MMC **CYBER**
HANDBOOK 2016
Increasing resilience in the digital economy

MARSH   GUY CARPENTER   MERCER   OLIVER WYMAN
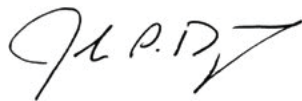
FOREWORD

Cyber risk exposures are embedded in the operations of organizations across all sectors and countries. No company is fully secure, no matter how sophisticated its cyber defense mechanisms. With cyber risk, you face active adversaries who are constantly changing their attack strategy. Technology advances also create new forms of cyber risk. For example, as more innovative Internet of Things (IoT) devices are deployed to monitor the safety of buildings or the performance of equipment, new cyber exposures are created and need to be managed. Other changes in the technology landscape – from the migration of data and software to the Cloud to the use of artificial intelligence in commercial applications – are also shifting the nature of cyber risk.

An effective cyber risk management strategy includes a deep understanding of the range of persistent cyber threats, a robust assessment of their potential impact, plans for both cyber risk prevention and response, and a management approach that reflects the role of all employees – from the boardroom to the backroom – in implementing cyber defenses.

Cyber is a "risk" issue, not an "IT" issue and managing it effectively requires broad cross-functional engagement. Yet research shows that few companies have made this mindset shift; fewer still have made the concerted organizational effort to identify the range of cyber scenarios that could affect them, assess the cyber risk of their suppliers and customers, and build fully operational cyber risk prevention and response plans.

Marsh & McLennan Companies' Cyber Risk Handbook 2016 includes articles, report extracts, and perspectives from our cyber leaders and leading third-party experts with whom we collaborate. The articles cover a wide range of topics, from changes in the external landscape, to developments in cyber risk quantification techniques, to cybersecurity-related HR strategies.

We hope this publication provides you with some new insight that can help strengthen your cyber risk management approach and enable your organization to succeed in the emerging digital environment.

John Drzik
President, Global Risk & Specialties, Marsh
Chairman, Cyber Risk Working Group,
Marsh & McLennan Companies

CONTENTS

STRATEGY

RISKS

PEOPLE

STRATEGY

THE **EVOLVING** CYBER RISK LANDSCAPE

Alex Wittenberg

Six years ago, the 2010 edition of the annual *Global Risks* report prepared by the World Economic Forum with Marsh & McLennan Companies found in the annual survey of global experts that: "Most experts perceive the risk of a potential breakdown of "Critical Information Infrastructure" (CII), as well as of data fraud/loss, as comparatively low – both in terms of likelihood and severity. Moreover, these two risks were assessed as being among the least interconnected risks." [1]

TIMES CHANGE FAST

The *2016 Global Risk Report* tags the "Rise of cyber dependency" as one of the long-term patterns that could contribute to amplifying global risks. Cyber attacks were ranked in the top 10 global risks – placing seventh over the next 18 months and eighth over the next 10 years. (See Exhibit 1.) The scope, scale, and impact of cyber attacks are growing rapidly along with increasing digitization of the public and private sectors. It is estimated that the cost of data breaches will reach $2.1 trillion globally by 2019, which is almost four times the estimated cost of breaches in 2015.[2] The impacts of cyber attacks are moving from the virtual to the physical world. In 2015, a hack on three Ukrainian power distribution companies caused outages to 80,000 energy customers.

Cyber risks are permanent and persistent. However, the awareness of the extent of the risk and the focus on the risk varies around the world. North American and European risks leaders are particularly concerned about the preparedness for cyber risks and critical systems failure. Several Asian economies, including Japan, Singapore, and Malaysia also identify cyber attacks as a primary risk.

EXHIBIT 1: RISKS OF HIGHEST CONCERN BY TIME HORIZON

Rank Next 18 months		Rank 10-year horizon	
1	Involuntary migration	1	Water crises
2	State collapse	2	Weak climate change response
3	Interstate conflict	3	Extreme weather
4	High unemployment	4	Food crises
5	National governance failures	5	Social instability
6	Fiscal crises	6	Biodiversity loss
7	Cyber attacks	7	High unemployment
8	Social instability	8	Cyber attacks
9	Extreme weather	9	Natural catastrophes
10	Asset bubbles	10	National governance failures

Legend:
- Economic
- Environmental
- Geopolitical
- Societal
- Technological

Source: World Economic Forum, Global Risks Report 2016
Note: Global Risk Perceptions Survey 2016

GROWING AWARENESS

The awareness on cyber risk has a relationship to high-profile attacks on the public or private sectors. Data breach notification has driven a high awareness of cyber risk in the USA. In Europe, the General Data Protection Regulation (GDPR), which comes into effect in 2018 and will require data breach reporting, is stimulating a greater focus on public private cooperation on cyber risk management, cross-industry data sharing, and focus on robust cyber risk management and response. In this changing context, organizations must adopt a robust cyber risk management approach based on an enterprisewide focus on early detection, response, and recovery to mitigate and better manage the consequences, and ensure business continuity.

Along with proactive cyber risk management are increases in the purchase of cyber insurance. Total annual cyber premiums have reached an estimated $2 billion and may reach $20 billion by 2025. The US remains the largest cyber insurance market, where nearly 20 percent of all organizations have cyber insurance and there are yearly increases in the number of companies purchasing cyber insurance and increases in the limits.[3] (See Exhibit 2.)

However, interest in cyber insurance is growing in other markets. For example, a recent Marsh survey of European Risk Managers found that nearly 25 percent planned to ex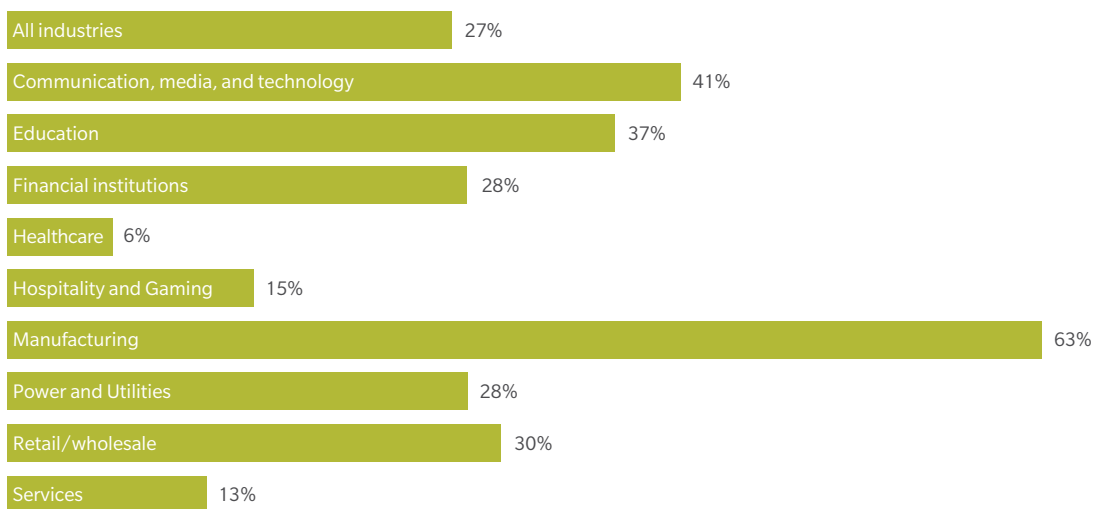plore cyber insurance options over the next 24 months, and a survey of UK risk managers shows that 20.6 percent of companies are buying insurance.[4] However, the same UK survey shows few companies are quantifying their risk exposures. Without a complete understanding of their company's exposure to cyber risk (75 percent) and/or a calculation of the financial impact should an event occur (64.6 percent), these organizations are in a poor position to approach the insurance market and place a value on transferring the risk.

CONCLUSION

As public and private sector organizations restructure and reorganize to become digital organizations, cyber risk management must be embedded in strategies and operations. Organizations that fail to do so will leave themselves exposed in a rapidly shifting risk landscape. ♦

Alex Wittenberg, based in San Francisco, is the Executive Director of Marsh & McLennan Companies' Global Risk Center.

EXHIBIT 2: 2015 CYBER INSURANCE GROWTH RATES BY INDUSTRY (MARSH CLIENTS)

Industry	Growth Rate
All industries	27%
Communication, media, and technology	41%
Education	37%
Financial institutions	28%
Healthcare	6%
Hospitality and Gaming	15%
Manufacturing	63%
Power and Utilities	28%
Retail/wholesale	30%
Services	13%

Source: Marsh Global Analytics

1 The word "cyber" appeared once in the annual reports 2006-2009 before it was flagged as a key emerging vulnerability in the 2010 report.

2 The Future of Cybercrime & Security: Financial & Corporate Threats & Mitigation 2015-2020, Juniper Research, 2015.

3 Sources: The Betterley Report, Cyber/Privacy Insurance Market Survey (2016); Cyber Insurance Market to Triple by 2020 (Sept. 2015); Marsh Benchmarking Trends: Operational Risks. Drive Cyber Insurance Purchases (March 2016)

4 European 2016 Cyber Risk Survey Report, Marsh.

EVERYONE IS AT RISK.

AS TECHNOLOGY AND DIGITAL CONNECTIVITY EVOLVE, COMPANIES GLOBALLY FACE MENACING NEW THREATS EVERY DAY – EVEN AS CYBERSECURITY IMPROVES.

It's a vicious cycle.
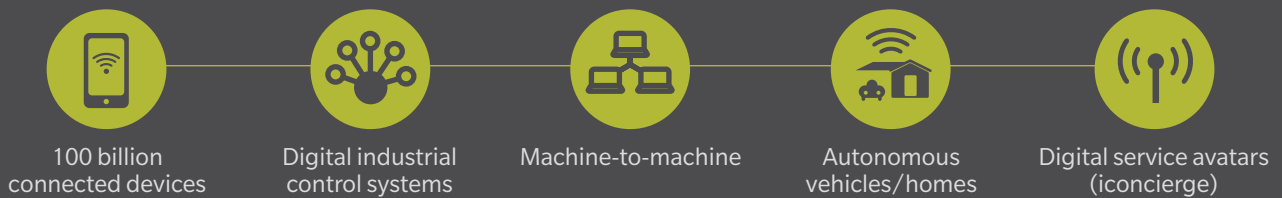As technology advances, our risk for new, sophisticated attacks increases.

Can your company withstand a significant cyber attack and continue operations?

$445 BILLION

THE ESTIMATED ANNUAL COST OF CYBERCRIME TO THE GLOBAL ECONOMY

WELCOME TO THE FOURTH INDUSTRIAL REVOLUTION
Built around cyber-physical systems, the Internet of Things, and the Internet of Services

100 billion connected devices

Digital industrial control systems

Machine-to-machine

Autonomous vehicles/homes

Digital service avatars (iconcierge)

CYBER-PHYSICAL SYSTEMS

THE PATH TO CYBER RESILIENCE

1

IDENTIFY YOUR MOST CRITICAL ASSETS

What do you have that is most valuable to others?

2

GATHER INTELLIGENCE ON CYBER THREATS

Who's threatening you?

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?

Source: *Cyber Resiliency in the Fourth Industrial Revolution*, Hewlett Packard Enterprise, FireEye, and Marsh & McLennan Companies, 2016

CYBER THREAT IS A
SHARED ISSUE

Mark Weil

Cyber criminals are smart, highly innovative, and persistent lawbreakers. The rewards for these offenders are huge. Not only are they after our personal information, they are after our money, and can and will steal it whenever they are able to. Traditional defenses no longer provide adequate protection. Not only will cyber criminals get into our systems – in many instances, they are already there, assessing which data is of value to them and waiting to act. In 2015, 90 percent of large UK organizations reported breaches, highlighting the urgency of addressing cyber risks.

DON'T GO IT ALONE

Actions by government to increase national cybersecurity need to be matched by the private sector. Although individual firms have taken certain measures to ensure their security and ability to recover from breaches, more needs to be done. Cyber threat is a shared issue, and there is little advantage in going it alone.

For example, cyber and terrorism are increasingly risks that overlap one another. Yet the bulk of information about cybersecurity is maintained within the private sector, while terrorism is handled by the public sector. Clearly, there must be greater partnership between the two to prepare critical infrastructure for these intertwined risks.

Furthermore, countries are now confronting a stark new reality of threats against physical assets – including electric grids, dams, telecommunications networks, transportation systems, and civilian nuclear facilities. Ubiquitous connections to the internet have increased vulnerability in the industrial systems that control these physical assets. As the vast majority of critical infrastructure in many countries is owned and operated by the private sector, it is vital that government and industry lock arms in confronting this risk.

Governments have recognized the economic threat presented by cyber risk and are taking a number of measures to

build technological and human resilience across the economy. More than 30 countries – including Germany, Italy, France, the UK, the US, Japan, and Canada – have unveiled cybersecurity strategies. In February 2014, Chinese President Xi Jinping announced a new national cybersecurity body to coordinate security efforts; and in April 2015, Singapore launched a Cybersecurity Agency to oversee policies and conduct cybersecurity outreach.

Governments are supporting the development of cyber defenses through support of research and innovation, knowledge and skill building, and by developing awareness of cyber risks. For example, the UK's Centre for the Protection of National Infrastructure provides good practice, technical guidance, and facilitates information exchange between sectors, including the energy sector and manufacturers of security equipment for national infrastructure. France's cybersecurity strategies, coordinated by the National Agency for the Security of Information Systems, are similarly based on promoting cooperation between the public and the private sector.

Governments are fostering collaborative sharing of information between the public and private sector. Understanding the full cyber risk landscape is difficult for many firms, and government or industry association efforts to support threat and response information are important. The UK's Cyber Security Information Sharing Partnership was launched to support the wider objectives of the UK National Cyber Security Strategy. Such mechanisms enable companies to confidently and safely share information on cyber threats without revealing corporate vulnerabilities, corporate secrets, customers' personally identifiable information (PII), or leaving a company exposed to lawsuits. They also allow companies within the same industry to share information without concerns of apparent collusion.

Police and law enforcement play a critical role in the fight against cyber threats, underlining the need for a

COUNTRIES ARE NOW CONFRONTING A STARK NEW REALITY OF THREATS AGAINST PHYSICAL ASSETS – INCLUDING ELECTRIC GRIDS, DAMS, TELECOMMUNICATIONS NETWORKS, TRANSPORTATION SYSTEMS, AND CIVILIAN NUCLEAR FACILITIES

joint approach between industry and government bodies. Currently, cyber incidents are underreported; organizations must report crime to the police or officials and share information regularly. Through greater cooperation with national bodies such as UK's National Cyber Crime Unit (NCCU) and international agencies such as the European Union Agency for Network and Information Security (ENISA), law enforcement will be able to bring more cyber criminals to justice.

CONCLUSION

To combat cyber threats, the government and private sector need to adopt a mindset that we are all in this together in an urgent fight against a common enemy. Cyber criminals are the hidden enemy, operating behind the scenes and inside our organizations and our devices, and incredibly difficult to detect, take down, and punish. Losing is potentially catastrophic and ultimately, avoidable. Winning will enable us to preserve our society and our way of life. ♦

Mark Weil is the Chief Executive Officer of Marsh's UK and Ireland region.

CYBER TERRORISTS
AND RANSOMWARE
INTERVIEW WITH SHAWN HENRY

W hen the Democratic National Committee based in Washington, DC discovered in June that its entire computer network had been hacked, it called on Shawn Henry, president of CrowdStrike and former head of the FBI's cyber division, to review the damage and identify the perpetrators, which were deemed to be agents of the Russian government.

In this *Brink* interview, Henry shares his views on dealing with the various adversarial groups lurking in the shadows of the internet.

BRINK: What's the biggest cybersecurity mistake you continually run into when you are consulting with companies and why does it keep happening?

Shawn Henry: Companies continue to be reactive, rather than proactive. In other words, they're responding to incidents after the fact, rather than proactively going out and deploying technologies that allow them to get better visibility into the environment and see what's coming. The proactive piece, where companies take security into their own hands or start actively hunting for adversaries in their environment, is the single biggest step that organizations can take.

BRINK: How pervasive is the threat from state-sponsored cyber crime? Does it happen across all public and private sectors and does it go beyond state-sponsored actors?

Henry: A wide range of groups are involved and are pretty prolific. Nation states are targeting organizations for intellectual property and research and development information and corporate strategies. Also, terrorist groups are targeting critical infrastructure. We know that they're developing these capabilities. The organized crime groups are targeting primarily the financial-services and retail sectors. They are increasingly using ransomware, targeting many other types of organizations where they feel that they can get some return on their investment, and it's turning out to be a sizable return for what little investment they make. Healthcare, financial services, manufacturing, government, educational institutions, energy, and transportation – no sector goes untouched.

BRINK: What do you say to a CEO who says, "I'm just a shoe manufacturer. We don't have anything that hackers would want to steal."

