FIREEYE™ | MARSH & McLENNAN INSIGHTS

ADVANCING CYBER RISK MANAGEMENT

FROM SECURITY TO RESILIENCE

Table of Contents

AUTHORS

Jaclyn Yeo
Research Manager
Marsh & McLennan Insights
Jaclyn.yeo@mmc.com

Rob van der Ende
Vice President, Mandiant APJ
FireEye
Rob.vanderende@mandiant.com

CONTRIBUTORS

FireEye

Kevin Mandia, FireEye
Rena Stern, FireEye
Chris Nutt, FireEye
Patrick Neighorn, FireEye
Merwin Shanmugasundaram, FireEye

Marsh & McLennan Companies

Kevin Richards, Marsh Risk Consulting
Kelly Butler, Marsh
Naureen Rasul, Marsh
Jono Soo, Marsh
Paul Mee, Oliver Wyman
Jayant Raman, Oliver Wyman
Alon Cliff-Tavor, Oliver Wyman
Wolfram Hedrich, Marsh & McLennan Insights
Leslie Chacko, Marsh & McLennan Insights
Jessica Koh, Marsh & McLennan Insights

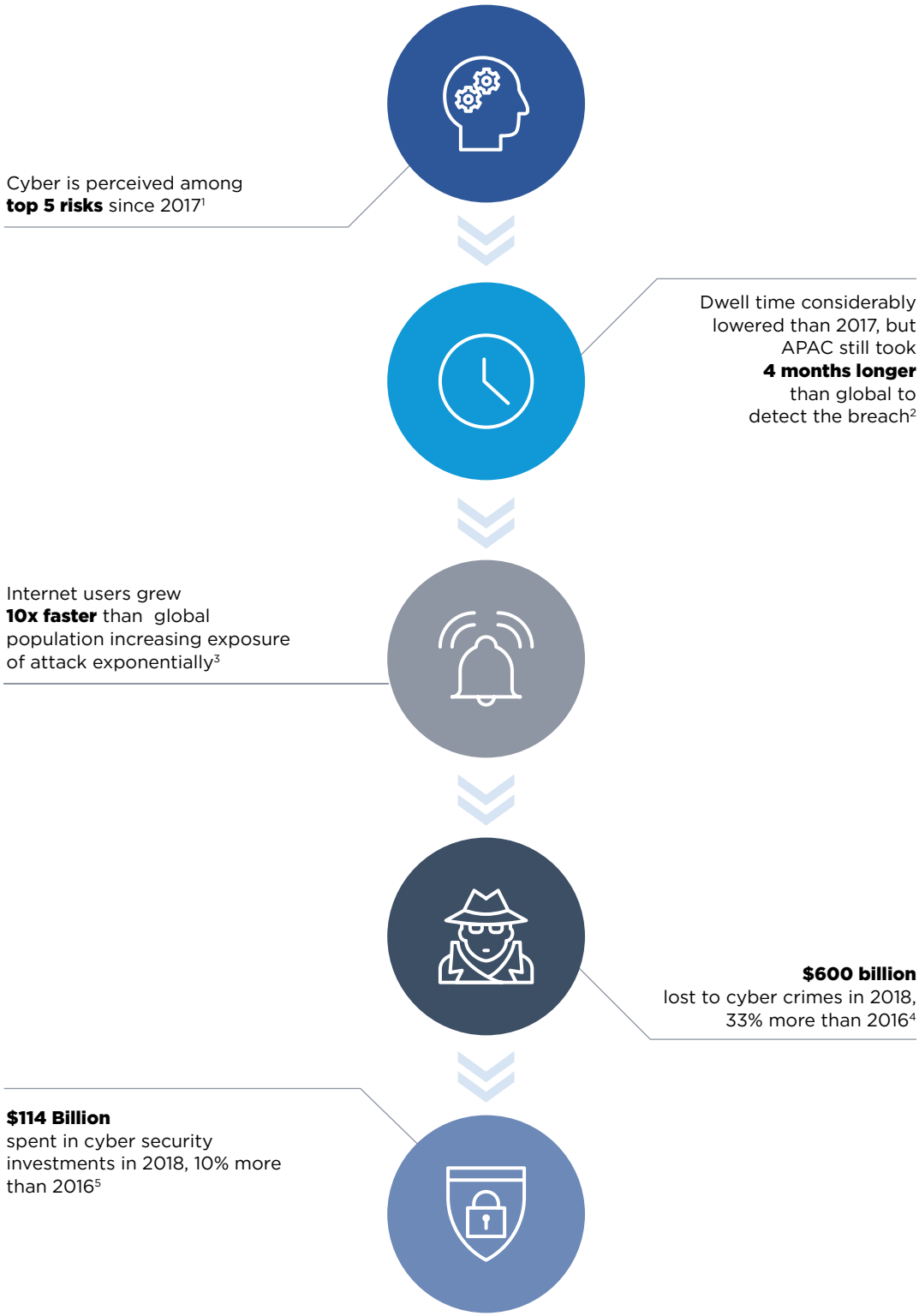
Executive Summary

Since 2017, risk experts have consistently ranked large-scale cyber attacks and data fraud among the top five mostly likely risks around the world. Despite growing anxieties about cyber threats, cyber resilience strategies and investments continue to lag. Globally, the time taken to discover a data breach has considerably lowered since 2017, but organizations in the Asia-Pacific region took four months longer than the global median. Internet users are growing 10 times faster than global population, exponentially increasing the surface area of attack. For example, in 2018, the total cost of cyber crimes grew by a third compared to 2016, to $600 billion, but investments in cyber security only increased 10 percent over the same period.

These trends point to a growing imperative and urgency for cyber resilience in the digital age.

Figure 1. Cyber threats and their impact.

Dwell time:
Dwell time is calculated as the number of days an attacker is present on a victim network, from first evidence of compromise to detection. The median represents a value at the midpoint of a sorted data set.



1 World Economic Forum (2019). The Global Risks Report 2019, 14th Edition.
2 FireEye (2019). M-Trends 2019.
3 Miniwatts Marketing Group (May 20, 2019). Internet World Stats, Usage and Population Statistics.
4 McAfee (February 2018). The Economic Impact of Cybercrime - No Slowing Down.
5 Gartner (August 15, 2018). Gartner Forecasts Worldwide Information Security spending to Exceed $124 Billion in 2019.

Rapidly evolving threats and infiltration techniques have rendered traditional cyber defense strategies insufficient and ineffective. The emerging threat vectors and speed of change amplified by the digital transformation cannot be addressed by traditional means. Globally, laws are also changing to keep pace as cybercrime evolves, knowing no boundaries. Therefore, organizations must be nimble and agile to keep pace with policy changes, especially when expanding across different jurisdictions.

This report highlights three strategic imperatives to strengthen cyber resilience:

- **Understand *(know your threats)*:** Identify organization- and industry-specific cyber threats and regulations calls for robust strategies that include cross-disciplinary considerations.
- **Measure *(know yourself)*:** Quantify the potential financial impact of cyber exposures to compare against the level of risk appetite acceptable to the board. This will determine the amount of investment necessary to mitigate and transfer any residual risk.
- **Manage *(know what you can do)*:** Proactively manage cyber risks by having clear action plans based on your capabilities and capacities to protect against cyber criminals.

It is inefficient and impractical to expect organizations to be ahead of every threat, but organizations should at least be on par with the evolution of cyber threats while ensuring compliance with changing laws and regulations. While cyber attacks are inevitable, proper preparation is the essential element that sets resilient organizations apart from the rest in managing risk, minimizing damage, and recovering quickly from any incidents.

Based on a True Story

A Classic Cyber Attack

Jun 27, 2017 – On a typical afternoon in the office, several work computers spontaneously restarted. Soon, colleagues were gathering at the tech help desk, almost all carrying their laptops. The screens were either blacked out or flashing messages in red and black lettering, "Repairing file system; DO NOT TURN OFF the computer," or "Oops, your important files are encrypted."

The latter message also demanded a payment of $300 worth of bitcoin to decrypt.

The frenzied response to this shock was a scene simultaneously replicated across regional headquarters and country offices around the world. Machines connected to the internet—laptops, servers, routers—fell like dominos, infected by the malicious ransomware. Within minutes, an emergency network shutdown was called to quarantine the infections, but the damage was already done. The main network and domain controllers were compromised and no one knew exactly what to do.

Nevertheless, the company endured and managed to rebuild the infrastructure network within 10 days of the attack to enable some business continuity. Full recovery took months and the initial financial losses due to business interruptions and client compensations were estimated at $300 million.

Post-incident investigations on the malware subsequently revealed further jarring news. In the months leading up to the malware attack, IT executives had requested a pre-emptive security review of the organization's global network, highlighting several vulnerabilities from software patching to outdated operating systems. But the cyber security review was never implemented because it was "over-budget" and not integrated into the key performance indicators for the senior management team.

Now, months later, many organizations are still learning and relearning some of these painful lessons.

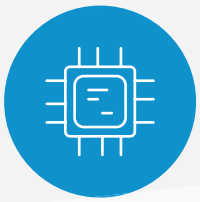
This story is not fiction and certainly not unique. Real companies go through experiences just like this, sometimes from a suspected state-sponsored attack such as this ransomware or simply clicking on embedded weblinks in emails that redirect to a phishing site from where network access and data records are compromised. The consequences are often devastating.

Cyber Risk: A Top Concern

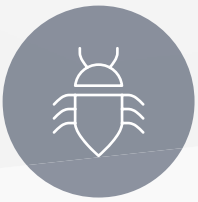
Technology continues to play a profound role in shaping the global risk landscape for individuals, businesses, and governments. Risk experts around the world continue to rank massive data fraud and theft and cyber attacks as their greatest and most likely risks over the next decade, a pattern that is consistent with previous years.[6] Most risk experts also expect cyber attacks to have a much greater impact through business disruption and the targeted theft of money, data and intellectual property. Our increased dependence on pervasive, integrated digital technologies also increases anxiety around cyber security (Fig. 2, 3).

