

Mitigation and transfer of financial risk

Cyber insurance can bolster cyber resilience by creating important incentives that drive behavioral change. As a threshold matter, the simple act of applying for insurance forces insureds to assess the strength of their cyber defenses. And, do so against a rapidly changing platform. Organizations are increasingly embedding technology and developing software and applications for their consumers in order to stay competitive. Oftentimes, however, there are inadequate tollgates for security or privacy. While risk transfer cannot substitute for proper preparation, it remains a component of cybersecurity strategy.

Whether prodded by a board of directors or desire to obtain coverage as inexpensively as possible, prospective cyber insurance buyers conduct gap analyses against industry benchmarks. Underwriters scrutinize whether these companies have disciplined procedures for patching software, monitoring their vendor networks, and preparing for breaches. Cyber insurance also prompts an evaluation of potential consequences by using statistical modeling to assess different damage scenarios.

Once a cyber insurance policy is purchased, the insurer has the incentive to help its policyholder avoid or mitigate cyberattacks. As a result, many insurers now offer monitoring and rapid response services to policyholders. Ultimately, in the event of a disabling attack, cyber insurance can limit an institution's economic damage and help accelerate its recovery.

This combination of economic incentives has driven significant increases in the purchase of cyber insurance. Figure 6 shows the 2015 cyber insurance take-up rates by industry sector. The number of Marsh U.S.-based clients purchasing standalone cyber insurance increased 27 percent in 2015 compared with 2014.

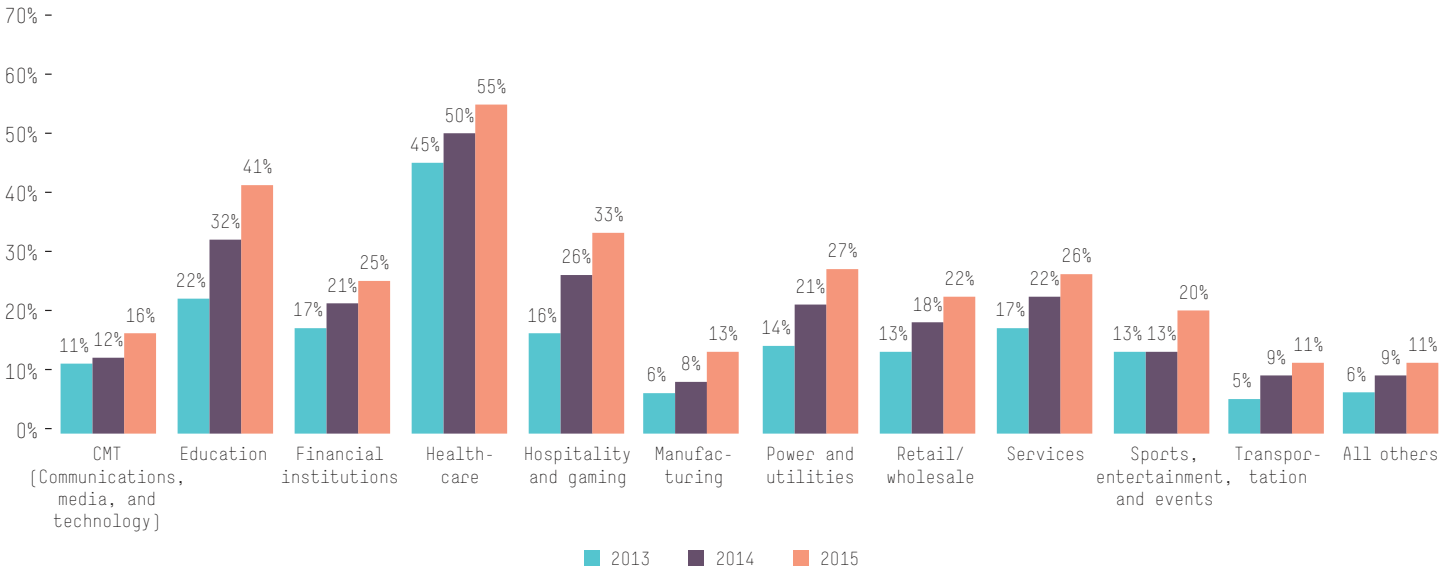


Figure 6: Cyber insurance take-up rate by industry[8]

[8] Source: Marsh Global Analytics

A call to action

Hewlett Packard Enterprise, FireEye, and Marsh & McLennan Companies joined together to offer this roadmap for cyber resilience. Our intent is to provoke thought and action—not fear and paralysis.

Look at your organization through a different lens. Perfection is not the goal. As in the previous industrial revolutions, organizations that exhibit the greatest agility in responding to changing circumstances will be able to achieve all that the Fourth Industrial Revolution has to offer.

About the authoring organizations

Hewlett Packard Enterprise
Creating a technology platform that helps your business thrive in a disruptive marketplace takes experience and an understanding of how IT systems interact with each other—and the people who use them. Let Hewlett Packard Enterprise be your transformation partner of choice—benefit from our unparalleled global reach, portfolio of world-class security service offerings, expertise, products, and technologies. **hpe.com/services/security**

For more information, please contact Andrzej Kawalec, HPE Security Services Chief Technologist at **andrzej.kawalec@hpe.com**

FireEye
FireEye is changing the way organizations worldwide prepare for and respond to advanced cyberattacks. Combining industry-leading security technology, threat intelligence, and incidence response expertise, FireEye provides a complete global threat management platform that stops attacks that bypass traditional security tools. FireEye detects and resolves these cyber breaches in minutes, limiting the loss of data and the damage to intellectual property and brand reputation. **FireEye.com**

For more information, please contact **info@fireeye.com**

Marsh & McLennan Companies
Marsh & McLennan Companies provide advice and solutions to mitigate cyber risk. As the world's most trusted cyber insurance broker, Marsh, Inc. advises over 1000 clients regarding network security and privacy issues and has won Advisen's award for Cyber Broker of the Year—2014 and 2015. **www.marsh.com/us/services/cyber-risk.html**

For more information, please contact Thomas Reagan, Cyber Practice Leader at **thomas.reagan@marsh.com** or Robert Parisi, Cyber Product Leader at **robert.parisi@marsh.com**

Hewlett Packard Enterprise | FireEye | MARSH & McLENNAN COMPANIES

Sign up for updates

★ Rate this document

4AA6-3809ENW, January 2016