Henry: Every business – regardless of what that is – has something that's valuable. First, every company that's in business has something that's of value, otherwise they wouldn't be in business. They have some type of commodity, they have business practices,

they have proprietary information that differentiates them from others in their industry.

Second, adversaries are not necessarily looking just to steal data. We've seen adversary groups that have destroyed networks simply because they're not happy with the company or the way a company is doing business. These adversaries are using the networks as an opportunity to make a statement. It's not just being prepared to protect your data, it's also being aware of the critical risk you face if somebody accesses your network and decides they want to wreak havoc for whatever reason.

BRINK: What's your position on whether companies should pay up when they become victims of a ransomware attack?

Henry: I think that companies shouldn't pay and that instead they should invest their money in developing a continuity of operations plan, such as having a backup strategy so that they can reconstitute their network.

BRINK: The debate over whether companies should be able to "hack back" is getting some more play these days. What's your opinion on that?

Henry: Companies cannot legally leave their network to target somebody else. They can't try to track them down and steal their data back. They can't send malware out to another party. There is probably going to be more debate on this subject as the situation continues to worsen, and there will be calls for companies to be able to take some type of action. But for right now, the law is very clear: They can't do it.

BRINK: Would you support a change in the law that lets companies do that?

Henry: In doing that, you face the risk of companies getting engaged in foreign countries, in foreign laws, and even in dealing with nation states. However, there is a lot that companies can do in terms of collecting and sharing intelligence with the government and work in a more coordinated fashion with others in their industry, to do a better job of identifying who the attackers are. ♦

GO TO **CYBER EXTREMES**

WHAT TO DO WHEN DIGITALIZATION GOES WRONG

Claus Herbolzheimer

For years, conventional wisdom has dictated that organizations focus on preventing the most common types of cyber attacks, rather than preparing for that one all-encompassing disaster that might never occur. But in reality, it is no longer possible to make such a trade-off. Full-blown cyber crises – some of them life threatening – are becoming more common. Increasing digitalization and interconnectedness are exposing organizations more frequently to more sophisticated kinds of cyber threats. Planning for worst-case scenarios is no longer optional.

Consider that just last year 500 million personal records were stolen or lost. Ransomware attacks grew by 35 percent and spear-phishing incidents by 55 percent. These types of attacks are no longer just harming desktop computing. They are starting to cause the malfunctioning of critical medical equipment, emergency services, and fundamental communications. Few organizations' cyber defenses are keeping pace. We estimate that only a third of companies are sufficiently prepared to prevent a worst-case attack. Based on a recent survey by Marsh, Oliver Wyman's sister company, a quarter of companies do not even treat cyber risks as significant corporate risks. Nearly 80 percent do not assess their customers and suppliers for cyber risk. (See Exhibit 1.)

As companies roll out more digital innovations, they need to adopt more flexible and ubiquitous cyber defense measures to meet the more extreme threats they now face. Failing to do so risks unanticipated costs, operational shutdowns, reputational damage, and legal consequences. For example, in response to growing ransomware and spear-phishing attacks, many leading organizations are drawing up fallback plans to operate offline in the event that their operations are crippled. Some are going even further and making operating offline their preferred approach: In response to hacktivists crippling the government's websites through a series of cyber attacks in 2013, Singapore is cutting off access to the internet for nearly all government computers. Healthcare providers and hospitals in the United States and Germany are taking

NEARLY 80 PERCENT [OF COMPANIES] DO NOT ASSESS THEIR CUSTOMERS AND SUPPLIERS FOR CYBER RISK

critical systems partially offline where connectedness is not required and are prepared to go back to pen and paper in case an incident impairs their digital operations.

NEW DATA STRATEGIES

Some organizations are changing the way they use and store data. Classic forms of data and legacy information technology systems are not flexible or smart enough to keep up with rapidly shifting needs to protect records. To respond to cyber threats more rapidly, some companies are radically simplifying their business setups and technical systems. By doing so, companies limit the places where a hacker can enter and hide. Splitting data up and storing the pieces in different systems also reduces the amount of sensitive data vulnerable at any one time.

Other companies are replicating their core information technology systems so clients can receive basic services even if their own systems entirely collapse. For example, some banks are reproducing their key IT systems in the "cloud" to guarantee basic operations can be maintained. Others are striking deals with competitors to step in as proxies in the event of a cyber crisis. These organizations understand

that the ramifications of an attack on their systems go far beyond the damage to their own business: An economic crisis could result if millions of businesses and people were suddenly denied access to their accounts, preventing them from being able to pay salaries or bills.

At the same time, leading organizations are examining if adequate safety nets are in place to minimize the aftershocks of cyber attacks that cascade to the point that they bring down more than one company or industry. Government-backed "cyber pool funds," for example, could mitigate the financial impact of a complete cyber meltdown, similar to funds set aside to assist with the aftermath of terrorist attacks or natural disasters.
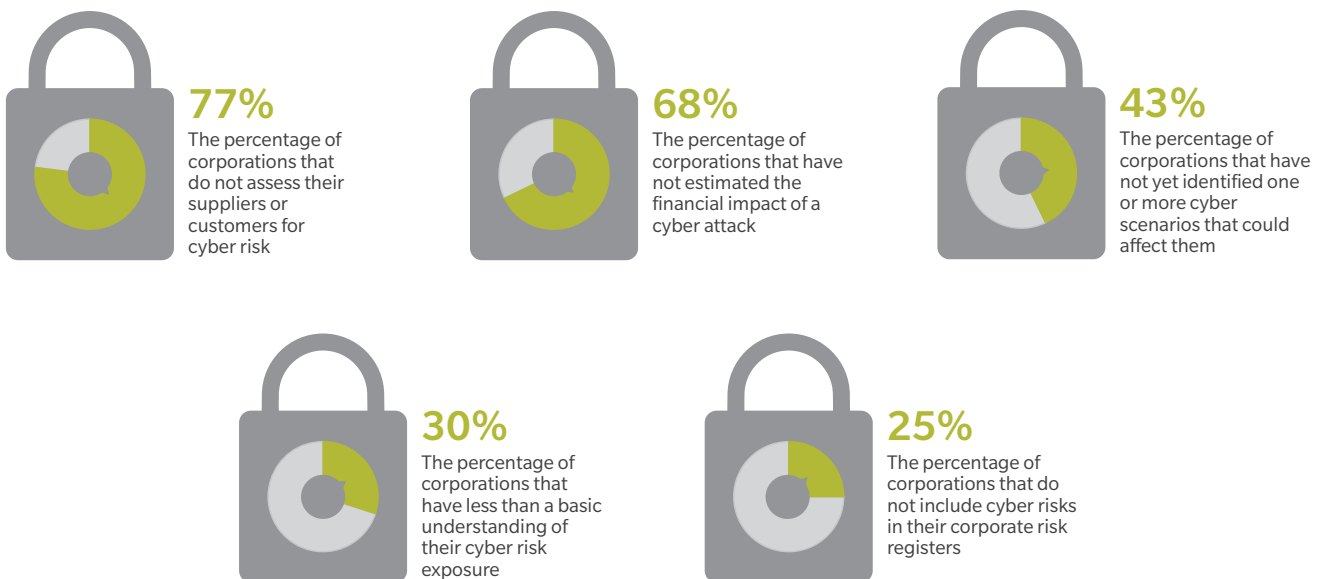
CONCLUSION

The cyber threats that many companies previously considered to be unthinkable are now daily news. To avoid becoming another headline, organizations must prepare for the worst – including the unthinkable. ♦

Claus Herbolzheimer is a Berlin-based partner in Oliver Wyman's Digital practice.

EXHIBIT 1: THE STATE OF CYBER RISK MANAGEMENT AT A GLANCE

Even though the number of targeted cyber-attacks is growing by double digits annually, many medium and large-sized corporations still do not devote sufficient resources to cyber risk management.

77%
The percentage of corporations that do not assess their suppliers or customers for cyber risk

68%
The percentage of corporations that have not estimated the financial impact of a cyber attack

43%
The percentage of corporations that have not yet identified one or more cyber scenarios that could affect them

30%
The percentage of corporations that have less than a basic understanding of their cyber risk exposure

25%
The percentage of corporations that do not include cyber risks in their corporate risk registers

Source: European 2015 Cyber Risk Survey Report, Marsh, Global Risks 2015

HOW EUROPE CAN
FIGHT CYBER ATTACKS
(AND WIN)

Peter Beshar

The cyber landscape in Europe is about to change. As the U.S. presidential campaign enters its home stretch, the issue of cyber security is front-and-center. Rarely a day goes by when a new report of a corporate or government breach fails to make headlines. Across Europe on the other hand, news of major cyber attacks, particularly against European companies, are rarely found on the front pages of *Le Monde, Der Spiegel or La Repubblica*.

Have European institutions done a better job of safeguarding against attacks than their American counterparts? Has Europe just been exceptionally lucky?

The answer to both questions is a resounding no. The unfortunate truth is that breaches are occurring with frequency across Europe.

Last week, I was invited to join a panel at the European Parliament to discuss the state of cyber security and what European companies – and the EU – can do to prevent and prepare for future attacks. There were three core takeaways.

First, the cyber landscape in Europe is about to change profoundly. The adoption of the EU General Data Protection Regulation (GDPR) is a watershed event. For the first time, companies across Europe will be required to disclose data breaches to national data protection authorities and, where warranted, affected individuals. Importantly, failure to do so may result in extraordinary penalties of up to four percent of total revenues.

We already have a window into how the post-GDPR reality will look. After Dutch authorities adopted a "mini-GDPR" that requires companies operating in the Netherlands to report data breaches, more than 3,600 incidents have been logged so far this year. Extrapolate that across the EU and the press, regulators and supervisory boards will demand change in the way European companies conduct business.

Second, companies operating in Europe have quite a journey to travel to prepare for this changed landscape. To gauge their state of readiness, Marsh & McLennan just completed a comprehensive study of the cyber security practices of more than 750 companies across Continental Europe.

On the good news front, awareness of cyber security risk is unquestionably on the rise. The number of companies that listed cyber as a top-five concern has doubled in just the last year, according to the study. And whereas a quarter of European companies in 2015 didn't mention cyber security as a concern at all, this number dropped to 10 percent in 2016.

Yet, while consciousness is rising, far too many companies lag behind. Seven in 10 companies this year reported that they do not have a strong understanding of their cyber posture, according to the study. Moreover, even among companies that profess to have awareness of the threat, too few are taking the necessary steps to defend against attacks or respond to them. In America, the conversation has turned from "if" to "when." Yet in Europe, just 40 percent of companies in our survey have a written incident response plan.

Third, no one has all the answers. Not government. Not industry. And the stakes are rising by the day. Just last week, the director of the International Atomic Energy Agency publicly disclosed for the first time that there was a "disruptive" cyber attack against a nuclear plant.

Against this backdrop, the European Union merits praise for emphasizing that a joint effort between government and industry is required to enhance our collective cyber resilience.

That collaboration can take many forms. An important priority is the monitoring and detection of cyber breaches. This early detection is crucial for reducing the so-called "dwell time" – the amount of time from intrusion to ultimate detection.

According to forensic experts, companies in Europe are currently taking three times as long to identify penetrations of their IT systems.

Just as important, the EU must help companies peel back the secrecy that currently enshrouds cyber incidents. If companies take the step of sharing greater details about the types of attacks and intrusions that are occurring, government should reciprocate by disseminating cyber threat intelligence in real-time. To be effective, the flow of information cannot be a one-way street. While companies are rightfully protective of sharing private, confidential data, there is ample precedent to show that a reasonable balance can be struck between privacy considerations and liability protections.

In recent years, the technology revolution has changed the way virtually every industry conducts business. The lesson of this disruption has been clear: companies that adapt, survive and flourish, while those that stubbornly cling to the past, are left behind. Combatting cyber attacks is no different. With the number and sophistication of attacks on the rise – and the GDPR creating significant financial implications for non-compliance – now is the time to prepare. ♦

Peter Beshar, based in New York, is Executive Vice President and General Counsel of Marsh & McLennan Companies.

NEW **DATA PROTECTION** LAW IN EUROPE

Corrado Zana

We now have a new data protection law in Europe. It has taken more than four years from the publication of the first draft of the regulation in January 2012, but after some painstaking work by European Union (EU) bodies that had to consider an unprecedented 4,000-plus comments and submissions by national supervisory authorities and other stakeholders, it has now been made law.

On May 4, 2016, the General Data Protection Regulation (GDPR) was published in the *Official Journal of the European Union*, and then entered into force 20 days after publication. However, there is a two-year implementation period before EU member states must be fully compliant with the regulations. (See Exhibit 1.) This implementation period allows both EU member states' supervisory authorities and the entities that will be subject to the GDPR time to prepare their organizations for the changes in practice that the GDPR will require.

For those organizations that have not been following the path of this regulation too closely, the sooner you assess the implications of the regulation for your business and implement the required changes, the better. Complying with the regulation will require many organizations to implement a complex privacy management system as an integral part of their information and cybersecurity management system. In addition, key provisions of the GDPR will affect the exposure profile of captured entities, and organizations should review and update their transfer and risk financing strategy. The penalties for noncompliance can be severe, and it is therefore important that compliance be demonstrated well in advance of the end of the implementation period.

WHY DO WE NEED A NEW REGULATION?

The obvious response to this question is to point to the significant evolution in technology that has changed the way in which data is collected and used since the EU Data Protection Directive 95/46/EC (Directive) (implemented in the UK by the Data Protection Act 1998) was adopted in 1995. To provide some context, 1995 was the year that Amazon was launched, but still predates Facebook and Google.

The GDPR text acknowledges that the dramatic increase in data collection and sharing enabled by technological developments means that both public and private entities are able to make use of personal

THE NEW REGULATION WILL HAVE A BROADER TERRITORIAL SCOPE, APPLYING TO NON-EU COMPANIES TARGETING THE EU MARKET

data on an unprecedented scale. The impetus for the European Commission's proposals to update and modernize the Directive was twofold: first, to empower individuals by guaranteeing the right to the protection of personal data that was recognized by Article 8 (1) of the Charter of Fundamental Rights of the European Union and Article 16 (1) of the Treaty on the Functioning of the European Union; and secondly, to help build trust in the online environment, which plays a central role in the wider plans to create a Digital Single Market (DSM).

WHO DOES THE REGULATION APPLY TO?

The new regulation will have a broader territorial scope, applying to non-EU companies targeting the EU market by either offering goods or services or monitoring their behavior. Thus, the regulation will not only apply to companies that are established and/or process data in the EU, it will also apply directly "to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behavior as far as their behavior takes place within the Union."

It is important to understand where your "main establishment" is considered to be under the regulation, as this will govern which member state's supervisory authority will take the role of lead supervisory authority in the event of any complaint and any associated enforcement action. The "main establishment" is not necessarily the corporate HQ, as the regulation defines this to be "where the decisions on the purposes and means of the processing of personal data are taken."

For data processors, the change is even starker, as they are now captured directly by this new regulation. Rather than having their duties defined solely under a

contract with the data controller, the GDPR introduces direct obligations on data processors. As a result, supervisory authorities will now be able to enforce the terms of the regulation directly against processors. The "main establishment" of the processor will be deemed to be "the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union." If their processing activities extend beyond the instructions of the controller, then they may also be deemed a joint controller under the regulation.

KEY CHANGES

Fines: The biggest headline will undoubtedly be the dramatic increase in the size of the fine that can be levied against an offending entity or individual. The single set of rules applying to all EU member states will now reset the fines to EUR20 million or four percent of worldwide annual turnover, whichever is the greater. (Currently in the UK, it is set at a maximum of GBP500,000.)

Looking beyond the stated monetary cap, the more worrisome amendment for many organizations will be the percentage figure, the fact that it is based on turnover and not profit, and the fact that it is based on worldwide turnover rather than the turnover of the entity in the EU country or countries where the offence occurred. For any global organization with activities inside the EU that are captured by the regulation, this will be of particular concern.

Territory: As discussed in the preceding paragraphs, many organizations that were not previously subject to EU data protection law will now find that they are captured by the new regulation. These organizations will need to ensure that their business practices as regards personal data reflect the requirements of the

EU, as well as any additional territorial regulation that they may have been operating under.

Consent: The GDPR will impose some stricter obligations on organizations where processing is based on consent, making it far harder to obtain. The new regulation requires data controllers to demonstrate that consent was given and requires there to be "clear affirmative action." Silence, pre-ticked boxes, or inactivity will not constitute consent. In addition, where controllers rely on consent for the processing of sensitive data, the regulation requires consent to be "explicit."

Profiling: Always a highly contentious area of data protection practice, the regulation will introduce new restrictions aimed at targeted advertising based on data subject profiling. Specifically, it prohibits organizations from taking decisions "based solely on automated processing, including profiling, which produces legal effects concerning [a data subject] or similarly significantly affects [a data subject]."