Figure 2.
Factors that increase cyber risk in a digital global economy.[7]

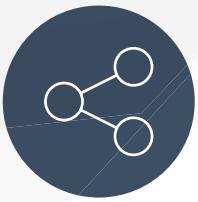
Pace of Innovation
Companies are innovating more and more rapidly



Technology Complexity
Technology is getting more intelligent, sophisticated and pervasive



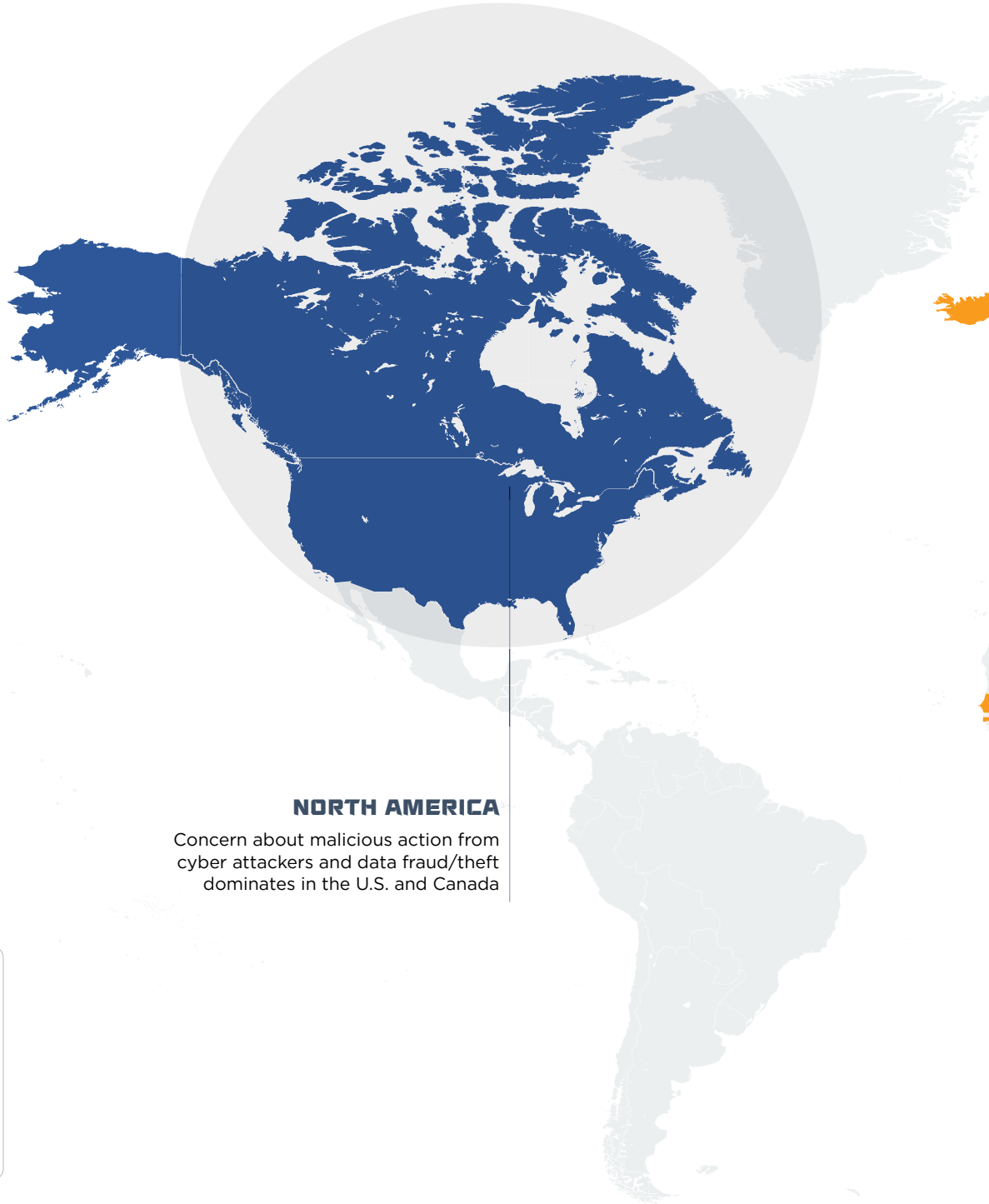
Attack Sophistication
Actors are increasingly organized, sophisticated and devious



Data Sharing and Interconnectivity
Growing Interconnectedness combined with massive increase in velocity, volume and variety of data

6 World Economic Forum (2018). Regional Risks for Doing Business 2018.
7 Ibid.

Figure 3.
Cyber risks: locations of greatest concern.[8]

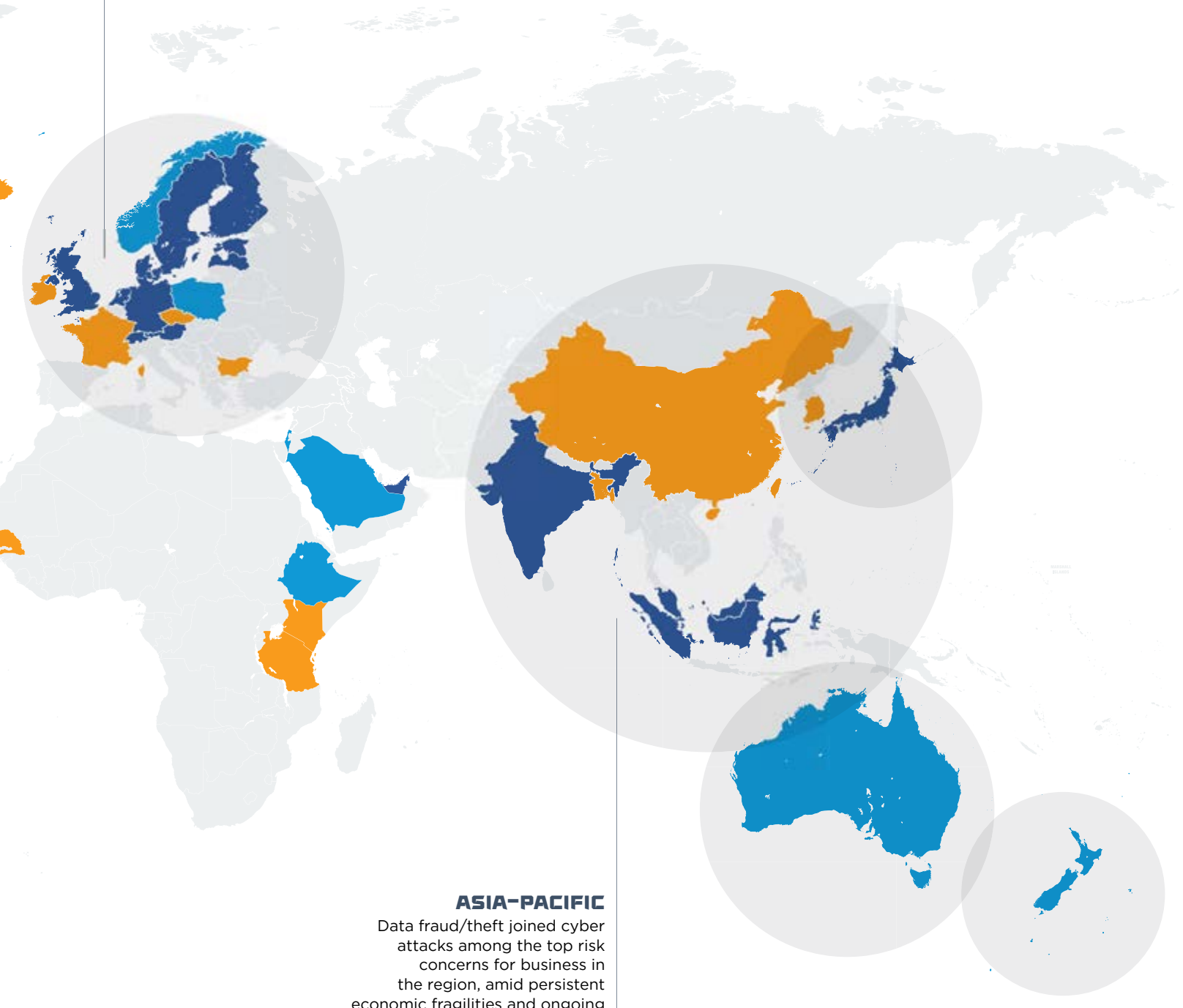


Cyber-related risks include cyber attacks, and data theft and fraud. Countries are shaded if either risk appeared in their top three risks of most concern. If both risks appear in the top three, shading corresponds to the higher risk.

8 World Economic Forum (2018). Regional Risks for Doing Business 2018.

EUROPE

Cyber threats have become the top concern for businesses after rising four rankings from 2017



ASIA-PACIFIC

Data fraud/theft joined cyber attacks among the top risk concerns for business in the region, amid persistent economic fragilities and ongoing governance challenges

RAPID COMPANY INNOVATION

The pace of business innovation has been driven by technology and connectivity megatrends such as mobile, the Internet of Things (IoT), big data and cloud solutions.

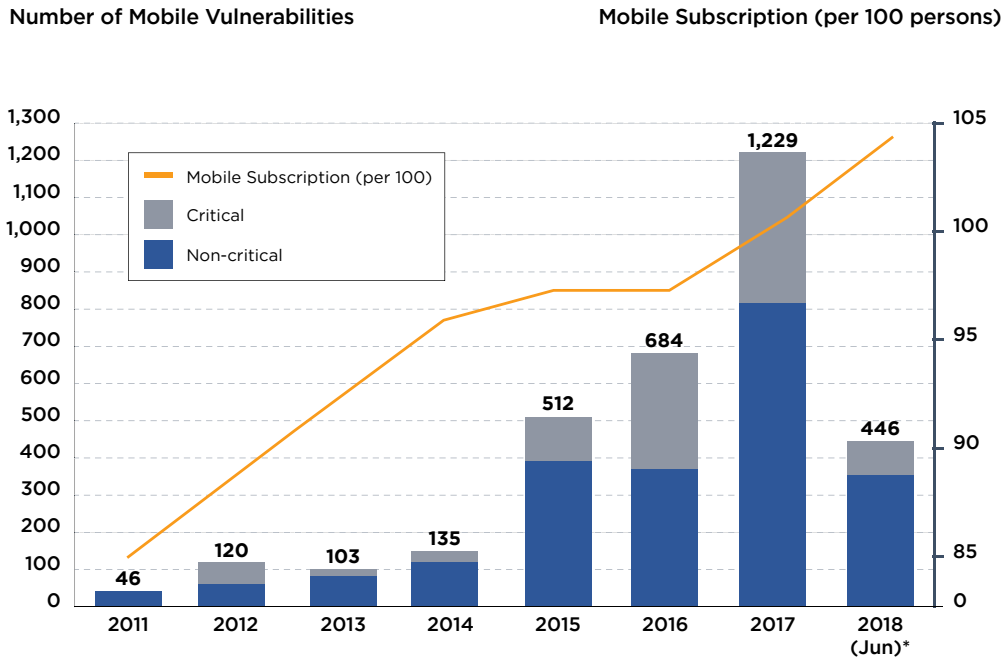
The adoption and use of mobile devices have surpassed that of desktops since the last quarter of 2016,[9] with mobile traffic accounting for 52 percent of total internet traffic in 2018.[10] While business benefits include greater convenience and productivity, the use of mobile devices for both work and personal reasons has blurred the lines between sensitive corporate and confidential personal data, which are increasingly exposed to weaker application security features, mobile malware and other vulnerabilities (Fig. 4).