Privacy Function: Going forward, there will be no requirement to register data collection and processing activities with supervisory authorities, or lodge any statements (as required by certain member states' supervisory authorities) as to the nature of processing activities. However, the regulation does set the requirement for detailed records of data collection and processing activities to be kept internally that will likely go beyond that information currently submitted to supervisory authorities. Controllers will not just have to comply with the law, but be able to demonstrate and verify compliance through implementation of "appropriate technical and organizational measures."

Data Protection Officer: Where the processing is carried out by a public body or where "the core activities of the controller or the processor consist of processing operations which, by virtue of their nature,

EXHIBIT 1: TIMELINE FOR IMPLEMENTATION OF GDPR
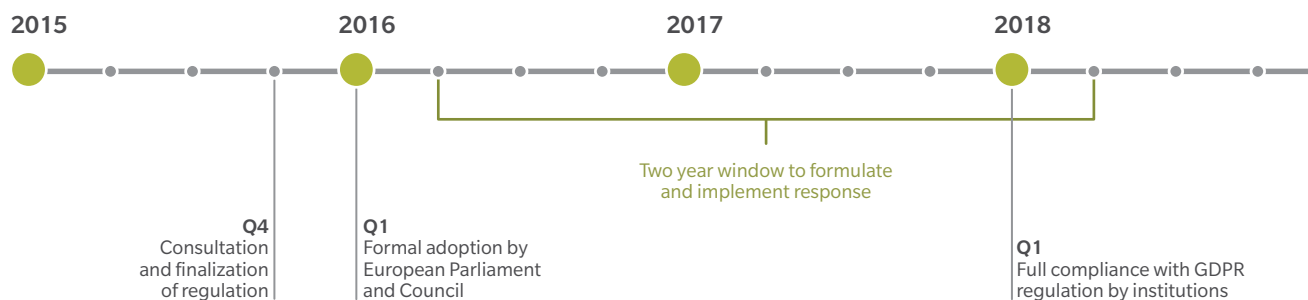
Source: Marsh Risk Consulting

their scope, and/or their purposes, require regular and systematic monitoring of data subjects on a large scale, or the core activities of the controller or the processor consist of processing on a large scale of special categories of data," there will be an additional requirement to appoint a Data Protection Officer, and the regulation lays down certain requirements as to who that can be and the nature of the role.

Privacy by Design: The GDPR will embed privacy considerations in the design phase of any new product or service that touches personal data or technology that processes it. To ensure this happens, there is now a specific requirement (previously recommended by certain member states' supervisory authorities) for organizations to undertake data privacy impact assessments in the event that the relevant processing operation is "likely to result in high risk to the rights and freedoms of natural persons."

Breach Reporting: The Directive contains no specific requirement to notify either the relevant supervisory authority or affected data subjects of a data breach, though a patchwork of national laws and guidance papers had begun to emerge to plug this gap. Now, under the GDPR, all organizations will be required to notify a personal data breach to the supervisory authority "without undue delay and, where feasible not later than 72 hours after having become aware of it," unless the breach is "unlikely to result in a risk to the rights and freedoms of natural persons." Organizations will also be required to notify personal data breaches to data subjects when the breach is "likely to result in a high risk to the rights and freedoms of natural persons." These stiff new reporting requirements bring the EU far more in line with the US, where the notification of data breaches has been the norm for many years. An exemption from notifying data subjects exists where data is "unintelligible," for example, as a result of encryption.

Enhanced Rights: Data subjects will have certain rights enhanced in the new regulation that will create certain operational challenges for organizations in order to comply. Those rights include enhanced subject access rights and the more widely discussed right to erasure (commonly referred to as "the right to be forgotten"), which previously existed under law in relation to deletion of data, but has been expanded, in particular, following the decision by the Court of Justice of the European Union (CJEU) in *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014).*

Insurance Implications: This new set of data protection obligations introduces certain additional

DATA BREACH
BY THE NUMBERS

Data breach cost to European companies is an average of **US$146 to $211 per compromised record** (approximately 46 percent pertains to direct costs and 54 percent to indirect costs)*

$3,925,000
Average total organizational cost of data breach in Europe*

52%
The percentage of breaches caused by negligence or IT glitches*

In the UK, **90 percent** of large organizations and **74 percent** of small organizations reported they had a security breach**

76%
The percentage of scanned websites with security vulnerabilities***

Sources: *Ponemon 2015 Cost of a data breach study;
**HM Government 2015 Information Security Breaches Survey
***Symantec Internet Security vulnerability report April 2015 volume

EXHIBIT 2: RESPONDING TO GDPR: HIGH-LEVEL ACTION PLAN

The General Data Protection Regulation (GDPR) is now a reality and European companies and non-EU controllers and processors treating data of EU citizens should immediately begin to adapt and implement privacy management systems.

GAP ASSESSMENT	BUSINESS NEEDS	PLANNING	IMPLEMENTATION
What personal data is managed, how and why, data flow	What we will continue to do, what we will not do anymore, what we are going to do	Implementation of the privacy risk management program distinguishing and integrating a Management plan and a Technology plan	Overall Privacy Management System
Role and management of external Data Processors	How to manage data to ensure compliance with regulation		Technological measures
IT related key points: processed and stored digital data, system administrators' procedures, logs, ...	What technical and organizational solutions have to be implemented		Organizational measures
			Third-party risk management process

Source: Marsh Risk Consulting

obligations, sanctions, and breach response requirements that have the potential to dramatically alter the financial impact of an instance of noncompliance. These financial consequences are likely to see an upwards shift in the loss estimates attached to any data protection items in the company's risk register, potentially breaching acceptable risk tolerances. This adjustment is likely to lead to a re-examination of the adequacy of insurance arrangements. Indeed, it can be expected that the compulsory notification of data breaches will likely drive a growth in the EU cyber insurance market as per the US, which is currently the largest cyber insurance market, worth at present more than US$2 billion.

REVIEW INSURANCE COVERAGE

Organizations will need to understand the effectiveness of the coverage bought, the sufficiency of any applicable indemnity limits, as well as the availability of enhanced insurance protection if existing arrangements fall short of requirements. In particular, organizations may wish to consider their insurance protection related to the following:

- The ability under the GDPR for complainants to seek a judicial remedy of a supervisory authority's decision not to pursue a complaint and/or the right of the data subject(s) to seek compensation for the breach as part of a group action. This may lead to a higher number of litigation cases from data

subjects and more aggressive enforcement by supervisory authorities who are reluctant to see their decisions challenged.

- The maximum level of fine is due to increase to the greater of EUR20 million or four percent of worldwide turnover for the entire organization and not just the offending entity. This will significantly add to the potential financial downside for more serious breaches of the regulation. Not only should organizations consider the higher level of fine, not always fully insurable in EU countries, but due to the amounts involved, there is the potential for a more protracted and costly legal process as organizations are likely to explore all potential avenues of challenge against the supervisory authority's decisions.

- The new requirement to notify data subjects without undue delay when a data breach is "likely to result in a high risk (to) the rights and freedoms of individuals" will result in significant expenditure for organizations to implement and manage the practical steps of this requirement where high volumes of personal data are involved.

- The potential for high public awareness of data breaches with associated press attention driven by the new notification requirements should cause organizations to consider any short-term trading impact due to diminished reputation and customer trust. Organizations may also wish to consider the cost of implementing any reputational

mitigation strategy and insure the additional expenses related to brand protection, such as advertising campaigns,hiring of specialized crisis communication firms.

These changes are set to bring the exposure profile of European organizations more in line with US firms, which have had to deal with breach notification obligations and associated privacy litigation for more than a decade. The US experience provides a useful reference point for analysis of the potential cost of EU data breaches in the future, particularly the cost of delivering the crisis management response. For any organization concerned with the status of their existing insurance arrangements, the following questions should be addressed:

- Does the insurance program deliver adequate protection for a breach of privacy law and regulation?
- Does the insurance program deliver adequate protection for the cost of delivering against GDPR breach notification obligations?
- Does the insurance program deliver adequate protection for group action litigation by affected data subjects?

- Does the insurance program deliver adequate protection for the costs connected to an investigation by a supervisory authority?
- Does the insurance program deliver adequate protection for legally insurable fines imposed by a data protection supervisory authority?

CONCLUSION

Along with assessing existing insurance arrangement, organizations should consider their overall exposure and the optimal risk financing approach, including the following steps:

- Using risk identification and exposure modelling of data and technology-related risks to create a unique profile for the organization.
- Completing an insurability assessment to identify the effectiveness of existing coverage arrangements against the risk profile and deliver recommendations for future treatment.
- Defining the optimal insurance solution utilizing the additional capabilities of the insurance market to deliver specific cover against privacy and technology-related exposures. ◆

Corrado Zana, based in Milan, Italy, is the Business Resilience Practice Director for Marsh Risk Consulting Continental Europe.

KEY POINTS

- Fines for the most serious breaches to increase to the greater of EUR20 million or four percent of total worldwide annual turnover.
- Extraterritorial scope.
- Requirement for data controllers to demonstrate that consent was given and requirement for there to be "clear affirmative action."
- Explicit consent required to collect sensitive data.
- Direct obligations on data processors.
- New restrictions on the profiling of data subjects.
- Requirement for organizations to be able to demonstrate and verify compliance.
- Requirement to appoint a data protection officer for public bodies or where processing operations require regular and systematic monitoring of data subjects or where they are processing on a large scale special categories of data.

- Data privacy impact assessments are required for certain new or changed products and services.
- Organizations are required to notify a data breach to the supervisory authority "without undue delay and, where feasible, not later than 72 hours," unless the breach is "unlikely to result in a risk to the rights and freedoms of natural persons."
- Organizations are required to notify a data breach to data subjects "without undue delay" when the data breach is "likely to result in a high risk to the rights and freedoms of natural persons."
- New and enhanced rights for data subjects, including the right to erasure and enhanced subject access rights.

CYBER RISKS **BY INDUSTRY**

POWER AND UTILITIES

- Critical power and utilities infrastructures face unique cyber risks, as digitization and direct connection of operational technology to enterprise IT networks and the internet dramatically increase cyber exposure. The industrial control systems (ICS), and supervisory control and data acquisition (SCADA) systems on which these infrastructures depend can be vulnerable to cyber attacks.
- The risk is real. A December 2015 hack on three power distribution companies in the Ukraine caused power outages to 80,000 energy customers. The hack began with a spear-phishing campaign that targeted IT staff, and from there the attackers remotely manipulated the utility's SCADA systems.
- To mitigate the impact and costs of a power grid interruption, utilities continue to increase cybersecurity measures and work together on cross-industry cyber threat intelligence-sharing initiatives. The industry is embracing the transformational potential of digital technology, while continuing to preserve the resiliency and reliability of the power grid.

FINANCIAL SERVICES

- Cyber attacks on financial services firms can not only lead to financial losses, but can also increase litigation exposure and damage to an institution's reputation and brand – and with it, customer confidence and trust.
- With losses to cyber crime among financial institutions estimated at nearly $1 billion over the past two years, banks are not immune. In February 2016, cyber attackers on a Bangladesh bank made off with $81 million through a transfer over the SWIFT network, which is used globally for inter-bank transfers. The attackers are still unknown.
- To manage risks, companies in the financial services sector must find a risk-based operating point in cybersecurity that balances protection against cyber attack with detection and response capabilities.

HEALTHCARE

- Healthcare companies are attractive targets for cyber attacks due to the sensitive – and salable – data they manage, including private health information (PHI) and financial data.
- One survey found that US healthcare companies were the target of 88 percent of ransomware attacks that can limit access to critical files or systems.
- The industry faces increasing challenges with the growing deployment of internet-enabled medical devices, online healthcare portals, advanced consumer-oriented applications and wearable devices, and increased use of electronic health records.

MANUFACTURING

- Manufacturing is susceptible to cyber threats, given increasingly complex supply chains, network-controlled production lines, and the hyper-connectivity of "Industry 4.0." The manufacturing sector was the leading target of infrastructure cyber attacks in the US in 2015.
- In 2014, hackers attacked the business and production network of a German steel mill to access to the mill's control systems and trigger an unscheduled shutdown of the furnace, causing massive damage to equipment.
- Cyber risks inherited from external connections, such as supply chain and trading partners, service providers, and other affiliates, are particularly acute in the manufacturing sector, and must be continuously monitored, analyzed, and managed with a well-defined program.

RETAIL

- Point-of-sale (POS) systems have been a key entry point for many retail data breaches. Along with recent advances in POS technology comes new malware that targets POS systems to capture payment card data and gain access to other corporate systems.
- In recent years, hackers have acquired the credit card information of millions of retail shoppers, which they can readily sell with point-and-click e-commerce functionality on the hacker Dark Web.
- Technologies that retailers and the payments system as a whole are implementing to protect against cyber attacks include end-to-end encryption (E2EE), tokenization, becoming EMV compliant, testing systems, and focused staff training on POS system security.

EDUCATION

- Universities and other institutions of learning, with their culture of openness and information sharing, are highly susceptible to cyber risk. Data breaches can turn into high-visibility problems, such as identity theft, electronic stalking, compromise of health data, theft of intellectual property (first- and third-party), and other liabilities.
- In early 2016, a well-known US university fell victim to an attack on its financial management software that compromised the information of 80,000 current and former students, employees, and vendors.
- Educational institutions are taking efforts to increase risk mitigation. For example, in 2015, there was a 37 percent increase in cyber insurance purchases in the education sector. Educational institutions must focus on ensuring all users, including staff, academia, and students, follow effective cybersecurity practices.

RISKS

QUANTIFYING CYBER RISK

THE CORE OF EFFECTIVE RISK MANAGEMENT STRATEGY

Arvind Parthasarathi

No matter how much money you spend on cybersecurity technology, no vendor can guarantee that you will not suffer a breach. As executives attempt to optimize their dollars spent on the best cyber solutions, the focus has moved away from chasing technologies that address this or that specific threat, and towards the more sustainable solution of understanding risk and transferring it accordingly. The question has shifted from: *What processes and technology can I put in place to guarantee that I do not have a data breach?*, to: *What is the likelihood that my company will suffer a breach, and what is the associated severity of potential events?* Quantification of cyber risk in probabilities, as well as in dollars and cents, is crucial to drive a meaningful and impactful cyber risk management strategy.

The growing frequency and severity of cyber incidents have alarmed major credit agencies, prompting many to begin assessing the overall cyber risk of their rated entities and evaluate what effect this risk has on a company's likelihood of credit default. Furthermore, key financial regulatory bodies, such as state departments of insurance, are including cyber risk assessments of their regulated entities in examining market conduct and capital adequacy. Recently, New York state proposed the nation's first cybersecurity regulation, which requires institutions regulated by the New York Department of Financial Services to establish and maintain a cybersecurity program that protects consumers and ensures the soundness of the financial services industry in New York.

As the cyber insurance industry gathers momentum, understanding the frequency and severity of events has become critical for the companies purchasing coverage, the brokers placing coverage, and, of course, the insurers providing the capacity and assigning a price to the risk. Spending on cybersecurity technology and services has grown steadily over the past few decades, eclipsing $75 billion in 2015, yet the frequency and severity of breaches has also continued to grow exponentially over the same time period. Companies that spend hundreds of millions of dollars get breached right alongside those that spend a fraction of that amount. How then does an insurer distinguish and price risk?

UNDERSTANDING CYBER DEFENSE AND OFFENSE

To date, cyber risk assessments have focused on the cybersecurity technology implemented by a company. But technology, while important, is an insufficient predictor of a company's defensive cyber posture; to gain an adequate understanding of the company's susceptibility to attack, an analysis of the company's people and processes behind that technology must also be included.

Although attacks are often technical in nature, their lynchpins typically reside in human and behavioral elements. Additionally, a majority of the events covered by cyber insurance policies have nothing to do with issues relating to the cybersecurity technology a company has in place, but are instead due to human errors from lost or stolen devices and erroneously sent documents to malicious employees exploiting legitimate system access to engage in criminal activities. Any assessment of a company's defensive cyber posture must therefore include an evaluation of the people and processes behind the technology in order to accurately measure a company's resilience in fending off attacks. Consider that in some recent high-profile breaches companies had the latest monitoring software, which performed its task and detected malware. However, when the people and processes behind the technology failed to respond adequately to the alarms, the technology proved of little consequence. Knowing how susceptible an organization is to a cyber attack goes well beyond knowing what technology it has in place.

Moreover, assessments that focus primarily on a company's susceptibility are the equivalent of betting on a football game while knowing only the quality of a team's defense – and ignoring its offensive capabilities. To gain a better understanding of a company's overall cyber risk, we must model the situation appropriately as a multifactor human behavior problem where rational actors are optimizing their own value functions (theft, espionage, vandalism, activism, etc.). Unlike hurricanes, earthquakes, and tornadoes, cyber attacks are deliberate acts, not random stochastic events; in dealing with motivated and capable adversaries, we must look beyond the traditional technology audit and

consider the lenses of game theory and behavioral economics. Susceptibility (defense) and motivation (offense) provide a balanced perspective on a company's potential to fall victim to a successful attack resulting in data breaches, business interruptions, and cyber extortion events.