In addition to the Internet-enabled mobile devices that drive innovative businesses, such as mobile payment platforms and e-commerce, many companies begin their digitalization journey with cloud migration.

By enabling unprecedented speed, agility and data storage access, the cloud can provide a quick and easy way to implement business process changes and find new ways to engage clients. However, increased use of the cloud to store and process sensitive data may result in increased exposure to cyber attacks.[11]

Continual innovation depends on transformative technologies, but their widespread adoption carries the risk of increased vulnerability and exposure to cyber threats.

Figure 4. Security vulnerabilities increase as mobile subscription accelerates globally.[12]



*Number of mobile vulnerabilities was last published in Jun 2018.

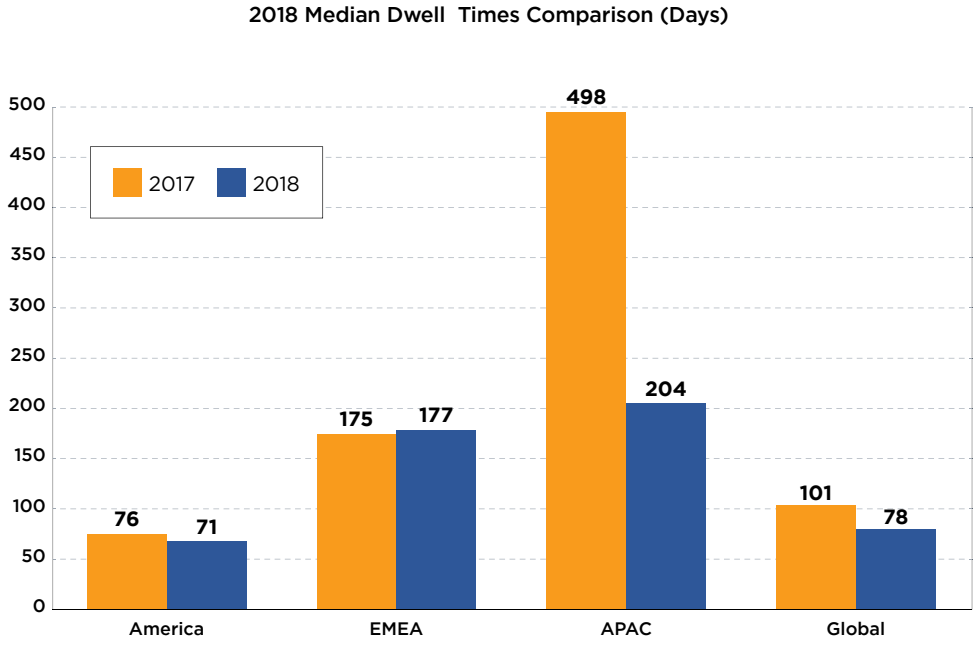
9 StatCounter (November 1, 2016). Mobile and tablet usage exceeds desktop for first time worldwide.
10 Statista (2018). Percentage of all global web pages served to mobile phones from 2009 to 2018.
11 Tech Wire Asia, 2019. How do you manage cybersecurity in a multi-cloud environment?
12 ESET (August 29, 2018). Semi-annual balance of mobile security.

PERVASIVE, SOPHISTICATED TECHNOLOGIES

A recent study by FireEye Mandiant revealed that cyber attackers have followed cloud-reliant organizations, such as software-as-a-service and cloud computing, into the cloud.[13] Mandiant researchers observed an increased volume of attacks against organizations with access to vast amounts of personal and confidential data, such as cloud providers, telecommunications, and retail and hospitality. More than 730 investigations were performed by Mandiant experts globally in 2018, a higher volume than any year before and an increase of more than 30 percent over 2017.

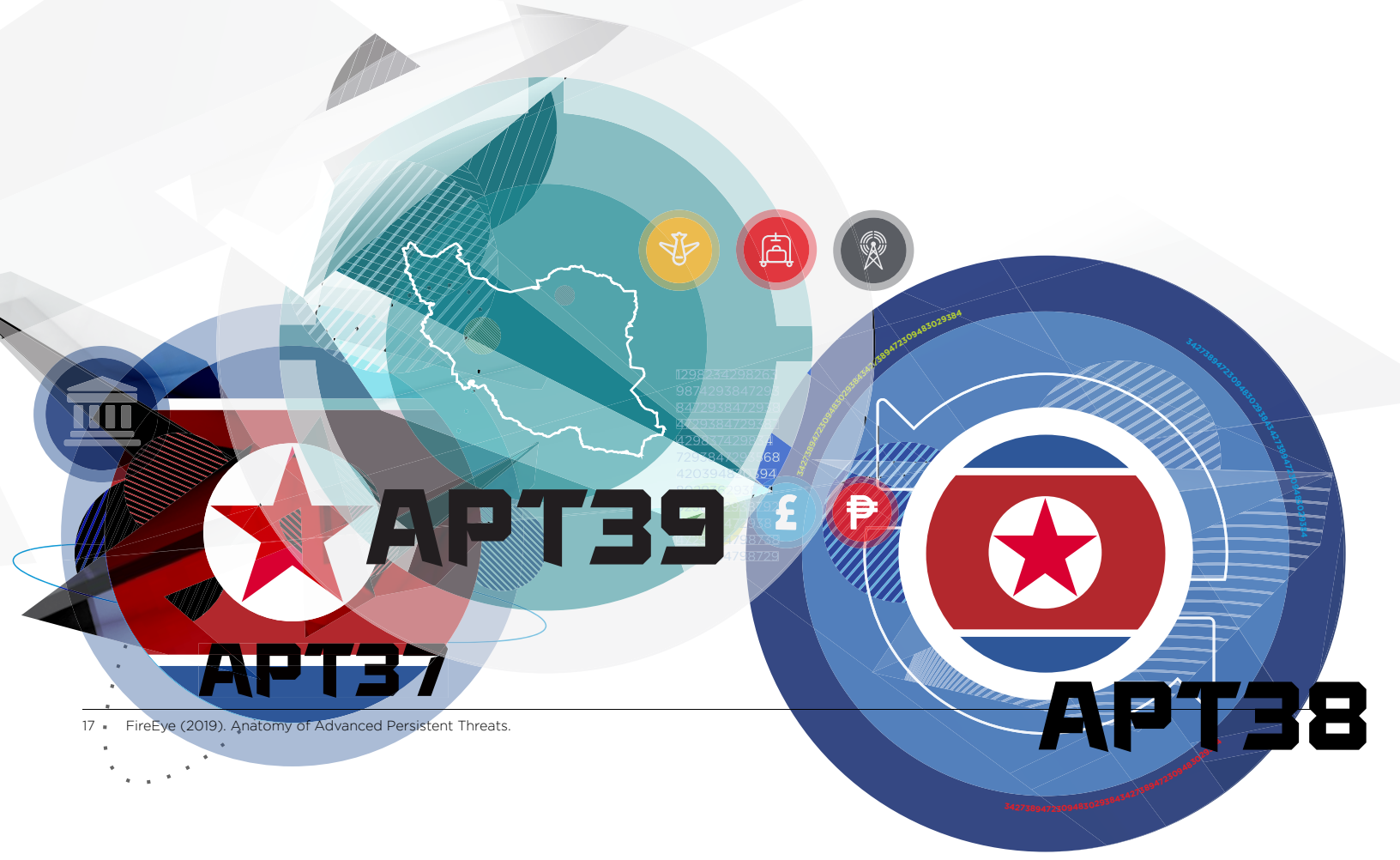
Rapid technological advances, including heightened cyber awareness, may also suggest that organizations are reducing the time spent detecting threats.[14] Mandiant reported that the global median[15] dwell time in 2018 was 78 days, suggesting that attackers are operating, on average, for fewer than three months in the compromised network before detection; considerably lower than the global median dwell time of 101 days in 2017 (Fig. 5). Unfortunately, Asia-Pacific (APAC) still registered a median dwell time of 204 days, the longest across all regions worldwide, even though it was a significant decrease compared to 2017. All in all, while this is a noteworthy improvement from previous years, it is far from sufficient.

Figure 5. Organizations are generally detecting breaches more quickly.[16]



13 FireEye (2019). M-Trends 2019.
14 FireEye (October 4, 2017). FireEye Expands Cybersecurity Threat Detection with Major New Releases.
15 The median represents a value at the midpoint of a sorted data set.
16 FireEye (2019). M-Trends 2019.

Today, advance persistent threat (APT) attacks are becoming more frequent because they have relatively higher success rates. An APT attack is a prolonged and targeted cyber attack in which the cyber criminal gains unauthorized access to a network and remains undetected for an extended period.[17] Using multiple pathways (i.e. vectors), techniques and entry points, APT attacks require huge efforts, resources, and detailed planning to gain the initial access. Operating in stealth mode, any evidence of the APT attack is usually removed to avoid detection, but the network would have already been compromised. APT attacks generally do not cause significant damage to the network or local machines, as they are the gateway established to allow cyber criminals to return any time after to continue the data exfiltration.



17 ▪ FireEye (2019). Anatomy of Advanced Persistent Threats.

SOCIAL ENGINEERING:

The non-technical strategy to a successful cyber attack

Cyber threat actors and their techniques have evolved, but most attacks still contain elements of social engineering. Without complex tools, software or extensive knowledge about the security platform, social engineering is an effective, non-technical strategy used by cyber criminals (Fig. 6). It relies primarily on human interaction to gain trust and manipulates people into breaking standard security practices.

Common social engineering techniques used to target users include phishing and pretexting.

Phishing is a predominantly email-based attack that exploits the human curiosity and entices unsuspecting users to click on a link or access an attachment that activates malicious software. Pretexting creates a false narrative or identity to obtain information or influence behavior. It usually involves a conversation by phone or email, or across social media messaging platforms, and often targets employees in Finance or HR departments. Together, phishing and pretexting are present in 93 percent of all breaches, while email was the most common vector at 96 percent.[18]

Today, social engineering is recognized as one of the greatest security threats facing organizations.[19] More than 90 percent of cyber incidents are caused by social engineering techniques (mainly phishing attacks) and are therefore considered as threats that lead to "human-enabled" network compromises.[20]

While security teams need new defense tools and strategies to expel malware and strengthen their cyber security, organizations need to dispel common misconceptions about insider threats and acknowledge that social engineering is a real risk to both individuals and large corporations. It's critical to prioritize employee education and awareness as a first line of defense and integrate them into any layered security strategy.[21]

Figure 6. Social engineering statistics.

SOCIAL ENGINEERING

Number #1 greatest security threat facing organizations

CYBER ATTACK VECTORS

96%

Email continues to be the most common vector at 96%

90%

Phishing accounts for more than 90% of successful attack

THREAT ACTOR MOTIVATED

59%

Financial Gains

38%

Espionage

HUMANS — THE WEAKEST LINK

90%

Human-enabled insider threats account for more than 90% of all cyber incidents

18 Verizon (2018). 2018 Data Breach Investigations Report, 11th Edition.
19 Keepnet Labs (October 26, 2018). Data Breach Record of 2018 in the First Half.
20 Dogana (May 14, 2018). Estimates of the number of Social Engineering based cyber-attacks into private or government organizations.
21 Oliver Wyman (2019). The Increasing Threat from Inside: A Proactive and Targeted Approach To Managing Insider Risk.

DEVIOUS, ORGANIZED THREAT ACTORS

The modern cyber risk landscape is rapidly evolving and populated by threat actors with a myriad of motivations and attack sophistication levels (Fig. 7). The methodologies can vary from highly-targeted and deliberate, to mass-scale with self-distributing malware. Different threat actors also have different motivations and ambitions that can be uniquely destructive.

Figure 7. Taxonomy of cyber-related threat actors.[22]

Insider Threats
- **Malicious intent can be motivated by emotional backlash, financial benefit, political ideology or a combination of factors**
- **Unintentional threat due to lack of understanding or misplaced technology**

Competitors
- **Motivated by financial gains**
- **Seek Information research data and intellectual property**
- **Exploit for strategic market advantage**

Script Kiddies
- **Motivated by making names for themselves**
- **Usually unskilled but rely on pre-made exploit programs (“scripts”) to attack networks or deface websites**

Hacktivists
- **Motivated by ideological activism**
- **Bring awareness to a cause (political, economic, social)**
- **Exploit to compromise confidentiality, integrity or resilience**

Organized Crime
- **Motivated by financial gain and power**
- **Exploit and extort organizations to access and monetize personal, financial, or health data**

Cyber Terrorists
- **Motivated by malicious intent to gain support for and deter opposition to a cause**
- **Attack and damage reputation, inspire fear or threaten harm to force a political change**

State-Sponsored Actors
- **Motivated by interests of nation-states**
- **Receive direction, funding, technical assistance**
- **Highly sophisticated often targeted and persistent**

22 Oliver Wyman (Proprietary materials) and Rand Corporation, 2018. Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data

Motivations and methodologies of threat actors can also overlap with one another. In many cases, similar tools and techniques are used by different groups since those may be the only tools available. In some cases, state-sponsored actors may even work with hacktivists to carry out an attack.

Some threat groups demonstrate increased determination by maintaining persistence in victims' networks. Some APT attackers plan out their modus operandi and patiently pursue their goals over a long period of time—months or years—before they launch their attack. They rapidly adapt to a victim organization's attempts to remove them from the network and frequently target the same victim again if access is lost.

After an organization has been successfully attacked, there is a higher probability of re-compromise. According to FireEye, globally two in three (64 percent) compromised organizations were successfully attacked again within a year. It is more significant in APAC where almost eight in 10 (78 percent) of compromised organizations are likely to face at least one additional significant attack over the next year.[23]

Organizations that have been attacked should strengthen their cyber security defenses and close any identified gaps to mitigate risks; unfortunately, this doesn't always happen.

23 FireEye (2019). M-Trends 2019.

The anonymity of the Internet further ensures little or no risk of repercussion for cyber criminals.

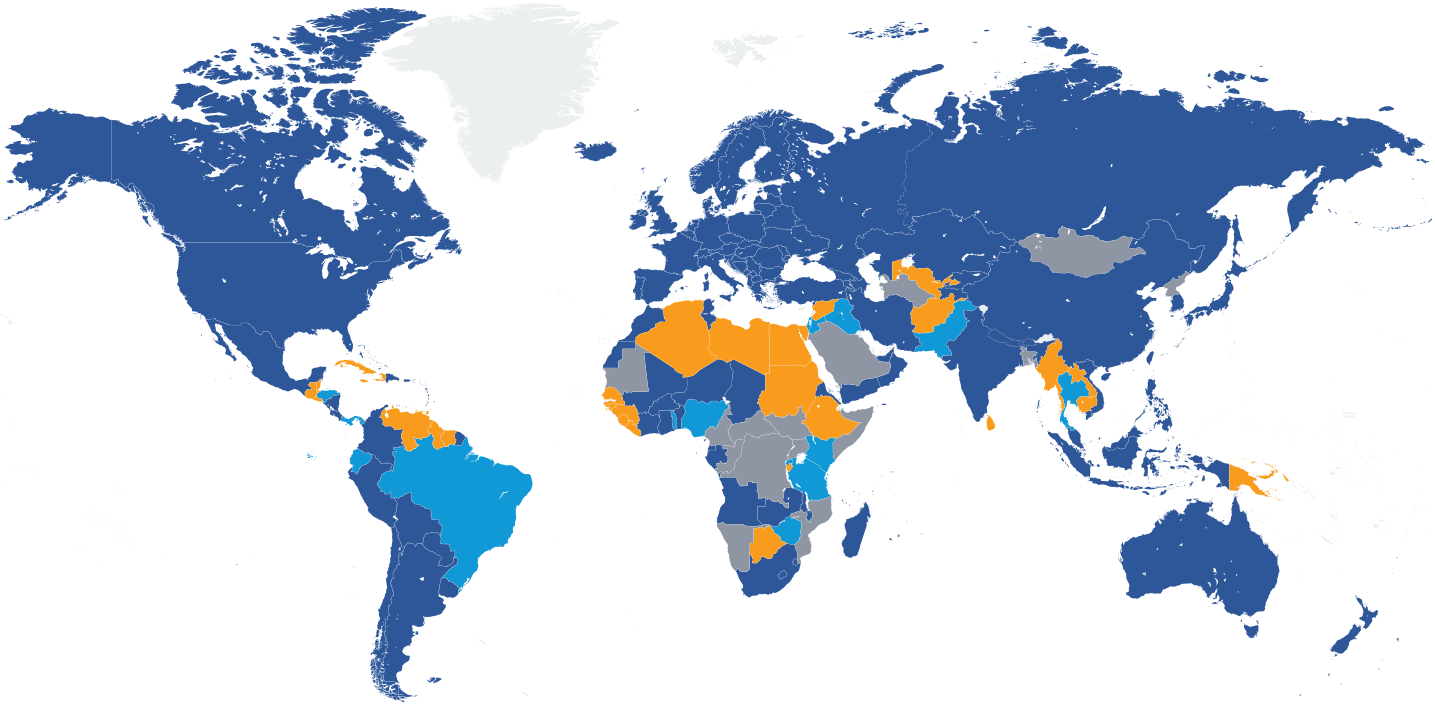
DATA SHARING ECONOMIES

Data sharing is inevitable as we accelerate into the digital economy. Our growing interconnectedness is combined with a massive increase in velocity, volume, and variety of data shared across boundaries and jurisdictions. The accelerated digitalization of countries and industries amplifies the systemic effects from cyber attacks and increases the severity of successful cyber attacks.

With the advent of digital and transformative technologies that change the nature of business, policymakers are challenged to maintain the robustness of cyber laws and legislations. The anonymity of the Internet further ensures little or no risk of repercussion for cyber criminals.

According to FireEye CEO Kevin Mandia, "We are on a slippery slope in terms of frequency and seriousness of cyber attacks" and it is likely to get worse unless serious consequences can be put in place for criminal behavior.

Although cyber regulations have lagged behind evolving cyber threats, the past years have seen a substantial increase in new cyber laws and other regulatory schemes, and this is expected to continue (Fig. 8). Most regulatory schemes aim to protect data and privacy and fulfil notification obligations by breached organizations, but disclosures and notifications are critical first steps to reveal the volume, frequency and complexity of breaches before data protection and privacy can be further improved.



58% COUNTRIES WITH **LEGISLATION**

10% COUNTRIES WITH **DRAFT LEGISLATION**

21% COUNTRIES WITH **NO LEGISLATION**

12% COUNTRIES WITH **NO DATA**

Figure 8.
Strength and distribution of data protection and privacy laws around the world.[24]

24 United Nations Conference on Trade and Development (2019). Data Protection and Privacy Legislation Worldwide.

Complications That Impact Cyber Resilience

In an increasingly complex business and cyber landscape, organizations encounter greater challenges when trying to balance their business resilience and cyber security priorities.

Between 2016 and 2018, the rate of growth for internet users was 10 times faster than the global population. Correspondingly, the surface area for attack has expanded exponentially.[25] The exposure is estimated to impact up to six billion internet users by 2022, approximately three-quarters of the projected world population.[26] Increased connectivity coupled with the expanded adoption of mobile devices makes building cyber security defenses much more challenging since every employee or web-connected device now represents a potential vulnerability.

25 Miniwatts Marketing Group (May 20, 2019). Internet World Stats, Usage and Population Statistics.
26 Cybersecurity Ventures (July 19, 2018). How Many Internet Users Will The World Have In 2022, And In 2030?