Cyence has created a comprehensive platform for the economic modeling of cyber risk – from assessing the individual risk of companies to examining the potential aggregate effects of accumulated events harming multiple companies simultaneously. The Cyence platform draws from both an understanding of an organization's defenses, through a technology, people, and process-driven lens, as well as an understanding of the motivation behind threat actors such as criminals, hacktivists, and rogue insiders. Cyence's risk assessments are used by Marsh to help their customers to efficiently and effectively evaluate an enterprise's own risk, as well as the risk of their vendors, business partners, or potential acquired companies. Cyence is also used by insurers to make underwriting and pricing decisions, and monitor accumulation risk.

When looking at a broad swathe of about a million companies, Cyence's models are able to differentiate between high risk and low risk companies with significant precision. Those companies rated as the riskiest had 1,500 times the number of events as those companies rated as the least risky between July 2015 and July 2016.

A solid understanding of the likelihood of a company falling victim to a cyber event is essential to assessing overall cyber risk and developing a board-level enterprise risk strategy around it. Companies can use this information to drive discussions around the value of dollars spent to mitigate cyber risk through improved technology and processes or spending money on risk transfer solutions like cyber insurance policies. Understanding the severity of losses is the next piece of the risk puzzle needed to answer questions for enterprises such as: *How much insurance coverage should I buy?*, or questions for underwriters: *How much coverage should I offer? And at what premium and retention levels?*

Cyber events have a wide range of potential impacts from minor events affecting a few customer records to major events incapacitating systems and affecting hundreds of millions of records, thus jeopardizing enterprises existentially. Perhaps the most valuable assets protected by a company are its intellectual

THOSE COMPANIES RATED AS THE RISKIEST HAD 1,500 TIMES THE NUMBER OF EVENTS AS THOSE COMPANIES RATED AS THE LEAST RISKY BETWEEN JULY 2015 AND JULY 2016

property and brand reputation, both of which are lacking meaningful coverage or capacity from the insurance markets, but which nevertheless have massive financial impact for the company. Cyence has built company-specific event severity models to help quantify not only how often events are likely to occur, but also the severity distribution for different companies.

While there has been much discussion around retail and healthcare companies, the reality is that all sectors are at risk to cyber events. For instance, when looking at a leading multibillion dollar material manufacturing company, we can see from their loss distribution that events range from $0 to rare but extreme losses exceeding $1.5 billion. Armed with this information, companies and boards of directors can employ a data-driven enterprise risk strategy, and insurers can craft policies in a sustainable manner to account for the cost of the underlying risk.

UNDERSTANDING AGGREGATED RISKS IN THE SPPLY CHAIN

Frequency and severity are the fundamentals necessary to evaluate and price the risk of an individual company in a vacuum, but enterprise risk management and insurance portfolio management also require knowledge of the accumulation of common risk among groups of entities. Due to a variety of common paths in technology and business choices, as well as nondiscriminating attacks from some bad actors, there exists correlated cybersecurity risk across companies. A portfolio (or supply chain) of great individual risks can still present a host of aggregation issues due to accumulations of risk on a variety of dimensions, from the obvious ones like common service providers and ubiquitous hardware and software technologies to the more esoteric and nonobvious. These paths of aggregation can lead to cascading losses in a portfolio, or concurrent service interruptions in a supply chain.

Just as a hurricane can decimate an entire shoreline neighborhood, cybersecurity risk has the potential for aggregated single events or groups of events causing harm to many parties simultaneously.

For example, many companies share common infrastructure when accessing the internet and cloud computing resources. An outage at a technology service provider operating this shared infrastructure has the potential to affect many companies simultaneously. Once you understand accumulations within a portfolio, it is important to explore disaster scenarios to test the potential outcomes of everything from power outages to ISP interruptions to cloud provider disruptions to the emergence of new zero day vulnerabilities on a variety of the most widely used software and hardware technologies and many others, all based on real data.

When simulating a disaster scenario of a week-long outage at one of Amazon's most commonly used data centers, we see that losses depending on the exact scenarios to the S&P 100 group of companies can potentially exceed $12 billion. Insurers will need to incorporate these tail loss events when evaluating the adequacy of their pricing. Increasingly, regulators and rating agencies are paying closer attention to these extreme events and insurers' aggregate exposure when evaluating capital adequacy and credit risk.

Lloyds of London's has been very public on their goals of understanding accumulations for various cyber disaster scenarios. But beyond direct cyber incidents like a cloud provider outage, perhaps the more concerning incidents are silent cyber scenarios exposing noncyber insurance products to potential cyber-related losses. Lines of coverage like property tend to have limits that are orders of magnitude higher than a typical tower of cyber insurance coverage; additionally, these policies have not contemplated or charged for cyber-related risks and, unless specifically excluded, could be exposed to losses occurring at the intersection of cyber and physical events.

CONCLUSION

By examining both the cyber risk of individual organizations, as well as the potential aggregate impacts of a range of scenarios and outcomes, Cyence enables the development of a comprehensive view of the elements that contribute to an organization's cybersecurity risk, how it benchmarks against its peers, and how to manage that risk over time. Understanding the primary vectors of cybersecurity risk to an organization can help drive informed enterprise risk management strategies and empower insurers and reinsurers to efficiently, effectively, and consistently evaluate cybersecurity risk of insureds, and monitor the accumulation exposures of portfolios accordingly. ♦

Arvind Parthasarathi is a founder and the
CEO of Cyence.
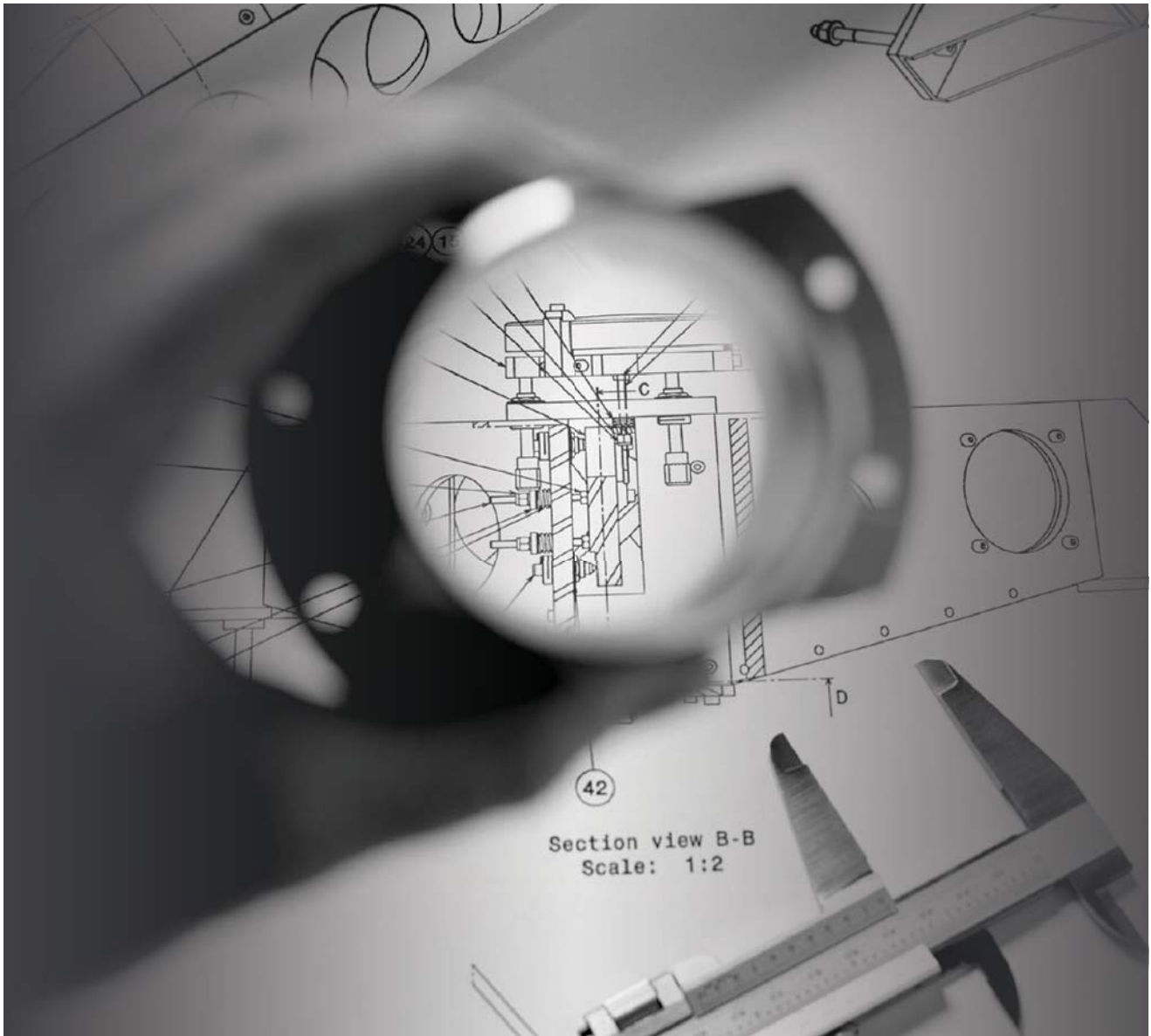
MEASURING CYBER AGGREGATION RISK

Ashwin Kashyap and Julia Chu

Cyber risk is now an embedded feature of the global risk landscape, and preventative risk management and post-event remediation are gaining importance as shareholders, customers, supply chain partners, and regulators are increasingly focused on how companies are managing for cyber risks. Insurance is becoming an important piece of the strategy for helping businesses address these risks.

Cyber insurance is one of the fastest growing lines for insurers and reinsurers. While insurers are developing pricing tools for underwriting cyber risks, the focus on aggregation has increased – how to understand and control their potential exposure. Unlike traditional property insurance where aggregation is monitored by physical locations, cyber insurance

aggregation can span connected systems that extend beyond physical geographies. While a large systemic risk has not yet materialized, it does not mean the risk is not present. Moreover, there is limited history and lack of data for this emerging exposure, which makes it difficult for insurers to measure cyber risk and calculate capital needs. In other words: how to grow a portfolio of cyber risks profitably, without exceeding risk tolerances.

For decades, insurers have considered aggregation from natural perils, and developed catastrophe models. These models go beyond the insured loss experience by blending the historical evidence and expert understanding of the nature of the peril, and provide a more robust understanding of future exposure. Modeling for cyber risk introduces new challenges, including:

- **Changing perils:** The types of cyber attacks, as well as the nature/motivation of the attackers, are in constant flux.
- **Extended duration:** Related attacks against different defenders may take place simultaneously, or may repeat over a period of months.
- **Definition of damage:** Cyber damage is harder to quantify, due to the gap between the technical and business impact.
- **Reporting lag:** It may take days/years to discover the cyber attack

Much of the cyber aggregation research to date in the insurance industry and academia has concentrated on finding a handful of potential attack scenarios and assessing the likely impact. But there is a gap in understanding who is likely to launch these attacks, what their primary motivations are, and ultimately how they accomplish these attacks without getting compromised. All of these dimensions play a critical role in the quantitative assessment of risk posed by these scenarios.

Symantec, in collaboration with Guy Carpenter, has developed a series of frameworks to systematically break down this complex problem into tractable components. Many of these components are impossible to observe directly from insured exposure or historical loss (much as wind or tides could not be inferred purely from insured hurricane loss.) But as a cybersecurity expert, Symantec has spent decades tracking the emergence of new cyber threats and attack vectors, and has unparalleled proprietary telemetry database, providing a unique capability to identify and quantify the nature of each phase of cyber attacks.

First and foremost, it is important to distinguish between the technical and business impacts of a cyber attack. The technical impact provides a mechanism to

CYBER INSURANCE IS ONE OF THE FASTEST GROWING LINES FOR INSURERS AND REINSURERS

understand how an attack was carried out, but rarely provides a handle on the far greater consequences on a collection of businesses. To resolve this, Symantec has invented the CUBE framework that clearly articulates every facet that is relevant to a business user.

The framework consists of six complementary dimensions to break down the technical complexity of a cyber attack into a meaningful and complete narrative. The dimensions are:

- Attackers
- Targets
- Objectives
- Vulnerabilities
- Impact
- Consequences

We will take a specific aggregation scenario to illustrate how this framework plays a useful role in describing these events. A cloud service provider disruption scenario has been widely regarded as one of the manifestations of aggregation on cyber portfolios. In the narrative below, the business impact on a leading cloud platform lasts for 24 hours and causes cascaded impacts on other businesses dependent upon its services. The attack is caused by a state-sponsored threat actor whose primary motivation is to showcase their sophisticated technical capabilities to the rest of the world. This scenario can play out in many different ways, and we can use the CUBE framework to showcase one such realization of this scenario.

The multi-dimensional view of risk provided by the CUBE framework not only helps insurers understand the key aspects of a scenario but also helps them control risk aggregation by avoiding higher degrees of exposure in their portfolios to the "footprints" of each of the attacks. The framework also minimizes the possibility of a misrepresentation of the description of a scenario and, consequently, the quantification of its frequency and severity. In essence, the CUBE framework provides a foundation to create an event set that can be understood easily by business users in the context of managing cyber aggregation risk.

It may be essential to think beyond the CUBE framework for building sophisticated risk models where

ATTACKER(S)

NAME Iranian Cyber Army

TYPE OF THREAT ACTOR Nation State

SUB-TYPE Nation State-sponsored

OUTSIDER/INSIDER NATURE Outsiders

GEOGRAPHY Iran

DEMOGRAPHICS Unknown

TRACK RECORD Operation Abadil (2012)/
Operation Cleaver (2014)

MODUS OPERANDI APT

COMMUNICATION CHANNEL(S) Unknown

TARGET(S)

NAME Leading cloud platform provider

VERTICALS Cloud Services

LOCATION Global

PRIMARY ASSETS All types – GovCloud-focused

EMPLOYEE COUNT Est. 15,000 - 20,000

CUSTOMERS 1 million (30%+ market share)

RECORDS HELD -

ANNUAL REVENUES $8 billion (2015)

HISTORY WITH CYBER ATTACKS Mostly at
individual customer level

PEERS Amazon Web Services, Microsoft Azure,
IBM Cloud Services, Google Cloud Platform,
Salesforce Service Cloud, Rackspace Cloud, etc.

OBJECTIVE(S)

PRIMARY MOTIVE Compromise targeted system
availability as long as possible

SECONDARY MOTIVES None

INTENDED IMPACT (1) triggering relatively small
short-term economic losses (business
interruptions), (2) shattering corporate
and public confidence in cloud solutions, and (3)
showcasing Iranian Cyber Army capability as
payback for recent wave of intrusion (payback)

LIKELIHOOD OF SCALING ATTACKS
Low-Medium

CUBE FRAMEWORK
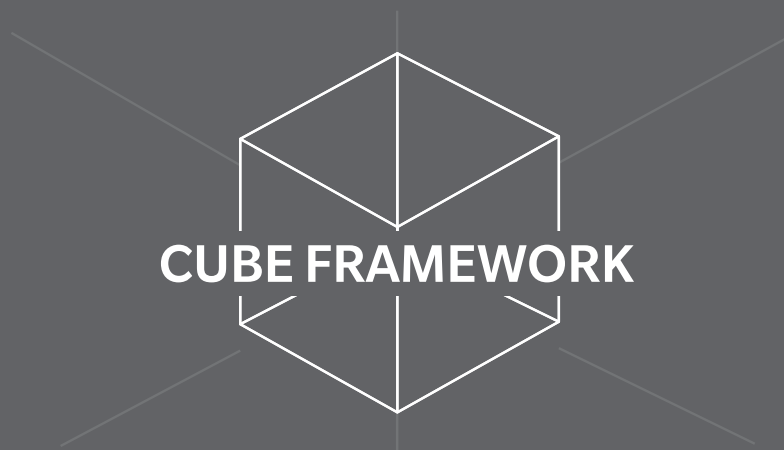
VULNERABILITIES

**VULNERABILITIES MOST LIKELY TO
BE EXPLOITED** Human targets (large employee
count/very large user base), software
vulnerabilities (host servers use variants of
Red Hat Linux and Xen hypervisor), reliance on
critical infrastructure (electricity, network, etc.), etc.