Most traditional measures...fail to detect and block "inbound attacks"—rendering the "perimeter defense" approach irrelevant.

THREAT ACTORS HAVE LEARNED TO BYPASS TRADITIONAL NETWORK SECURITY

Cyber attacks are no longer broad, scattershot attempts at mischief. They have been replaced with APT attacks focused on acquiring and exploiting valuable data records.[27] Modern cyber attacks are often conducted across multiple vectors and using different mechanisms, such as viruses, spyware, spear phishing, malicious email attachments and drive-by downloads; attacks often comprise several phases that require meticulous and patient planning.[28]

Some mechanisms do not rely on the user to enable the attack, while others wait quietly in a system an unsuspecting user to activate them. For example, once malicious software finds its way into a system through self-installation via phishing emails, it may discreetly seek out network vulnerabilities before initiating data extraction and exploitation activities.

Most traditional measures, such as antivirus software, firewalls and password protection fail to detect and block "inbound attacks"—those that manifest internally—rendering the "perimeter defense" approach irrelevant. As a result, these evolving threats and infiltration techniques have eclipsed traditional cyber security measures that struggle to keep up with the complexity, volume and speed of attacks.[29]

27 FireEye (2019). How Cyber Attacks Compromise Your Network.
28 An unintentional download of malicious code to the computer or mobile device that takes advantage of an application, operating system, or web browser that contains security flaws due to unsuccessful updates or lack of updates, hence leaving the user exposed to cyber attacks
29 Nick Ismail (September 12, 2018). Cyber security in the energy sector: Defending the industry - Part 2.

UNDERLYING TRENDS IMPOSE ADDITIONAL LAYERS OF FIDUCIARY RESPONSIBILITIES

Rapid digitalization amplifies the systemic effect of cyber threats, which leads to more cyber regulations and policies.

In addition to safeguarding the interests of individuals and businesses, governments and policymakers also aim provide a conducive and well-regulated environment to develop transformative technologies to spearhead their respective digital economies. Unsurprisingly, their business models are impacted by new cyber laws and regulations.

As these laws are introduced, revised and enacted, companies can find themselves in a continually reactive state when attempting to comply with changing policies. Organizations with operations across national boundaries face additional compliance costs as they attempt to navigate diverse regulations in different jurisdictions. While GDPR has led to the convergence of cyber security and data protection laws in the EU, cyber regulations in other parts of the world remain largely localized and diverse (See GDPR sidebar).

GDPR:

Impact on worldwide cyber transparency.

In 2018, the European Union (EU) began enforcing the General Data Protection Regulation (GDPR), and its extraterritorial effects have far reaching implications across different jurisdictions.

For example, when the GDPR was approved in the European Parliament in 2016, there was a corresponding spike in the number of standards, guidelines and amendments to cyber laws related to e-transactions, consumer protection, data protection and privacy and cybercrime observed in 11 of the APAC[30] member states of the United Nations Conference on Trade and Development (UNCTAD) (Fig. 9).[31]

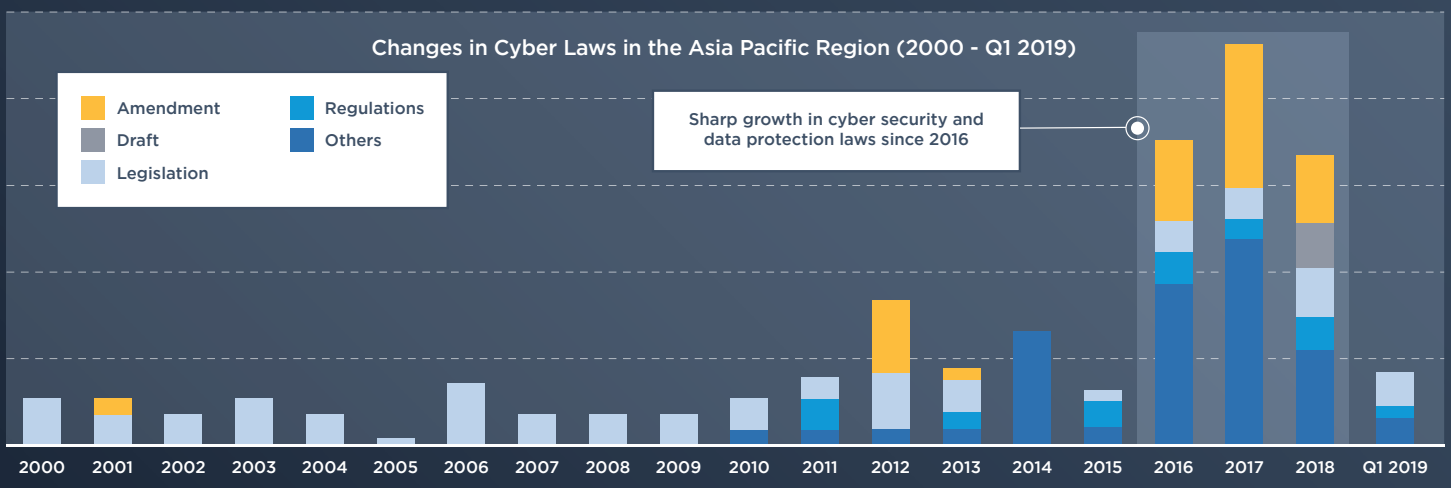
Regulators in Asia became more transparent about their growing cyber threats and malicious data breaches in response to the GDPR, to more accurately reflect the cyber threat level in the region. For example, Hong Kong issued a circular to inform the public of the possible impacts of a large-scale cyber attack, while Singapore released a factsheet for organizations to highlight the implications of the GDPR on their businesses.[33,34]

Other Asian regulators also embraced the GDPR to learn and reflect for reforms. Parts of the data protection regulations in Thailand, India and China are suspected to be modeled after the GDPR, while several legal terms directly draw from the GDPR, such as "right to be forgotten" in Indonesia and "data portability" in the Philippines.[35,36]

Globally, the GDPR has also enabled consumer advocacy groups to file lawsuits against large technology companies, giving companies around the world pause about potential associated fines and penalties.[37,38]

Regardless of whether the GDPR can take sole credit for these trends, the significant increase in public attribution conducted by governments, policymakers and consumers should not be ignored.

Figure 9. Governments in APAC accelerate changes in laws and policies to mitigate cyber risk.[32]



Others include circulars, codes of practice, standards and guidelines that are not legally binding but provide the respective industry best practices.

30 The 11 member states selected for the study include: Australia, China, Hong Kong, India, Indonesia, Japan, Malaysia, New Zealand, Republic of Korea, Singapore, and Thailand
31 United Nations Conference on Trade and Development (2019). Data Protection and Privacy Legislation Worldwide.
32 Ibid.
33 Office of the Privacy Commissioner for Personal Data (May 25, 2018). EU General Data Protection Regulation (GDPR).
34 Personal Data Protection Commission Singapore (2017). European Union General Data Protection Regulation Factsheet for Organisations.
35 Mark Innis (January 25, 2017). Indonesia: New Regulation on Personal Data Protection.
36 Damian Domingo O. Mapa (2018). Mapping the Philippine Data Privacy Act and GDPR: A White Paper from the EITSC.
37 Alex Hern (May 25, 2018). Facebook and Google targeted as first GDPR complaints filed.
38 Alex Hern (January 21, 2019). Google fined record 44m by £French data protection watchdog.

RE-THINKING A CYBER RESILIENT CULTURE

To reduce our growing vulnerability to human-enabled cyber threats, workplace culture needs to change. The outlook, attitudes, values, moral goals and legacy systems shared within an organization have a direct impact on how cyber threats are perceived and managed. While cyber security involves many different technical and information solutions, necessary defenses and resilience cannot be fully achieved without the right mindset.

To establish a cyber resilient culture, everyone in the organization—from executive leadership and management to data analysts and salespeople—have an equal and important role to play in defense.

Through social engineering, threat actors increasingly exploit individuals as the weakest link of the cyber security chain. Therefore, cyber security and resilience must begin with the individual. Although Finance or HR departments may be primary targets for potential access to sensitive information, other executives and employees may also be targeted to gain network access.

To establish a cyber resilient culture, everyone in the organization has an equal and important role to play in defense.

Organizations need to ensure that they can be cyber resilient, comply with cyber laws and still thrive economically. To accomplish this, stakeholders within the organization must collectively create a resilient culture. Organizations can then work to quantify the nature and extent of potential cyber-related losses, implement cyber security programs to reduce those losses and consider other business priorities.

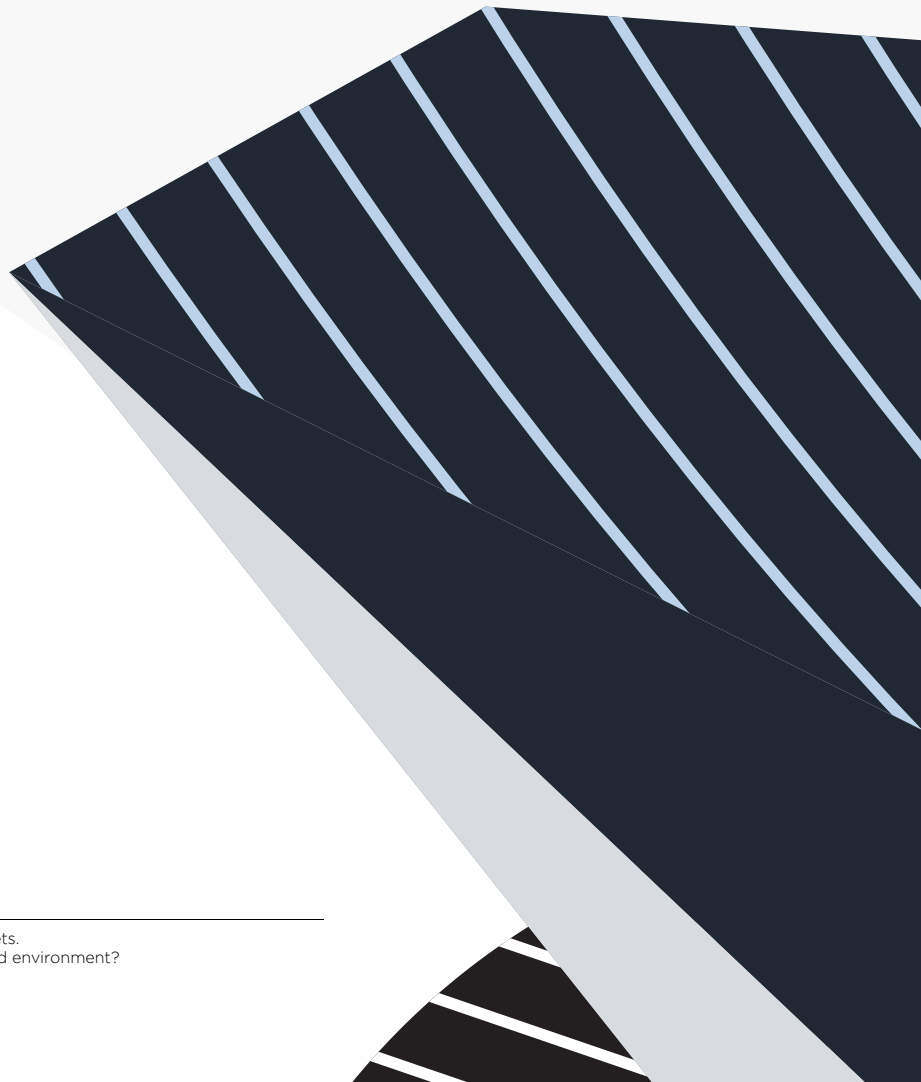
How To Line Up Your Defense

Given the reality of the cyber threat landscape, you need to determine the tools you need to mitigate and respond to inevitable cyber attacks.

Unfortunately, while both the aggressiveness and sophistication of cyber attacks have accelerated, defensive capabilities have been relatively slow to evolve and respond.[39]

Darren Thayre, Partner in the Digital, Technology and Analytics Practice for Asia Pacific at Oliver Wyman, mentioned that typical cyber security discussions are often absent when organizations initially strategize on cloud implementation, a process normally driven by developers or infrastructure demands.[40]

Many victim organizations and those working diligently on defensive improvements still lack the fundamental security controls and capabilities to either prevent breaches or to minimize the damages and consequences of an inevitable compromise.

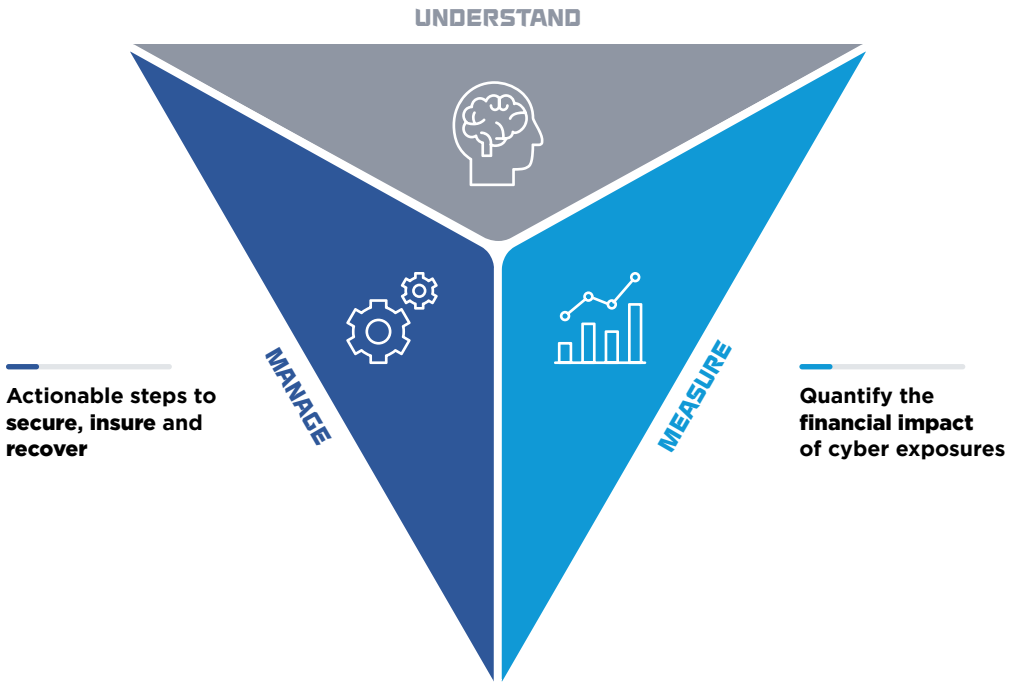


39 BlackRock Blog, 2019. What a major cyber-attack could mean for markets.
40 Tech Wire Asia, 2019. How do you manage cybersecurity in a multi-cloud environment?

Based on trend observations, Kelly Butler, Head of Cyber Practice, Pacific, Marsh, stated that while security remains important in the 2019 cyber landscape, it is becoming more about resilience. Organizations must maintain a posture of continuous cyber resilience to prepare for and adapt to the changing threat landscape and recover from the disruptive attacks (Fig. 10). Otherwise, they risk facing significant gaps in both basic security controls and—more critically—visibility and detection of targeted attacks.

The saying goes, "what gets measured, gets managed," but you can only measure what you understand.

Figure 10. Building cyber resilience is the result of an end-to-end cyber risk management process[41]



41 Marsh, 2019. Understanding, Measuring, and Managing Fast-Evolving Cyber Risks (Webcast).

Understand Cyber Risks From a Business Perspective

Cyber risk is now at the forefront of most corporate risk agendas. Organizations are increasingly looking to understand and assess the nature and extent of their potential cyber-related losses—a necessary first step to mitigate those losses.

A **cyber defense strategy** delivers substantial benefits for both the senior management and the organization, especially when the strategy and associated action plans are mandated from the top and prioritized with the necessary investments and budgets. A proactive cyber defense strategy demonstrates to regulators that the organization takes cyber risk management seriously and has clear priorities in place.

A cyber security strategy is how you direct and focus the creation of an actionable roadmap and **build a comprehensive cyber security program** (Fig. 11). This process allows you to clearly link gaps identified in the program assessment to your organization's cyber security investments.

However, developing a fit-for-purpose strategy and obtaining buy-in for the cyber security program from senior management can be difficult.

Figure 11.
A strategic cyber defense program.[42]

Leadership Alignment
Ensures that CEO and Board of Directors are supportive of and invested in the direction of the cyber program, helping the CISO navigate and avoid roadblocks

Investment Prioritization
Allows the organization to focus investment in the areas that are aligned to the strategic objectives

Consistent Approach
Drives consistency across disparate business units, resulting in cost and defense efficiencies and enabling centralized control with decentralized execution

Preparedness
Enables the organization to be proactive, rather than reactive by forcing management to consider the trajectory of the organization's cyber risk management capabilities in light of the evolving ecosystem

Regulatory Communication
Demonstrates to the regulators that the organization takes cyber risk management seriously, is investing appropriately, and has a clear set of cybersecurity priorities

Challenges commonly cited from businesses include:

Overcome and adapt to organizational inertia, which may involve the distraction of short-term earnings rather than a focus on strategic goals

Keep pace in a rapidly developing environment, that includes threats, regulations, and other factors

Change the mindset that cyber security is only a technology problem

42 Oliver Wyman (unpublished).

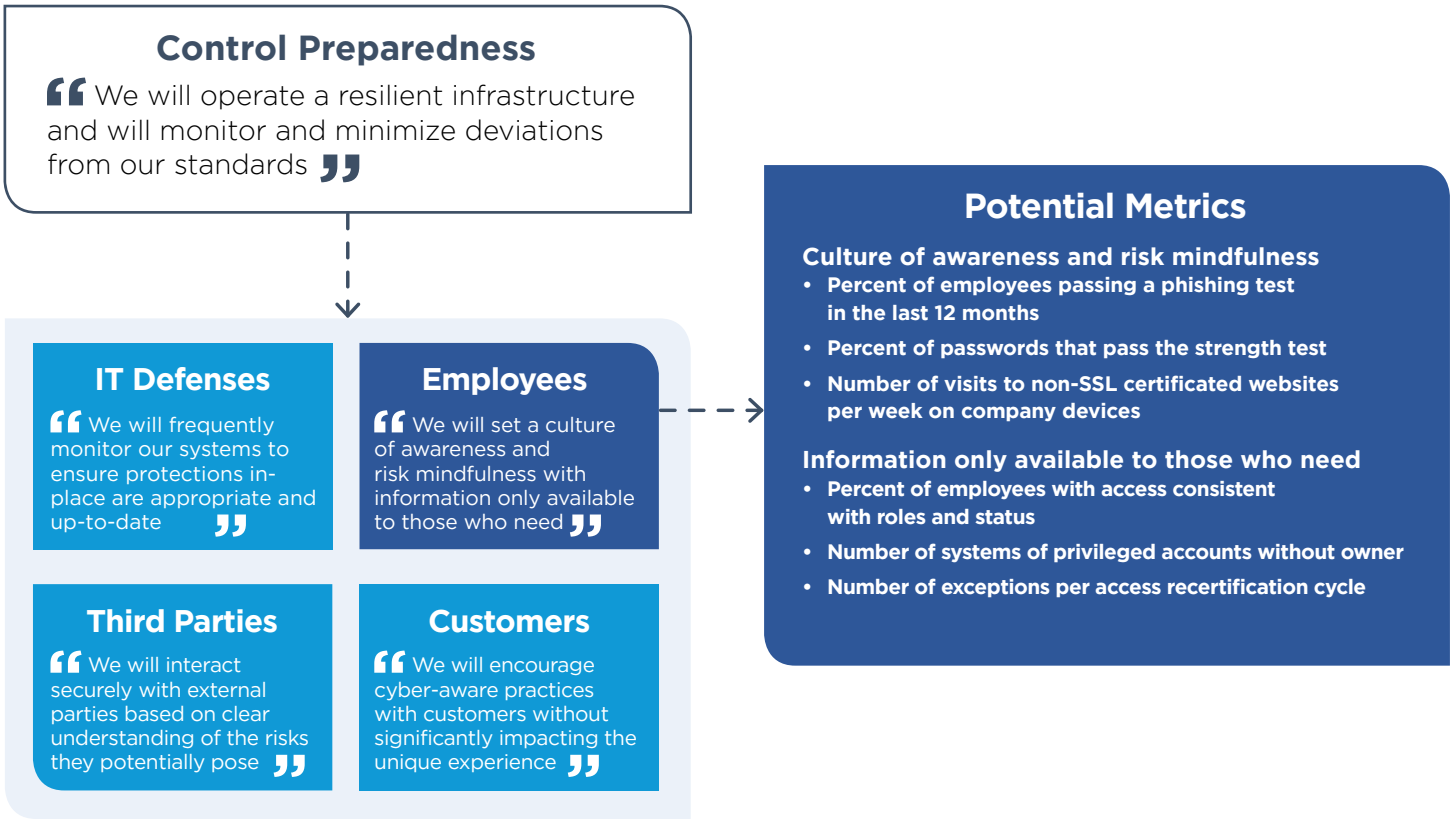
Measure the Financial Impact of Cyber Exposure

After you understand cyber risks from a business perspective, you need to **identify how much cyber risk is acceptable** (to be absorbed) across your entire organization. This baseline helps make decisions related to cyber risk and implement controls.