HORIZONTAL Outage

DEFENSE POSTURE OF TARGET Advanced –
secure overall architecture – playbook for
standard DDoS attacks

**RELATIVE PREPAREDNESS OF TARGET
COMPARED TO PEERS** Highest

**LIKELIHOOD OF SUCCESSFUL ATTACK GIVEN
DEFENSE POSTURE** Low-Medium

Source: Symantec

IMPACT

LOSS QUANTIFICATION ASSUMPTION
Bottom-up economic model

ACTUAL ECONOMIC LOSSES $75 million

ACTUAL REPUTATION LOSSES 2% - 5%
market share

INSURABLE COMPONENT OF LOSSES
$10 million

**DURATION AND INTENSITY
OF ATTACK** Cloud services unavailable
for 24 hours

REALIZED IMPACT Shattered confidence in
the the cloud services industry creates
concern among companies

CONSEQUENCE(S)

TIMING OF INSURANCE CLAIM FILING Six plus
months after the event

AFTERMATH FOR TARGET Forensics
investigation/computing job day credits offered
to affected customers/additional expenses
incurred to beef up security
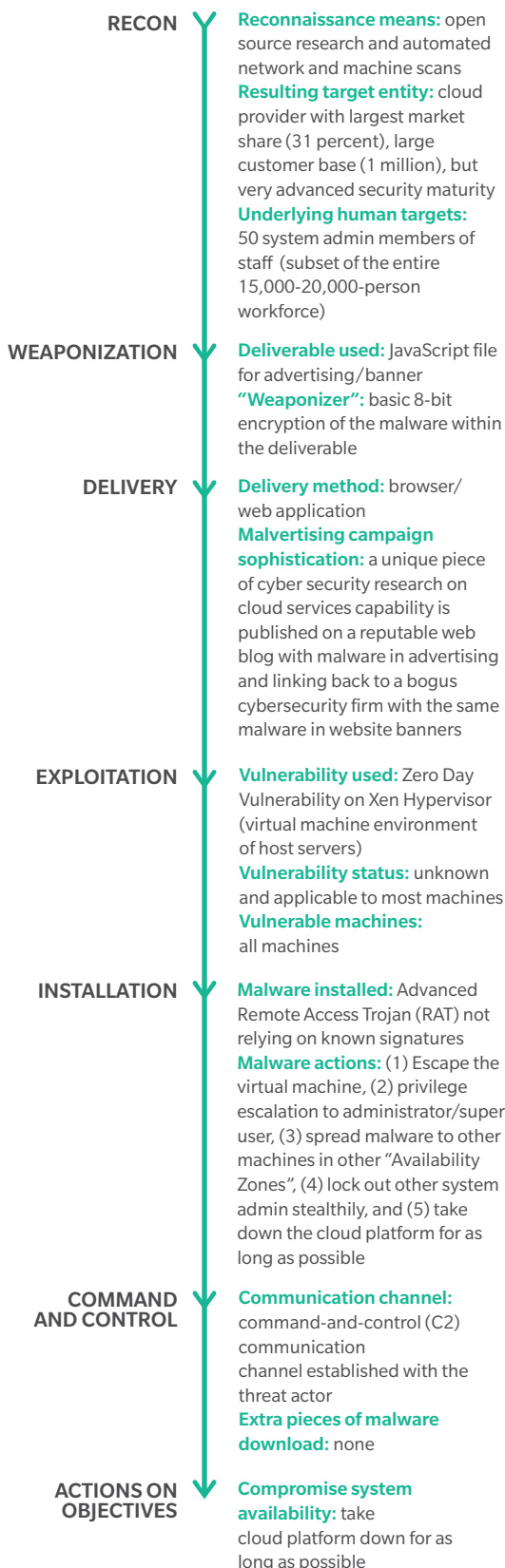
LEGAL REPERCUSSIONS FOR TARGET Most
likely none

RESTORATION DURATION Two to three days for
full service/performance recovery

AFTERMATH FOR THIRD-PARTY Cyber
insurance business interruption claims made
by companies/some customers challenge
the vendor

LEGAL REPERCUSSIONS FOR ATTACKER None

EXHIBIT 1: EXAMPLE KILL CHAIN

RECON

Reconnaissance means: open source research and automated network and machine scans
Resulting target entity: cloud provider with largest market share (31 percent), large customer base (1 million), but very advanced security maturity
Underlying human targets: 50 system admin members of staff (subset of the entire 15,000-20,000-person workforce)

WEAPONIZATION

Deliverable used: JavaScript file for advertising/banner
"Weaponizer": basic 8-bit encryption of the malware within the deliverable

DELIVERY

Delivery method: browser/web application
Malvertising campaign sophistication: a unique piece of cyber security research on cloud services capability is published on a reputable web blog with malware in advertising and linking back to a bogus cybersecurity firm with the same malware in website banners

EXPLOITATION

Vulnerability used: Zero Day Vulnerability on Xen Hypervisor (virtual machine environment of host servers)
Vulnerability status: unknown and applicable to most machines
Vulnerable machines: all machines

INSTALLATION

Malware installed: Advanced Remote Access Trojan (RAT) not relying on known signatures
Malware actions: (1) Escape the virtual machine, (2) privilege escalation to administrator/super user, (3) spread malware to other machines in other "Availability Zones", (4) lock out other system admin stealthily, and (5) take down the cloud platform for as long as possible

COMMAND AND CONTROL

Communication channel: command-and-control (C2) communication channel established with the threat actor
Extra pieces of malware download: none

ACTIONS ON OBJECTIVES

Compromise system availability: take cloud platform down for as long as possible

Source: Symantec

uncertainty quantification becomes the primary goal. For this purpose, Symantec recommends using the "kill chain" methodology below for a technical persona to capture the different phases of a cyber attack. For example, an insider attack on a confidential database in a large data aggregator will have a very different likelihood when compared to a financially motivated threat actor carrying out the same attack through a phishing campaign. A sequential model can capture this differentiation, specifically in the area of frequency quantification. More importantly, the quantification can be driven by security telemetry that Symantec has access to.

Here is a description of the same scenario from above using the kill chain to illustrate the concept. The kill chain provides an end-to-end temporal sequence of different states in the overall scenario.

The kill chain tends to fall closer to the technical end of the spectrum in cybersecurity and is not as business-friendly as the CUBE framework. It is, however, extremely useful in understanding the diminishing probabilities of success as you move down the kill chain, where each subsequent step in the attack process poses a challenge to the attackers that not only depends on the motivation and capability of attackers but also the security controls that exist within the target(s).

CONCLUSION

The relative importance of each of these frameworks is context dependent. If you are trying to model the frequency and severity of scenarios as an actuary or a data scientist, you will find the kill chain much more similar to your toolkit of techniques, but if you are a portfolio manager or a business stakeholder within an insurer, you are likely better served by the CUBE framework which transforms layers of complex cybersecurity concepts into simplified "snackable" content. ♦

Ashwin Kashyap is a San Francisco-based Director, Product Management at Symantec Corporation. **Julia Chu** is a New York-based Managing Director at Guy Carpenter, where she focuses on Global Strategic Advisory.

EVOLVING CHALLENGES IN CYBER RISK MANAGEMENT

PROTECTING ASSETS AND OPTIMIZING EXPENDITURES

Richard Smith-Bingham

D espite the recent surge in cyberattacks, companies should accept that the coming years will most likely bring an even greater rise in criminal activity. These cyber crimes will become manifest for a wider range of targets, with constantly shifting attack vectors and more sophisticated execution. Advantage will continue to lie with the "offense" rather than the "defense" due to technological innovation and the challenges associated with attributing attacks, accessing perpetrators, and appropriately punishing them. No company will be below the radar, no company will be safe.

THE CYBER THREAT LANDSCAPE IS BECOMING MORE COMPLEX…

The agenda of cyber criminals will extend far beyond simple data theft, as attackers continually re-evaluate the most rewarding and least risky ways of deploying their capabilities for strategic and financial advantage – either their own or that of their backers. Security threats will impact not just the safety of corporate and customer data, but also the resilience of product innovation, corporate strategy, physical operations, and supply chains.

Two points of evidence stand out. First, the dark net is increasingly awash with commoditized attack vectors and payloads that enable opportunistic criminals to infiltrate companies with outdated defenses and weak capacities for detecting an incursion. This library of attack tools is lowering the bar for cyber criminals. Second, highly sophisticated, multimodal strikes targeted at specific corporate assets are becoming more common, with a rise in attacks that involve multiple phases of action and layers of deception to conceal both incursion and exfiltration.

While large-scale data breaches and Distributed Denial-of-Service (DDoS) attacks, will no doubt continue to occur in large numbers in 2016 and beyond, other types of incidents will probably rise in significance: corporate extortion hacks (threats t o release customer or company data to the world if certain demands are not met); intellectual property theft (for use by a competitor); and data sabotage (where digital data is manipulated to compromise its integrity, thereby causing high levels of uncertainty).

Over time, we should also expect more cyberattacks that carry physical consequences, as hackers find a stronger rationale for undermining industrial control systems and exploiting the growing Internet of Things (IoT). Vulnerabilities to these attacks have certainly been demonstrated (such as the successful penetration of the Ukrainian power system and multiple hacks of connected cars), and this likely presages further incursions to come.

Any single attack may have any combination of the above characteristics. Indeed, the growing scope for

contingent business interruption due to cyberattacks on third parties (such as supply-chain nodes or critical infrastructure) makes for a whole new set of risk considerations for companies.

BUT COMPANIES CAN INCREASINGLY OBTAIN A CLEARER PICTURE OF THEIR EXPOSURES…

Good situational awareness and cyber risk analytics are vital in helping firms identify weaknesses, rank threat scenarios, identify countermeasures, and set priorities for intelligence gathering.

Too few companies have properly documented their core information technology assets – their databases, intellectual property, or computing resources, for example. Without this information, it is hard to form a firm view on critical dependencies within the network for short- and long-term business success. A review of assets may also reveal parts of the network that are adding limited commercial value but giving rise to significant cyber risk.

Building on this, it is important to adopt the perspective of likely adversaries: What might they want, and why? How sophisticated are they? Many will just want to steal easily tradable data or siphon off funds. Others may scent more niche value in intellectual property, such as confidential pricing data and innovation research, or early intelligence on strategy direction, acquisition targets, decisive legal disputes, or pivotal regulatory negotiations. A third group may want to cripple operations, either because they have an aversion to the company or to fulfill more strategic, if obscure, objectives.

Clarity on the company's assets and the possible ambitions of intelligent, adaptive adversaries helps focus analysis into where the firm might be exposed and the potential cost of that vulnerability. Establishing how easy it is to penetrate a company system – through its web presence, stolen mobile devices and emails via firewall breaches, encryption failures, the exploitation of privileged accounts, and general

network porosity – provides insight into how badly it might be compromised.

Understanding the scope of the threat is vital, but robust risk quantification is also essential for communicating risk, prioritizing security safeguards, and allocating resources. For too many companies, this currently means little more than a heat map representation of potential damage, which is often misleading, as it combines frequent small losses with rare large losses for each type of incident in the form of a single expectation of likelihood and impact.

A more reliable and functional approach is to build distributions, or risk curves, from whatever company-specific and industrywide incident data is available by means of a Monte Carlo simulation. This has a number of benefits. It helps companies understand the range of outcomes and associated costs for each attack vector on a probabilistic basis. Application across attack vectors makes it possible to compare the different cost profiles and to determine which are causing the most losses overall. It may transpire that attack vectors that are low on the C-suite radar are in fact more troublesome than those that are of high concern. Moreover, the ability to adjust cost and incidence assumptions in a transparent way gives risk managers the opportunity to future-proof analyses in the light of current known trends.

Not only can this type of modeling properly compare attack vectors on a like-for-like basis, it can also support the aggregation of all cyber risks to quantify impact at an identified level of confidence. This provides an analytical foundation for considering the acceptability of cyber risk levels for the firm and discussing the value of risk transfer and mitigation investments.

Scenario analyses can be deployed using the same modeling technique to examine extreme events and emerging threats for which little data is available and where "what if" type thinking is required to explore second- and third-order consequences, such as reputational impacts.

ENABLING INVESTMENT DECISIONS THAT BETTER BALANCE SECURITY AND COMMERCIAL NEEDS...

Concern has risen among senior management and boards that higher budgets for cybersecurity are not necessarily delivering better corporate resilience in either the short or the long term. As cyber risk and

SOLUTIONS ARE IMPERFECT, RESOURCES ARE FINITE, INSURANCE CAPACITY REMAINS LIMITED, AND THE THREAT ENVIRONMENT IS CHANGING

associated expenditures are more visible at the senior level, the situation is no longer sustainable.

The analytics referred to above offer a platform for assessing the value of different security safeguards. If, for example, it is clear that a certain countermeasure will impede the ability of an adversary to move through a network to find assets of interest, it should be possible to compare the cost of that intervention against the amount of risk that is reduced, and therefore against alternative expenditure options. In conducting such an analysis, it is important to assess whether there are any material second-order costs, such as constraints on commercial activity.

Likewise, and where appropriate, companies should bring cyber risk into the assessment of new commercial ventures, along with the consideration of other risks. If expected returns, taking into account mitigation costs, insurance premiums, and residual risk do not meet the hurdle rate, approval of the investment may not be justifiable.

Indeed, with cyber risk now presenting as a critical and expensive business risk rather than merely as a technological irritant, security efforts should be considered both in a strategic manner and on a risk-return basis. Solutions are imperfect, resources are finite, insurance capacity remains limited, and the threat environment is changing. Resilience options need to be prioritized with the right level of senior oversight and endorsement. It may be the case that firms have to accept a higher level of cyber risk if mitigation and transfer opportunities are limited or unaffordable.

Technologically, companies should at first aim to close vulnerabilities by putting current best practices in place. This can be achieved by compartmentalizing the network and instituting key security controls such as full disk encryption, whitelisting certain software, careful network monitoring, strong authentication, routine incident logging, and periodic forensics. Strengthening corporate risk culture with regard to cybersecurity is also critical. Personnel should be encouraged to feel both more accountable and more

empowered, actively supporting company efforts by adhering to company policy and also reporting suspicious website and email activity – without being blamed for flagging their own failures in meeting recommended security standards.

But just as technological barriers can often be penetrated by the most determined and sophisticated attackers, so human error is inevitable in the face of sustained attempts at deception. More importantly, a balance needs to be struck between short-term needs and long-term requirements – between pragmatic fixes and strategic solutions. Likewise, tradeoffs between security and business objectives are inevitable, which may also clash with expectations that personnel have of the company's IT infrastructure. The necessary outcome (at least in the short term) may be sub-optimal capabilities, slower product and service development, and more restricted network access.

ALIGNING THE ORGANIZATION EFFECTIVELY AND SATISFYING GOVERNANCE CONCERNS

Better ex-ante justification of security investments may be the top priority, but ex-post monitoring is of increasing interest to support future decision making. Metrics and data that can show progress over time with regards to both incidents and their handling will be increasingly demanded by senior management

and the board. Boards are gradually becoming more familiar with cyber issues, through greater prominence of the topic on meeting agenda and the recruitment of members with appropriate expertise. Gone are the days when IT could do its job largely unchecked by the C-suite and subject to minimal reporting requirements on operational issues. Transparency and effectiveness are now the order of the day.

CONCLUSION

As a result, these principles are informing governance beyond the individual company. It is almost ironic, given the nature of cyber crime, that information sharing – with company leaders, other companies, insurers, and governments – is increasingly central to the development of cyber resilience. But a maturing dialogue is helping in a number of ways. Through it, companies can better understand how to allocate resources and identify risk transfer opportunities; insurers can provide greater coverage and protect themselves against accumulation risk; and governments can target policy efforts and strategic support more productively. ♦

Richard Smith-Bingham is a London-based Director at the Marsh and McLennan Companies Global Risk Center.

This article is based on an October 2015 expert workshop hosted by Marsh & McLennan Companies' Global Risk Center, Oliver Wyman, and the International Risk Governance Council. For the full report and more detailed observations, please visit www.marsh.com

MAKING THE MOST OF AVAILABLE INTELLIGENCE

Good data is certainly a challenge, but more information is available than ever before for careful use. Multiple reports and articles from the security industry and governments record attack trends, prevailing forms of malware, average corporate expenditures, and incident costs. Insurers and brokers sometimes publish data based on trends in claims. Informal peer group networks in more cyber-mature industries shed light on emerging cyber threats in a noncompetitive way, as do industry-government forums. Individual security experts have compelling anecdotes based on disguised client experiences. The dark web is a valuable,

if underused, resource for understanding criminal agenda and the price of traded items and activities.

Admittedly, all this intelligence needs to be calibrated. Some of it is overstated, partial, or hard to access. Well-publicized attack vectors (such as customer data breaches) are not necessarily the most prevalent risk for a company, or the most damaging. Many mundane attacks are never reported, and rarely can one read articles about extortion attempts and critical infrastructure breaches, where there are vested interests in concealment.

The most cyber-mature companies

are already mining their own data to understand what is driving the most risk. A well setup cyber incident log linked to cost data can be the foundation for identifying the prevalence of attack vectors and the range of impacts from each. Tracking provides a lagging indicator of key threats and known tail events, and how overall incident numbers and costs have varied over time. While valuable, this historic data does not, of course, represent the full scope of attack types and possible damage in a constantly evolving threat landscape.