For example, you can use a structured methodology (Fig. 12) to determine your organization's cyber risk appetite. Ideally, you should break down and prioritize your cyber risk appetite, and the metrics you need to inform and measure the risk appetite. Later, you can develop recommendations regarding governance and operating model requirements, which in turn will determine and influence corporate decisions with respect to cyber security investments.

After you assess the amount of acceptable cyber risk, **work to quantify your potential cyber risk exposure.** Measure its financial impact to inform the business case for cyber security investments as well as cyber insurance that can mitigate or transfer risk.

Figure 12.
How to identify preparedness metrics that support organizational goals (example).[43]



43 Oliver Wyman (unpublished).

Quantification determines nature and extent of risk impacts for different threats and scenarios. Figure 13 illustrates an example incident involving theft and disclosure of personal customer data. It highlights key elements that apply to the narrative and notes reasonable estimates of loss, including potential insurance coverage.

However, boards and senior executives often struggle to clearly and comprehensively gain a current understanding of their organization's cyber risk profile.

Typical challenges include:

Trade-offs between security and convenience that impact business agility

Technical jargon and data overload that often results in dense and overwhelming reports, with only weak associations to the overall risk appetite

Lack of clearly quantified risk acceptance, exposure and target state, which leads to deficient decision-making plans

Figure 13. Make better decisions by estimating the impact and distribution of loss due to cyber risk exposure (example).[44]

Key Drivers	Sub-Drivers	Insurance Coverage
Revenue loss	• **Loss in revenue due to down time** • **Loss of repayment to customer**	**Business interruption,** covering: • **Loss of income** • **Other extra expenditure or additional costs**
Operational Cost/Expense	• **Data restoration** • **Data forensic investigation**	**Digital asset rectification,** covering: • **IT forensic investigations** • **Data asset restoration**
	• **Mail/email notification**	**Notification costs,** covering: • **Call center** • **Credit monitoring**
	• **Staff training** • **System enhancement**	Exclusion of indirect or consequential loss of any nature Exclusion of indirect or consequential loss of any nature
Litigation Cost	• **Legal counsel and cost on penalties and settlement**	**Defense cost,** covering legal and regulatory advise
Regulatory Fines	• **Fines for data breach**	**Privacy and data breach,** covering legal costs associated with losing personally identifiable or corporate information
	• **Other regulatory fines for lack of controls**	**Regulatory fines and penalties** (where legal and insurable)
Reputational Recovery Costs	• **Brand building initiatives**	**Public relations** (PR firm costs associated with breach)
	• **PR consultant handling communications**	**Notification costs**
Other(s)	• **Ransom payments**	**Extortion** (where legal and insurable)
	• **Damages**	**Damages and settlement** to third-party vendors/partners
	• **Network liability**	**Legal actions** from spreading a virus transferred from infected network to third-parties

Insurance type: 1st party 3rd party

44 Marsh & Oliver Wyman (unpublished). MMC analysis.

Manage the Insurance and Recovery Process

The increased risk of cyber threats tends to push organizations to **proactively manage residual risks through insurance**. While insurers and brokers take a more reactive approach, there is a subtle shift in the market as the lines of coverage mature. More often, local insurers are willing to work with organizations to offer broader areas of coverage, such as social engineering fraud (either written-in or as an optional extension), in response to the varied cyber risk appetites.

Insurers in more advanced APAC economies continue to follow more mature international cyber markets, such as the U.S. and Europe. Global predictions indicate that cyber insurance premiums will increase at a compounded annual growth rate of 20.1 percent, between 2014 and 2020 (Fig. 14), three times faster than the general property-casualty insurance market, which grew at par with the global economy nominally at an average of 4.9 percent in 2018.[45] Moving forward, there will be greater access to more accurate claims data and loss trends, as well as policy tests for affirmative language and clarity of cover.

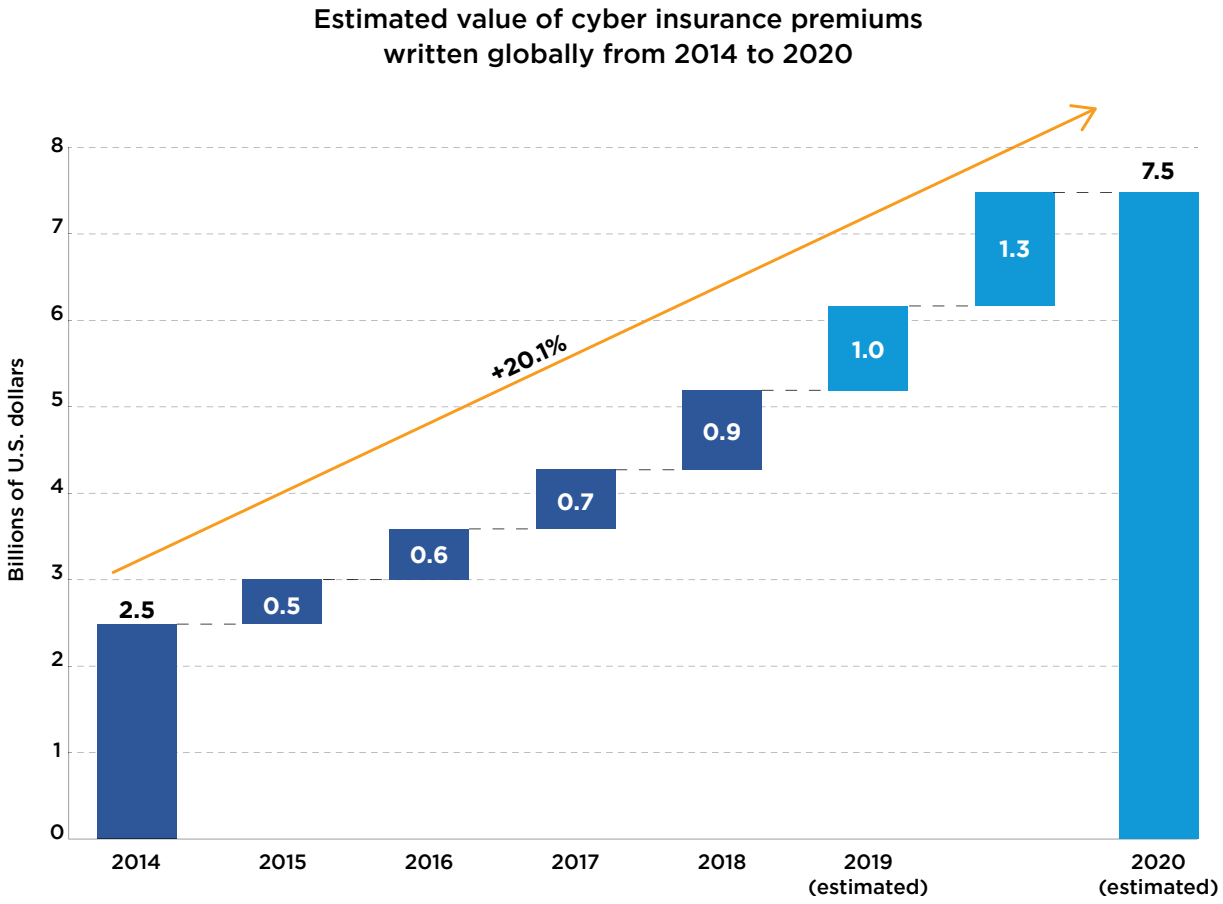
For many businesses in mature markets, core exposures and claims are predominantly first-party business interruption losses,[46] with the primary consideration being incident response expenses. On the other hand, in developing markets, most policies remain focused on protections against the loss of data due to cyber attacks with significant growth in first- and third-party coverage. Cyber risk planning needs to fully address both first-party and third-party scenarios.

Regional increases in collective cyber awareness are encouraging organizations to consider the loss of physical assets in the event of a cyber attack. As a result, organizations are more frequently demanding solutions that provide more comprehensive coverage to address more sophisticated attacks and the widening attack surface. **Recent conversations with organizations are increasingly focused on addressing cyber insurance solutions for physical losses stemming from cyber attacks, according to Naureen Rasul, Head of Cyber Practice, Asia, Marsh.**

Corporate directors and boards are beginning to understand cyber security is no longer the responsibility of the IT departments. Several recent high-profile cyber events have illustrated the devastating impact that lack of cyber readiness can have on a company's operations and public reputation.