CAN YOU PUT A **DOLLAR AMOUNT** ON YOUR COMPANY'S CYBER RISK?

Leslie Chacko, Evan Sekeris and Claus Herbolzheimer

Cyber breaches are one of the most likely and most expensive threats to corporations. Yet few companies can quantify just how great their cyber risk exposure truly is, preventing them from effectively protecting themselves.

Most managers rely on qualitative guidance from "heat maps" that describe their vulnerability as "low" or "high" based on vague estimates that lump together frequent small losses and rare large losses. But this approach doesn't help managers understand if they have a $10 million problem or a $100 million one, let alone whether they should invest in malware defenses or email protection. As a result, companies continue to misjudge which cybersecurity capabilities they should

prioritize and often obtain insufficient cybersecurity insurance protection.

No institution has the resources to completely eliminate cyber risks. That means helping businesses to make the right strategic choices regarding which threats to mitigate is all the more important. But right now, these decisions are made based on an incomplete understanding of the cost of the various vulnerabilities. Organizations often fail to take into account all of the possible repercussions, and have a weak grasp of how the investments in controls will decrease the probability of a threat. It's often unclear whether they are stopping a threat or just decreasing its probability – and if so, by how much?

It's essential that companies develop the capability to quantify their cyber risk exposure in order to form strategies to mitigate that risk. The question is, is it really possible to put a dollar sign on fast-changing cyber risks with data that is difficult to find and often even harder to interpret?

Estimating the true cost of a potential cyber breach may never become an exact science. The good news is that our understanding of why cyber risk forecasts keep falling short is improving. The main culprit is that companies quantify cyber risks the same way they do other operational risks – focusing narrowly on potential direct revenue losses. But companies can make much more accurate forecasts if they evaluate cyber risks on a broader set of losses associated with cyberattacks.

Companies come much closer to properly weighing how much they should spend to reduce their cyber risk and curb cybercrime when they consider these risks from three perspectives – foregone revenue and ancillary payments, liability losses, and reputational damage. One reason for this is that they are able to capture one of the biggest differences between cyber threats and other risks to their business: Cyberattacks can hurt a company even if there is no gain for the perpetrator other than accessing sensitive information.

The direct revenue losses for the companies involved in a cyberattack can be nearly negligible compared to the reputational damage incurred, which in turn can lead to future revenue losses. That is why it is essential for managers to quantify

cyber risks more broadly. It can be done, and can potentially save companies hundreds of billions of dollars every year.

The first step in putting a dollar figure on cyber risks is to identify your company's most important assets and its greatest vulnerabilities. Cyber risks generally fall into two categories: 1) those involving services shutting down, and 2) those that compromise information, ranging from sensitive data, to corporate secrets, to bank accounts.

But assumptions differ greatly depending on a business and its customers. For example, a utility company's greatest cyber risk could be a nuclear plant outage while a health insurer's top cyber risk may be losing medical data or having a hacker unexpectedly cripple critical surgical equipment. For another business, the greatest cyber risk could be the abrupt inability to bill customers, or perhaps, in the case of a bank, a shutdown that prevents customers from getting paid.

The challenge then is to build a smart, well-designed, cyber risk model that's able to analyze potential direct revenue, liability, and brand loss scenarios. For when a cyberattack happens, companies are hit not just with losses resulting from customers who stop buying products and services; they also face ancillary costs related to fixing their problem, such as regulatory fines, forensics, and consulting costs.

Liability losses, too, come into play in cases where critical data is accessed. A company may need to provide customers years of remediation, such as offering credit monitoring services, along with legal fees and penalties to settle multiple class action lawsuits. Finally, companies must quantify how much their future revenues will fall if a cyberattack has damaged their brand.

To understand the upper and lower boundaries of their risk, companies must gather general business, operational, and technical data that can be modeled against expected and worst case scenarios. Using both internal and external data related to the health of their business and operations, managers should be able to predict their expected and maximum cyber losses over a one- to three-year period, just as they can forecast their future revenues. They can also estimate what percentage of their future

customers will leave if an outage results from a cyber breach – or how much their stock valuation and margins could suffer if a cyberattack taints their reputation. Companies should also judge, in part from past incidents, which applications are at the highest risk.

Armed with this information, it's much easier for managers to judge if their companies have the right level of cyber risk protection and to budget for potential additional spending. Answers to questions like how much the company should invest in evaluating the state of their vendors' cybersecurity become much clearer. Or at what cost more authentication software is appropriate given the likelihood that critical data will be accessed.

Managers can also weigh if they should invest in more training of employees and vendors or in more technical controls to monitor potential cyber breaches. In some cases, managers may even discover that investing in a new product line may, or may not, be worthwhile given the cyber risks involved.

Quantifying cyber risks is challenging, but feasible – and you can't afford not to do it. Most firms have the technical knowhow and a strong enough grasp of the risks involved to help managers evaluate the trade-offs involved in mitigating cyber risks with a much smaller margin for error than in the past. What's needed now is leadership from managers to prioritize the need to gain a better understanding of how much they need to spend to curb their cyber risks and to put a halt to cybercrime. ♦

Leslie Chacko is a San Francisco-based principal in Oliver Wyman's Digital and Strategic IT practices; **Evan Sekeris** is a Washington DC-based partner in Oliver Wyman's Financial Services practice; and **Claus Herbolzheimer** is a Berlin-based partner in Oliver Wyman's Digital and Strategic IT practices.

WHY MODELING IS THE **HOLY GRAIL** OF CYBER INSURANCE

Robert Parisi

Are you able to quantify the threat of cyber risks to your business? What about quantifying and managing systemic risk? Put those questions to a group of insurers, underwriters, reinsurers, and data/analytics professionals and you'll get a wide range of answers. But the one thing everyone agrees on is:We need more modeling.

MODELING CAPABILITIES THAT DETERMINE CYBER LOSSES ARE INCREASINGLY SOUGHT AFTER BY INSUREDS, UNDERWRITERS, AND BROKERS

CYBER MODELING BUILDS UNDERSTANDING

Modeling capabilities that determine cyber losses are increasingly sought after by insureds, underwriters, and brokers. The cyber insurance market does not have the actuarial data that other product lines do, which is why we are often left in a quandary over how to get the information. To fill the gap, we have collected data from thousands of data breaches in order to build the Marsh Cyber IDEAL (identify damages, evaluate, and assess limits) predictive frequency and severity model.

Predicting losses can better arm you against cyber attacks. For example, the IDEAL model uses data from past events to estimate the costs of future events. A company holding two million payment card records (PCI) could see a one in 100 occurrence breach event that costs $21 million. Even if your organization has half that exposure, it's a significant loss. Why is modeling in the cyber insurance market so important? Generally speaking,it helps to:

- Price cyber insurance
- Evaluate claims loss data
- Understand cyber risk
- Enable the market to be more resilient in the face of dynamic cyber threats by predicting losses
- Apply modeling techniques pioneered in the natural disaster space to cyber
- Match predictive scenarios with the appropriate cyber coverages, which can help you determine if you will be paid forcyber losses

MODELING CHALLENGES

Modeling, however, can be challenging because the way that information is valued in the cyber insurance industry is constantly changing. For example, some models take cyber operational risks and scenario solutions into consideration. That's fine for organizations that might suffer large losses if, say, a website were to go down. But what about those companies that wouldn't be as affected by such an event?

And then there are different ways to build the models. Some threat models are developed based on value-at-risk analysis or another measure.

The coding of premiums is another issue; and improved coding could enhance cyber loss modeling. Currently, it is often difficult to predict the losses involved due to uncertainty over the premium allocation.

CONCLUSION

The good news is that brokers, insurers, and analytics companies are deep in the process of quantifying cyber risk. Models now can even pinpoint a company and an industry's potential breach exposure, which can provide assurance to senior management and the board.

Though it will take more time as an industry to aggregate additional data, the benefits of cyber risk modeling are clear. ♦

Robert Parisi, based in New York, is Managing Director and the National Practice Leader, Cyber, Marsh.

CYBER LOSS **EXPOSURE**

IDENTIFICATION AND DEVELOPMENT OF UNDERWRITING INFORMATION

Chris Beh

Although still considered an emerging risk, the awareness around cyber and cyber risk management is growing at a rapid pace. As this awareness grows and cyber risks become a common part of management-speak and boardroom talk, so has the awareness of cyber insurance as an avenue to fund losses associated with these risks. Purchases of cyber insurance across industry sectors and company sizes are growing. The US leads the market, but a 2016 Marsh UK Cyber survey showed about 20 percent of respondents had purchased cyber insurance and another third were considering purchases. A similar 2016 Marsh survey found about 25 percent of the responding European companies had cyber insurance.

As interest in cyber insurance grows, many companies have questions. Firstly, the insurance buyer may be unaware of the details their insurance policy, how it would respond in the event of a loss, and what its limitations and exclusions might be. Purchasing decisions may be driven by price and some form of insurance benchmarking – such as determination of the cyber program, limit and excess appropriate for the particular type of industry, and size and turnover of the organization based on past cyber insurance purchases. Secondly, the cyber insurance carrier market is still evolving and maturing. Insurers' proposal forms are being refreshed as their understanding of cyber risk improves or as technologies develop such

THE EFFECTIVE PURCHASE OF CYBER INSURANCE AND THE RIGHT COVERAGE SELECTION DEPENDS ON A CLEAR UNDERSTANDING OF THE ORGANIZATION'S CYBER RISK EXPOSURES

as Cloud services (from data management to software to infrastructure) or Bring-Your-Own-Device (BYOD) practices.

These proposal forms might be complicated for insurance purchasers or insurance brokers to complete – or else may be so brief that key underwriting information is missed. Furthermore, for larger organizations that operate in a multitude of jurisdictions or have several subsidiary companies, or organizations with complicated reporting, service, or organizational structures, the insurance proposal form may not accommodate an appropriate description of the nature and quality of the risk to be underwritten; additionally, the questions asked may not be of sufficient detail to fairly rate the quality of the risk.

The effective purchase of cyber insurance and the right coverage selection depends on a clear understanding of the organization's cyber risk exposures. A structured and risk-based approach

EXHIBIT 1: A STRUCTURED AND RISK-BASED APPROACH TO ASSESS CYBER EXPOSURES

UNDERSTAND YOUR POTENTIAL AREAS OF RISK	UNDERTAKE A RISK ASSESSMENT	RISK TRANSFER AND LOSS FUNDING OPTIONS	DEVELOPING UNDERWRITING INFORMATION

• Consider organization's internal and external business environment
• Examine current systems, practices and controls for monitoring, reporting and response, with regards to cyber-related risks
• Articulate organization's cyber risk appetite
  – Use risk consequence criteria/levels of impact
	• Include a variety of personnel across business, including:
	  – Key business assets and critical information systems
	  – Information system/security, legal and risk personnel
	• For each cyber loss exposure considered, identify potential scenarios of threat sources and risk drivers
	• Assess effectiveness of current controls and practices in place to manage each threat source and risk driver
		• For identified threat sources and risk drivers, confirm available contractual risk transfer and loss funding options
		• Undertake analysis of expected first- and third-party insurance policy response to each risk event/scenario
		• Enlist help from organization's insurance broker as needed
		• For non-insurance key risk events:
		  – Review vulnerabilities they cause
		  – Develop strategies and initiatives to improve systems and controls
			• Provide information amassed during previous steps to the insurance market. This will help:
			  – Cyber insurance market underwrite on an informed basis
			  – Organization's insurance broker negotiate best available cyber insurance policy cover, limits, pricing and terms

Source: Marsh Analytics

to assess cyber exposures allows an organization to understand the potential level of impact that these exposures could have and provide the information that would assist insurers to underwrite these risks on an informed and competitive basis.

UNDERSTAND YOUR POTENTIAL AREAS OF RISK

Establishment of the risk context is fundamental to performing a risk assessment and includes considering your organization's internal and external business environment. This involves articulating your principle lines of business, organizational objectives, and core business activities, as well as identifying the key areas of challenge for achieving growth, profitability, and other strategic goals. Along with this, you should identify its key business assets and critical information system assets that achievement of these goals would depend on.

The next step is to examine the current systems, practices, and controls for monitoring, reporting, and response with regards to cyber-related risks, including the associated cyber and information security processes. As a product of this review, the key organizational level cyber risks should become apparent and the significant cyber loss exposures be identified. Examples of cyber loss exposures include: failure of critical information technology infrastructure; system breach; critical data loss; extended service delivery failure; breach/failure of a Cloud provider; and failure of an outsourced service provider.

Context setting would also include articulating your organization's risk tolerance (or risk appetite) in the form of risk consequence criteria (or levels of impact) characterized as "strategically acute risks" (sometimes termed catastrophic, fundamental, severe, or very high risks) and "strategically chronic risks" (termed as major, significant, or high risks in some definitions). Risk consequence criteria can be considered under types of impact, such as financial/fiscal/investment (for example, revenue, EBIT, gross profit, asset value); reputation (media attention, brand damage); regulatory compliance; business interruption or service delivery; and strategies or strategic/competitive advantage.

PROVIDING WELL-CONSIDERED AND CONSOLIDATED INFORMATION TO THE INSURANCE MARKET PROVIDES ASSURANCE FOR THE UNDERWRITERS THAT POTENTIAL CYBER RISKS ARE IDENTIFIED, UNDERSTOOD, AND MANAGED

UNDERTAKE A RISK ASSESSMENT

A robust risk assessment process will include a variety of personnel across the business involved with the previously identified key business assets and critical information systems, as well as information system/security, legal, and risk personnel. For each cyber loss exposure considered, the risk assessment team would identify the possible/potential scenarios of threat sources and risk drivers that would cause strategically acute or strategically chronic impact in relation to the key business assets and/or critical information systems.

For example, the cyber loss exposure event of failure of critical information technology infrastructure could be due to aging infrastructure or failure of temperature monitoring/control; or for a system breach, the scenario might arise from a crypto virus compromising the network via a remotely connected staff device or equally caused by a disgruntled employee deliberately importing a virus.

The team would then review the current controls and practices in place to manage each threat source and risk driver and qualitatively rate the effectiveness of their controls. This would assist the organization in understanding the potential gaps in the control practices. Also, to further help prioritize the threat or risk event, it is suggested that the likelihood or relevance of the event be qualitatively and where possible, quantitatively, assessed.

RISK TRANSFER AND LOSS FUNDING OPTIONS

For each threat source and risk driver identified during the risk assessment process, the organization could then confirm what contractual risk transfer and loss

funding options it currently has available, including the insurance policies that it currently has in place. In order to improve its management of risk and improved understanding of its loss funding options, an analysis of the expected first- and third-party insurance policy response to each risk event/scenario could be undertaken. Your insurance broker could also assist with the identification of these gaps and further assist with understanding how a tailored cyber insurance policy might respond to mitigate these financial losses if these were to occur.

It should be noted that potentially not all key risk events identified will be insurable. Some, such as certain contractual failures/issues causing supply chain and service delivery failures or failure in aging hardware or network componentry, may not be fully insurable, if insurable at all. In this case, the firm could review its vulnerabilities caused by these events and develop strategies and initiatives to improve their systems and controls.

DEVELOPING UNDERWRITING INFORMATION

In going through the previous stages, the organization should have amassed a rich source of documented information that it could compile as part of its submission to the insurance market when negotiating cyber insurance policy cover, limits, pricing, and terms – should it wish to purchase a cyber insurance policy appropriate to its risk appetite and risk profile.

Providing well-considered and consolidated information to the insurance market provides assurance for the underwriters that potential cyber risks are identified, understood, and managed; and provides transparency and improved risk perception for insurers. It ultimately assists the cyber insurance market to underwrite on an informed basis and allows the organization's insurance broker to negotiate best available cyber insurance policy cover, limits, pricing, and terms. Relevant underwriting information would include:

- Background to the organization, its principle lines of business, organizational objectives, and core business activities
- How risk management is implemented in the organization including governance, framework, communication of risk management, and in particular training and awareness around cyber and information security practices
- The controls and practices established such as asset management, business continuity, cyber and information security policies, and procedures and risk register processes
- Its key cyber assets
- The cyber and information technology infrastructure, including any particular site (risk) features
- Key dependency risks
- Outputs of a risk assessment – as discussed above or other cyber and information security audits or assessments

CONCLUSION

By undertaking a structured and risk-based approach to understanding the nature of its cyber risk exposures and associated cyber and information security and risk management processes, the key potential loss exposures that an organization might potentially face can be established. Some of the risk drivers and causal events for the exposures may be insurable and a review of the risk transfer and loss-funding options for the risk components can be undertaken. Lastly, the information gathered from the risk assessment process can be utilized as information for the insurance market to enable insurers to underwrite cyber insurance policies on an informed basis, and allow insurance brokers to negotiate best available cyber insurance policy cover, limits, pricing, and terms. ♦

Chris Beh is a Principal for Marsh Risk Consulting in New Zealand.
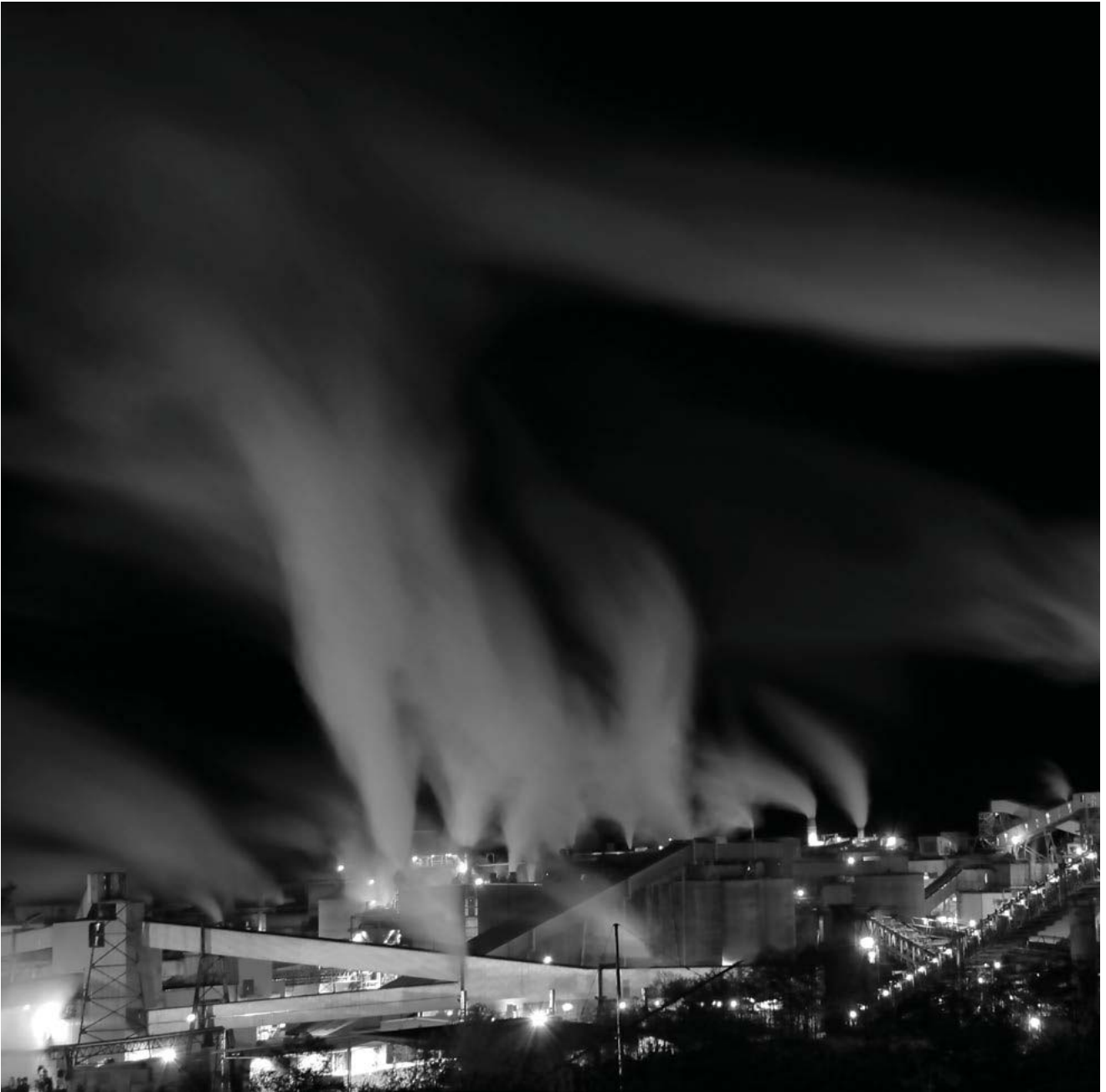
THE INSURANCE OF THINGS AND INDUSTRY 4.0

A MATRIX VIEW

Morley Speed

Technological progress and the accumulation of assets have not only stimulated the development of insurance products; they have in turn been nurtured by the availability of these offerings.

It is no coincidence that the origins of insurance lie in the marine class, where the financing of ships and trade is among the earliest examples of investment in technology and assets. Successive waves of technological progress have stimulated the development of corresponding insurance specialties – not just products, but also riskmanagement. These new "things of value" may have provided some challenges, but ultimately the (re)insurance industry has provided for the "Insurance of Things".

Today, the (re)insurance industry faces its greatest technological challenge yet. Can the Insurance of Things develop to insure the so-called "Industrial Internet of Things"?

We are experiencing a fourth industrial revolution, based on the "Internet of Things" combined with interconnected machines and people. This Industrial Internet of Things is also known as the "The Smart Factory", or simply "Industry 4.0".

According to the CRO Forum: "This new mode of production is characterized by the merger of the material and virtual worlds in 'cyber-physical production systems'."[1]

Cyber is now a much-reported topic and is usually classified between "affirmative cover" within specific cyber policies (up to now, largely concerned with data breach) and "silent" cover, which is essentially the first-party losses arising from cyber perils within mainstream P&C lines, predominantly property damage and business interruption (BI).

This so-called "silent" exposure is the subject of the Lloyd's "Business Blackout" scenario, which pointed to an ultimate potential insured loss of between $21.4 billion and $71.1 billion.[2]

This article examines coverage issues arising from Industry 4.0 first-party exposures. Fundamentally, it is about how the insurance industry is dealing with

1 The Smart Factory– Risk Management Perspectives – CRO Forum, November 2015.
2 "Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid," *Lloyd's Emerging Risks Report 2015.*

EXHIBIT1: DIRECT FIRST PARTY (NON BREACH) POLICY COVERAGE

PERIL	SUBJECT MATTER			
	Damage to...		Business interruption following...	
	A. Data assets	B. Physical assets	C. Physical damage	D. Non-physical damage
Cyber Tier 1				
1. Deliberate act	Covered (data)	Covered (data) + Covered (physical)	Covered (data) + Covered (physical)	Covered (data) + Covered (physical)
2. Accidental act	Covered (data)	Covered (data) + Covered (physical)	Covered (data) + Covered (physical)	Covered (data)
Cyber Tier 2 (following Cyber Tier 1)				
3. Damaged hardware	Covered (data) + Not covered (physical)	Covered (physical)	Covered (data) + Covered (physical)	—
4. Damaged software	Covered (data)	Covered (physical)	Covered (data) + Covered (physical)	Covered (data) + Not covered (physical)
5. Property	Covered (data) + Not covered (physical)	Covered (physical)	Covered (data) + Covered (physical)	—

COVERED

NOT COVERED
Although there may be an element of coverage or coverage is ambiguous

Source: Guy Carpenter

the merger of the material and virtual worlds. It does not address first-party data breach issues.

Broadly speaking, the material world is covered by the property line and the virtual world by the cyber line. However, the demarcation is not absolutely clear, resulting in some overlaps in coverage but also, more worryingly, some gaps.

The matrix (Exhibit 1) shows how the four types of subject matter (columns A-D) are generally covered by direct policies, relative to the various types of cyber and property perils (rows 1-5). Where cover is predominantly provided by property or cyber, the relevant icon is shown in blue. Where there is a degree of ambiguity, or coverage is limited, the icon is shown in gray. Clearly, this is a schematic simplification, but generally it would appear that coverage is fairly clearly assigned in columns A, B and C, as follows:

A. Predominantly in the virtual world and covered by cyber

B. Falls within the province of property

C. Naturally follows B, as this is for BI following B

The instances outlined in column D capture the complexities, particularly with respect to property.

BUSINESS INTERRUPTION FOLLOWING NONPHYSICAL DAMAGE

Column D outlines the areas in which cyber insurance would be expected to operate. However, to date, the cover has focused on data breaches rather than BI arising from disruption of industrial control systems.

The reliance of the industrial and commercial sectors on cyber technology, most notably in the context of Industry 4.0, suggests this is an area of significant opportunity for (re)insurers.

Although cyber would seem to be the logical destination for this exposure, there is the severe practical difficulty of monetary capacity. There are very few cyber limits above $500 million, whereas this is not an exceptional figure for corporate property.

As a consequence, nonphysical damage BI is finding its way into property policies, although it is recognized as generally being for sub-limits well below $500 million. However, even a sub-limit of $50 million

would represent a significant cyber limit and would certainly require significantly more underwriting information, and probably premium as well.

However, property cover is usually restricted to targeted malicious cyber attacks, whereas a cyber policy would give much broader cover for disruption of control systems.

The key strategic question is: Where will non-physical damage BI end up – within cyber or property?

To a large extent the answer will depend on reinsurers' risk appetite and requirements to control cyber exposures, particularly aggregation. However, it will also involve a realization by property underwriters that original clients buying BI cover do not necessarily make the distinction between the material and the virtual worlds.

CONCLUSION

In response to this exciting challenge, Guy Carpenter has established a joint initiative with Symantec, combining relevant and credible data with both traditional modelling approaches and innovative ones, such as application of the cyber "Kill-Chain" methodology.

It remains to be seen how the (re)insurance industry will align its capacity for Industry 4.0, but it is already clear that there will be increasing and sustained demand for such capacity in the future ◆

Morley Speed is a Managing Director in Guy Carpenter's London office

PEOPLE

STAFFING FOR CYBER RISK MITIGATION

THE BUSINESS CHALLENGE

Katherine Jones, PhD, and Karen Shellenback

With the growing recognition of the cost of cyber attacks, corporations are seeking the talent they need to better address the increasing risk to their data and organizations. Originally housed within the IT function for the most part, new Mercer Select Intelligence research reveals the increase in cyber risk positions within departments devoted to risk prevention and mitigation.

Organizations face three challenges related to cyber talent: Who is responsible for risk mitigation today; what skills corporations are seeking to staff this growing talent need; and what steps employers are taking to keep the talent they have today.

Give the enormity of the potential risk and its impact on lost business (Lloyds of London estimated that cyber attacks are costing businesses $400 billion in total[1]), far too many companies are strangely complacent. Only slightly more than half (53 percent) of the respondents in a 2016 Mercer Select Intelligence global survey reported that their organizations viewed cybersecurity as imperative across the entire organization.[2] While the majority of respondents felt that they were organized to meet the tasks and challenges ahead and were already sourced to build a flexible staffing model with the right mix of staff, consultants, and contractors, far fewer (47 percent) felt they were adequately resourced in terms of talent to meet tomorrow's challenges.

WHO OWNS CYBER RISK MITIGATION?

Traditionally, responsibility for computer-related security rested in the IT department, especially for those companies that have maintained a designated cybersecurity function for more than 10 years. For many organizations, we see a shift to departments of risk management for cyber responsibility. While this is a growing trend and development, it is less than a half decade old. (See Exhibit 1.) This may speak to one of several tendencies:

- An increase in organizational functions specific to risk management
- A growing trend to house cybersecurity within the overall corporate strategic risk function rather than in IT
- The growing focus of cyber risk management as a C-suite strategic risk issue

Interestingly, 21 percent of those responding organizations in which cybersecurity responsibility is housed in the IT function viewed it as a crucial priority *inside* IT but not as a priority within the business units or at higher levels of management. This contrasts significantly with those organizations that housed cybersecurity within a Risk Management department, for which not one respondent thought that cyber concerns were limited to his or her department. This finding showcases the overall shift in perspectives on cyber attacks as a strategic risk management function rather than solely an IT charter.

STAFFING CYBERSECURITY INITIATIVES IN THE FACE OF TALENT SCARCITY

The majority of companies (86 percent) indicated intent to increase spending on cybersecurity staffing within the next 12 months. Given the noted scarcity of cyber professionals, competition for talent is increasingly intense. Finding talent, training current employees, and retaining trained talent loom as major issues in this critical mission. The vast majority of companies surveyed

EXHIBIT 1: RESPONSIBILITY FOR CYBERSECURITY AND ITS DURATION
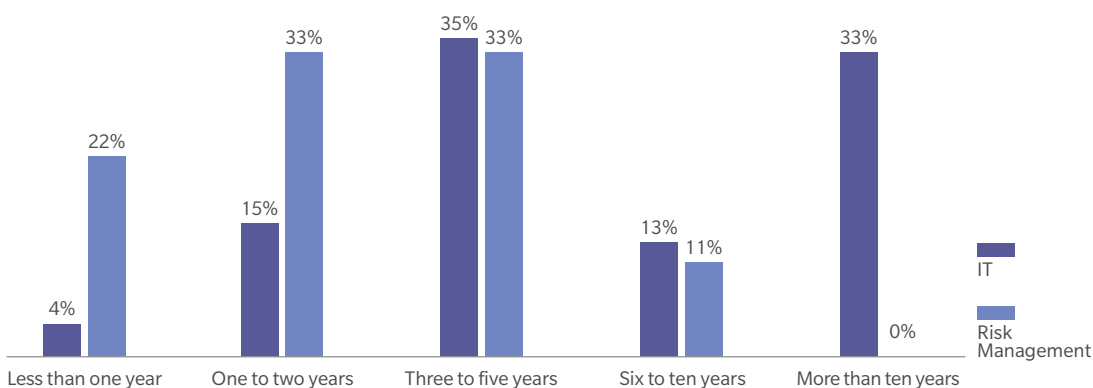
Source: Mercer Select Intelligence, 2016

1 Cyber Crime Costs Projected to Reach $2 Trillion by 2019. Steve Morgan. Forbes, Jan 17, 2016.
2 Proactive Prevention, Step I: Getting Cyber Staffing Right. Katherine Jones, Ph.D., Mercer Select Intelligence. 2016.

plan to increase the size of their cybersecurity teams over the course of the next two years, with 25 percent of those actively recruiting full-time employees today and another 25 percent activity recruiting part-time, contingent, or external vendors for support. While some organizations have no intent to expand (26 percent), none expect to contract.

CYBERSECURITY QUALIFICATIONS SOUGHT BY EMPLOYERS

Qualifications for cyber risk mitigation professionals and even initial entrants into related positions are stringent, with higher levels of education, experience, and certifications sought, whether the positions reside in a Risk Management division or within an IT department.

Education: Education varies with the position sought, with the majority requiring college levels of education, and top positions requiring advanced degrees. Fully 60-73 percent of respondents require a bachelor degree for all jobs and one-third of companies require a Masters for C-Suite positions (CISO, CSO, CTO, CIO).

Experience: Required years of experience sought are, in general, fairly high even among entry-level positions. Almost half of employers looking for cyber engineers, for example, require more than three years of related experience. Analysts appear to be better able to enter the job force in this field with one to two years of experience, though a quarter of respondents sought more than three years of experience for analyst positions.

SECURITY CERTIFICATION

As Risk Management and IT positions increase, so, too, does the desire for certified professional across the variety of cybersecurity job types. Some of the more common cyber positions are shown in the chart below, with the percentage of positions requiring that particular certification.

Some positions prefer multiple certifications; no positions for which employers are hiring require none at all. The Certified Information Systems Security Professional (CISSP) credential is the most generally sought certification over the widest range of positions, as this is the first credential in the field of information security to meet the stringent requirements of ISO/IEC Standard 17024.

THE CHALLENGE: FINDING TALENT WITH DESIRED QUALIFICATIONS

Given the extent of requirements for the positions open, predictably, these jobs are hard to fill. Almost one-half or respondents reported that filling cybersecurity positions was difficult or very difficult, and none responded that it was very easy.

Degrees of difficulty are of course dependent on the position and the level of qualifications: education, experience, and valid certifications sought. The analyst positions, for which one to two years of experience is sought, appears more difficult to fill than engineers with cyber or security experience, for which more

Certification Requirements per Position

	CISSP	CISA	SECURITY +	CISM	GIAC SECURITY ESSENTIALS	CIPP	SSCP	ISO 27001 LEAD AUDITOR
C-Suite or Director: CISO CSO, CIO, CTO, Global Information Security Director, etc.	76%	34%	21%	55%	21%	17%	14%	10%
Line of Business Officer: (Regional, division or functional) Information Security Officer, Cybersecurity Officer	83%	42%	42%	58%	13%	8%	21%	4%
Lead Engineer: Software Security or Security	73%	31%	54%	23%	35%	8%	19%	0%
Manager: Application Security	70%	35%	39%	26%	35%	4%	17%	4%
Analyst: Information Security, Security Operations, Risk/ Vulnerability, Network Security	68%	29%	46%	14%	39%	0%	14%	4%
Analyst: Threat Intelligence	68%	16%	36%	12%	44%	0%	8%	4%
Engineer: Cybersecurity or Security, Security Administration	74%	22%	41%	11%	37%	4%	11%	7%
Security Architect	76%	38%	41%	24%	45%	10%	17%	10%
Security Auditor	52%	57%	22%	22%	9%	4%	4%	26%

Source: Mercer Select Intelligence, 2016

than three years of experience was often required. Employers cite different reasons – external and internal – for this difficulty. The foremost reasons are the lack of experience and education in the market to fulfill cybersecurity roles especially at senior levels. Half of the respondents, however, view an internal failure to compensate at the market rate for such talent as the main reason they cannot attract the talent they need.