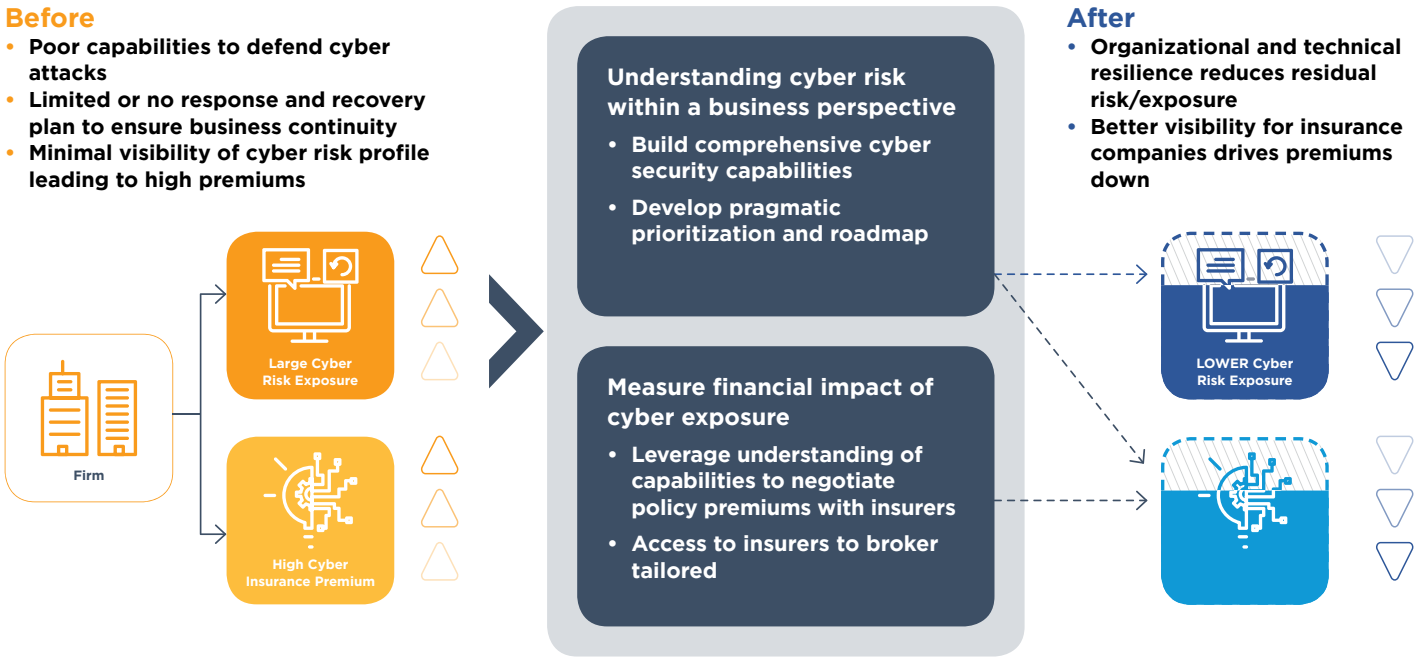
45 Munich RE (2019). Insurance Market Outlook for 2018/2019.

Figure 14.
The cyber insurance market grows three times faster than the general insurance market.[46]



46 Statista (2019). Estimated value of cyber insurance premiums written worldwide from 2014-2020 (in billion U.S. dollars).

Figure 15. Cyber insurance premiums can be reduced by managing risk exposure.[47]



47 Marsh & Oliver Wyman (unpublished). MMC analysis.

The increase in awareness, cyber data breaches and adoption of cloud-based services are a few of the factors that drive the growth of the cyber insurance market, while high costs inhibit growth. High premiums can be effectively overcome by systematically and clearly understanding organization-specific cyber risks to lower risk exposure and enhance risk profile (Fig. 15). For example, the use of data analytics to quantify risk exposure and underwrite cyber risks has proved to drive more efficient and effective risk profiling and provide more accurate policy coverage.[48]

With an internally aligned cyber risk strategy and adequately measured risk exposure around expected losses due to cyber attacks, organizations can better insure and **secure stronger financials to respond and recover** from an incident.

An incident response plan requires the support of proper security technologies and expertise. At a minimum, a response plan requires full view of IT assets, strong detection capabilities, clear roles and responsibilities and fast reaction times. The plan must also be regularly practiced through drills to ensure that personnel know their roles and to track and record various metrics that measure their performance. Frequent testing can help identify areas for improvement and provide opportunities to continually refine processes and protocols.

However, organizations often face several challenges to the implementation of response and recovery plans:

Misconception that frontline security defense and insurance coverage are mutually replaceable rather than complementary

Lack of knowledge on what a proper cyber incident response plan ought to look like, and uncertainty about which third party vendors can help create a viable plan

No standard protocols on stress-testing a cyber scenario, which often impacts business operations by requiring multiple sites to be offline

48 Marsh, 2019. Marsh Risk Consulting on strategic risk consulting services.

From Aspiration To A Call For Action

> "In our current state of cyber security, security breaches are inevitable. **This is an important fact, so I am intentionally repeating it. In our current state of cyber security, breaches are inevitable.**"

Kevin Mandia
CEO, FireEye[49]

The statement was made in 2011 after several high-profile data breaches had piqued concern among lawmakers, and it remains relevant today.

The question is not whether you will be breached but how you will respond when there is a breach. **Adopting an end-to-end cyber risk management approach provides a business-centric lens for organizations to address the growing challenge of cyber risk, emphasized Kevin Richards, Global Head of Cyber, Marsh Risk Consulting.** Through a discussion of technical controls, compliance, and the financial impacts of cyber risks, more effective decisions on future cyber security investments can help mitigate cyber threats.

Although cyber attacks may be inevitable, system compromises and impactful data breaches do not have to be. It may be impractical for organizations to attempt to keep pace with malicious threat actors, but it is the new normal—and no one can truly achieve zero risk.

Organizations have come a long way on their journey to cyber resilience. They began by understanding the evolving threat landscape and learning and reacting to the changing regulations. Future progress depends on internal investments toward shaping mindsets and culture, strengthening technical expertise and managing human capital.

49 U.S. House of Representatives, Oct 2011. Written Testimony of Kevin Mandia, Chief Executive Officer, Mandiant Corporation, before the Permanent Select Committee on Intelligence U.S. House of Representatives Cyber Threats and Ongoing Efforts to Protect the Nation

A More Secure Future
An Anticipated Cyber Attack

June 27, 2017 – It was a typical afternoon in the office when several of the work computers spontaneously shut down. Within minutes, all the other working devices, desktops, tablets, mobile phones, on the floor were disconnected from the network. Relying on traditional communication, one senior executive from the Business Resilience department shouted across the hallway, "Looks like an automated malware response! Let's take care of it."

The appropriate defense protocol was called up and the incident response (IR) plan initiated. It didn't come as a surprise, especially for the established personnel who had experienced a similar attack within the last 30 days. They knew their Finance department was one of the most heavily targeted areas of the firm, and across the industry .

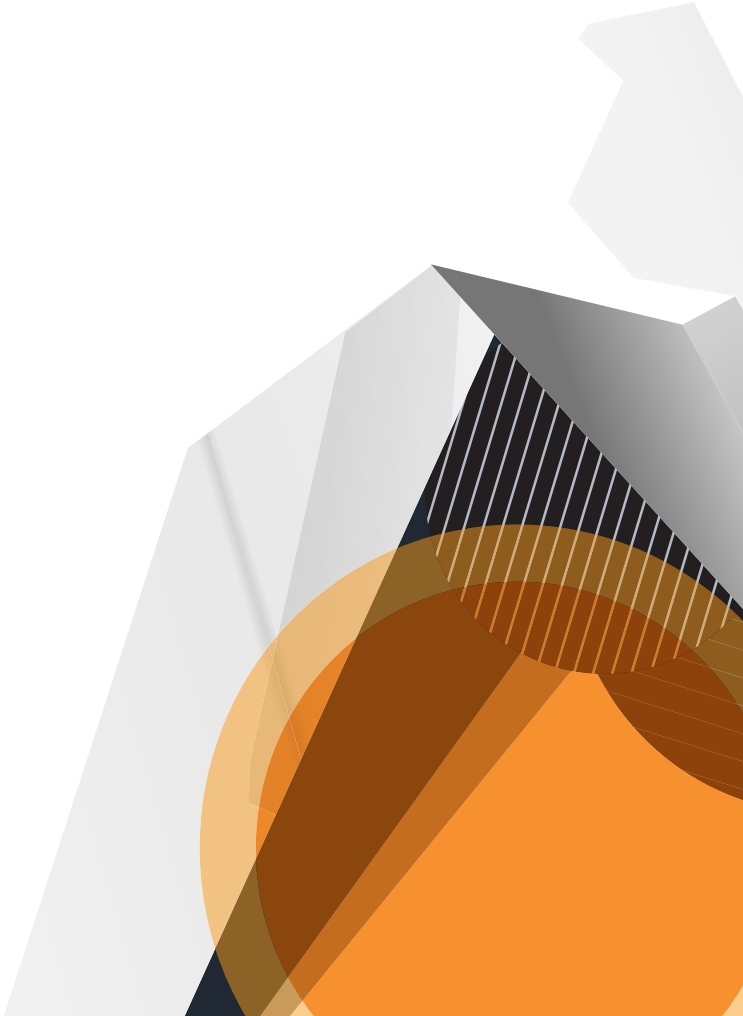
Soon, the four staff who were identified as having infected laptops deposited them at the tech help desk for quarantine and were given temporary replacements. Unaffected users who could not access to the network took a quick break or pursued offline work with colleagues.

Several phone calls were made to contracted breach consultants and insurance brokers to assess the potential damage and coverage. During the incident, although the staff remained calm, there was an undercurrent of tension and stress. However, all essential tasks were carried out smoothly within the first hour of detection, just as stipulated in the IR plan.

The later post-incident investigation revealed no evidence of data breach; all financial and personal identifiable data of both employees and clients were confirmed safe and intact. Relevant incident data was disseminated internally to legal, human resource, risk and finance functions, as well as the board, emphasizing that all critical functions remained unaffected and their business continuity management plans were successful.

Network connections were quickly re-established in the office. As the day wound down, everything that occurred earlier in the afternoon seemed distant as people started to pack their bags for the day. The following day would bring a review and improvements to their response processes. But that was tomorrow; today, they remained safe.

Definitely not just another day at work but a good day, nonetheless.



About FireEye

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

To learn more about FireEye, visit: **www.FireEye.com**

About Marsh & McLennan Insights

Marsh & McLennan Insights uses the unique expertise of our firm and its networks to identify breakthrough perspectives and solutions to society's most complex challenges. Marsh & McLennan (NYSE: MMC) is the world's leading professional services firm in the areas of risk, strategy and people. The company's 75,000 colleagues advise clients in over 130 countries. With annualized revenue approaching $17 billion, Marsh & McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading firms – Marsh, Guy Carpenter, Mercer, and Oliver Wyman. Marsh & McLennan Insights' digital news services, BRINK aggregate timely perspectives on risk and resilience by and for thought leaders worldwide.

For more information, visit **http://www.mmc.com/insights/themes/cyber-resilience.html**

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