Time to fill cyber positions is often protracted: 23 percent of respondents reported they exceeded 120 days to fill positions at the C-Suite or Director level, entitled, for example, CISO CSO, CIO, CTO, or Global Information Security Director. One-fifth (21 percent) reported that they target the 75-plus market data percentile for base salary when recruiting for these cybersecurity positions. Filling a role as an Analyst of Information Security, Security Operations, Risk/ Vulnerability, or Network Security took between 61 and 90 days for 16 percent of respondents.

While the slight majority of companies do not treat security candidates any differently in the recruiting processes, some are offering incentives to try to lure this specialized population. Flexible schedules, location choices, hiring bonuses, and higher base salaries are the predominant methods used to attract candidates to these positions.

KEEPING EXISTING CYBER TALENT

Most of the companies in our survey clearly had an internal cyber pool; while they were seeking additional talent, were they worried about keeping the talent they already had? Twenty-seven percent reported it was difficult to do so; only 15 percent thought it was relatively easy to retain their talent. Retention issues stem from two highly sought after positions: the analyst of Information Security, Security Operations, Risk/Vulnerability, or Network Security; and security auditor. Both positions were identified by 23 percent of companies as the hardest to retain.

The primary reason for the loss of cyber talent was the lure of higher salaries elsewhere, as perceived by 73 percent of respondents. Concern for career-relevant skills and lack of a fast career path were the next elements that led to employee loss to competitors. (See Exhibit 2.)

Given this, the majority address the desire for training as a primary lure for retention. Many do nothing, similar to those who do nothing to attract

EXHIBIT 2: RESPONSIBILITY FOR CYBERSECURITY AND ITS DURATION

Recruited away using higher salaries and/or bonus structures
73%

Career path is not fast enough
53%

Our talent wants to learn new skills and then leverage that experience in a new environment
40%

Career path is not clear
33%

High burnout rates
20%

Jobs are boring, repetitive, tedious
20%

Not enough workplace flexibility
13%

Diversity and inclusion issues
7%
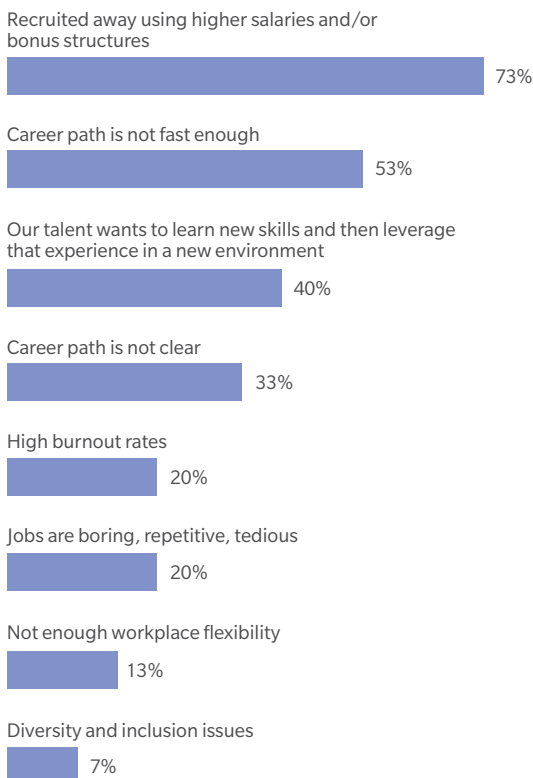
Source: Mercer Select Intelligence, 2016

candidates to their corporations. Combinations of flexible time and various bonus types are also used as retention devices.

CONCLUSION

Creating a sound basis for organizational cybersecurity starts from the top, but it does not end there. Based on this Mercer Select Intelligence research, the standard HR issues of sourcing, hiring, grooming, and retaining qualified staff clearly come in to play. Given the dearth of graduates from accredited programs specializing in data security, and the growing desire for personnel with related education, experience, and certification, talent to fill open positions is scarce. Companies may find themselves well-served in providing current staff with the education to achieve certified status, and then compensate them well enough to retain their newly trained talent from competitive offers. Maintaining a cyber risk mitigation environment is a race without a finish line – it is a threat that is not going to go away. ◆

Katherine Jones is a Partner in Mercer's San Francisco office, and serves as the Products and Insights Leader of Mercer Select Intelligence. **Karen Shellenback** is a Principal in Mercer's Denver office, in addition to being the Research and Insights Leader of Mercer Select Intelligence.

DON'T IGNORE THE
INSIDER CYBER THREAT

Basie von Solms

Company boards and CEOs are having sleepless nights thinking about the risk of cyber attacks and the impact such attacks can have on their companies. Some spectacular cyber breaches have occurred in the past few years, and many reports indicate that the risk of cyber attacks is increasing at an alarming rate. *The World Economic Forum's Global Risks 2015 Report* assigns cyber attacks a rating of 5 (on a scale of 1 to 7, with 7 being a likely risk with massive impact) when it comes to likelihood and impact.

Cyber attacks come in different forms and sizes, and cyber criminals have a wide range of attack vectors they are using to compromise a company's electronic assets.

One of these attack vectors that is easily overlooked is the so-called "insider threat." This refers to cyber attacks against the company originating with employees.

It is important to distinguish between external cyber attacks and insider cyber attacks. External cyber attacks originate from outside the company, but may target the employees of the company. Phishing –

specifically spear phishing attacks – is a well-used attack method. The targeted employee reacts and is caught by the attack mostly because of a lack of awareness and knowledge about such attacks. These employees do not originate the attack, but rather are the targets of the attacker. Often these attacks are categorized as insider cyber attacks, but that is not really correct.

Insider attacks originate from within the company, executed by a person who is in general authorized and trusted to access a company's electronic assets. The employee himself or herself is, "the threat originating from inside."

Insider threats are more difficult to counter and cannot be addressed by technology alone. A much more nontechnical and human-oriented defense approach is required. Securing a company against insider threats is a difficult process; very often, companies do not even take

REPORTS AND STATISTICS CLEARLY INDICATE THAT THE REAL INSIDER CYBER THREAT IS GROWING AND INCREASINGLY BECOMING A SERIOUS RISK

insider threats into account because they are focused on stopping external intruders.

Reports and statistics clearly indicate that the real insider cyber threat is growing and increasingly becoming a serious risk.

If we broadly define an insider as a permanent employee who has authorized access to a company's information systems and electronic assets, then we are already underestimating the risk. Insiders include anyone who has logical access to the company's electronic assets. This can include third-party contractors, visitors, and temporary employees.

The biggest insider risk is probably the disgruntled employee who, for whatever reason, deliberately decides to steal and compromise his or her company's electronic assets. Newer technologies make this so much easier: A single USB memory stick can contain a massive amount of information and is so small that the chance of preventing it from leaving the company premises is extremely unlikely. And if discovered, the employee can easily claim that he is taking it to work on the data at home.

The availability of personal cloud-based storage platforms makes it even easier to send data and information outside the company without physically having to possess it. In addition, the very popular bring-your-own-device approach is also a contributing factor when worrying about the insider threat.

COUNTERING THE INSIDER THREAT

Implementing fail-safe countermeasures to completely prevent insider threats is impossible. So what can be done to address this insider risk? What basic countermeasures can a company have in place?

It seems logical that the more a company can trust its employees, the less it has to worry about an employee "going rogue" and becoming an insider threat. A good way to start is to do as much as possible to manage an employee's complete employment cycle from pre-employment to employment termination.

The international standard ISO/IEC 27002, jointly published by the International Organization for Standardization and the International Electrotechnical Commission in 2013, is dedicated to specifying controls that can be implemented to create a secure information and cybersecurity environment. The standard consists of 14 security control clauses and 114 security controls. Control clause 7 on Human Resource Security (HRS) is specifically relevant to the aspect of insider threats. This

EXHIBIT 1: TOP BREACH RECORDS BY SOURCE

Malicious insider — 52%

Malicious outsider — 43%

Hacktivist — 4%

State sponsored — 1%

Accidental loss — 1%
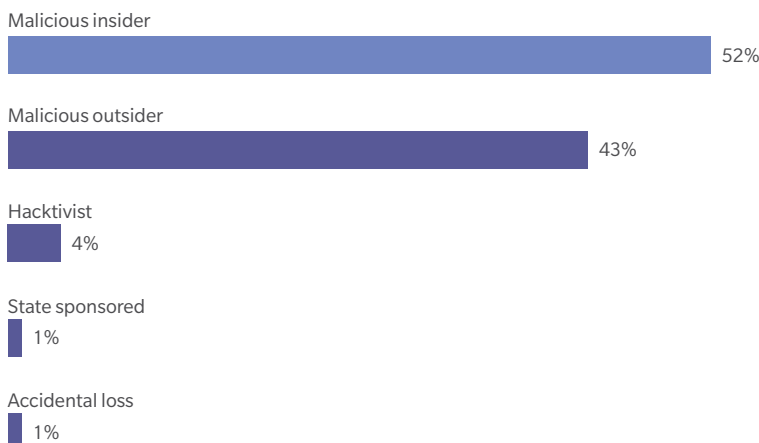
Source: Breach Level Index

clause covers HRS with respect to security controls, organized as follows:

- **Prior to employment:** Here, the aspect of pre-employment screening is emphasized and solid guidance is provided on what should be covered during the pre-employment phase.
- **During employment:** This phase includes security awareness, education, and training, as well as disciplinary actions for nonconformance to security and company policies.
- **Termination and change of employment:** Here, the important aspect of termination of logical access rights and related matters are covered.

Clear guidelines are provided on how to implement the suggested security controls specified in the clause.

Companies should study this ISO Standard – specifically clause 7 – in detail and implement the proposed security controls. This will go a long way to address aspects of insider threats.

CONCLUSION

This simple three-step approach will help any company address the potential of insider threats:

- Be aware of insider cyber threats as a significant cyber risk to the company and take them seriously.
- Although technical countermeasures do play a role, approach insider cyber threats from a nontechnical angle.
- Use the controls of clause 7 of ISO/IEC 27002 as the basis of the company's approach to insider threats. ♦

This article was published on *BRINK* on October 21, 2015. Brinknews.com is Marsh & McLennan Companies' global digital news hub providing perspectives on developing risk issues.

Professor SH (Basie) von Solms is a Research Professor in the Academy for Computer Science and Software Engineering and the Director of the Centre for Cyber Security at the University of Johannesburg in Johannesburg, South Africa.

A STRATEGIC APPROACH
TO CYBERSECURITY
OPERATIONS

Jim Holtzclaw and Tom Fuhrman

Any conversation about enterprise-wide cybersecurity today seems inevitably to turn into a conversation about technology. From perimeter protection to incident response, with vulnerability management, encryption, intrusion detection, data loss prevention, logging platforms, threat intelligence integration, and a host of others in between, technology is at the core of protecting networks, systems, and data from cyber attack. But in truth cybersecurity requires more than just implementing technology solutions. In the words of Walt Disney, it takes *people* to make the dream a reality.

The foremost challenge in cybersecurity operations today is the workforce challenge – recruiting, training, developing, mentoring, managing, and retaining the IT security professionals who make up the operations team. The issue is not only one of having too few cybersecurity-qualified people in the labor force: The management of the cybersecurity operations function within companies often does not receive the management priority it deserves. This problem needs attention in many enterprises. Failure to address it well can have a grave impact on the effectiveness of the security program.

The complexity and requirements of the entire cybersecurity operations function are formidable, but without enough well-trained, proficient, and well-managed operators, the promise of technology will remain just a dream.

CYBERSECURITY OPERATIONS: MAINSPRING OF THE PROGRAM

Cybersecurity operations consists of the day-to-day activities of implementing, configuring, tuning, managing, and monitoring security devices, and responding to the alerts they issue when a potential incident is detected. Operations differs from other enterprise cybersecurity roles in that operations people perform the hands-on work at keyboards, consoles, and equipment to implement and directly operate, manage, and monitor security devices. Operations is where "the rubber meets the road."

Several key factors make the cybersecurity operations workforce challenge both difficult and enduring, including:

- Cybersecurity operations is an arcane and inherently complex field requiring expertise in IT and IT security technologies, networking, system and network vulnerabilities, and an understanding

THE FOREMOST CHALLENGE IN CYBERSECURITY OPERATIONS TODAY IS THE WORKFORCE CHALLENGE

of the organization's IT and cybersecurity policies. Cybersecurity operators need expertise in how IT vulnerabilities are exploited, the tactics of hackers, how malicious payloads are delivered into networks, and a wide range of other technical security topics.

- The tempo of cybersecurity operations and the volume of data in the operational environment are high and require 24x7 attention (for example: traffic monitoring records, vulnerabilities, device images and configurations, user credential records, access control lists; security logging alone can generate many gigabytes per day for a midsize enterprise).
- Sophisticated threat actors continually advance their tradecraft, requiring defenders to do the same.
- There is a widespread shortage people in the labor force who possess the requisite experience, training, and qualifications to meet the demand. This gap became apparent in the 1990s as companies built dependence on the Internet into their business models, only recognizing later the criticality of cybersecurity. The gap has only widened since, as business needs have outpaced the ability of the society to produce enough qualified cybersecurity operators through education and job experience.

The cybersecurity operations workforce challenge has a direct bearing on the effectiveness of the overall cybersecurity program. To respond to the challenge, a four-part strategic approach is needed.

One: Structure the Workforce Strategically
Structuring the workforce strategically means identifying and aligning specific skills with well-defined needs. It means budgeting for personnel and planning for their professional development. And it means taking a long view of the company's cybersecurity operational needs in light of internal business and IT strategies and the evolution of technology and threats.

Define Roles: The first step for most companies is to define roles. Ideally this would be done comprehensively and with specificity. A good point of departure for many organizations is the tabula

rasa approach – begin with a clean slate and focus on identifying cybersecurity operations' needs, largely irrespective of the roles and skills of incumbent staff.

Fundamental questions to address include: What functions are necessary? What skills are required to perform them? How should the functions and skills be grouped into roles and people? Which roles can be outsourced and which need to stay in-house? How much capacity is needed in each role? What specific levels of expertise fit best into the strategy?

This work should be done collaboratively with Human Resources, IT, line of business leaders, and others as appropriate. Guidelines such as the *National Cybersecurity Workforce Framework*, published by the National Institute of Standards and Technology (NIST), can aid in this activity. It offers a common taxonomy and lexicon to describe all work and worker competencies in the cybersecurity field.

Recruiting: With some 200 colleges and universities certified by NSA as National Centers of Academic Excellence in Information Assurance Education, the labor market is starting to see measurable increases in college graduates with cyber-related degrees. College courses, assignments, research projects, exercises, and other educational experiences provide a much-needed foundation for the cybersecurity operations workforce.

However, there is no substitute for experience and that can only accrue over time. Many enterprises have discovered that they can hire college graduates at the bachelor's and master's degree levels who have the "book learning" but little or no operational experience. It is much more difficult to find experienced cybersecurity operators.

The recruiting approach and the broader workforce strategy must address this reality. A sound approach is to recognize that any new hires, especially cybersecurity operations hires, will lack experience and will need to grow professionally over time. Achieving this professional growth throughout the workforce should be the focus of the professional development strategy. With such a program, the desired expertise and experience are deliberately and strategically built into the cybersecurity operations workforce over a multiyear period. This is best done with prior planning, and not left to chance in the turbulent environment of day-to-day cybersecurity operations. Additional discussion is found in the "Train and Develop Staff" subsection below.

There are other reasons that professional development must include provisions for continuing education. A focus on helping the individual advance professionally, if done well, usually increases the

EXHIBIT 1: A FOUR PART ACTION AGENDA FOR CYBERSECURITY OPERATIONS

A STRATEGIC APPROACH TO THE DEVELOPMENT OF THE CYBERSECURITY OPERATIONS WORKFORCE SHOULD INCLUDE THE FOLLOWING MAJOR COMPONENTS:

STRUCTURE THE WORKFORCE STRATEGICALLY

Identify and organize cybersecurity workforce needs, roles, job descriptions, skills, and career paths based on business needs and the current and planned IT infrastructure.

ESTABLISH PERFORMANCE STANDARDS

Define standards of performance for cybersecurity operators that are meaningful and measurable. They should represent the end-to-end performance of technology and people.

TRAIN AND DEVELOP STAFF

Implement training for cybersecurity operations personnel to achieve current performance standards, stay up-to-date with technical developments, threats, and solutions, and advance to higher levels of performance in accordance with a career progression reference template.

EVALUATE PERFORMANCE AGAINST STANDARDS

Validate the end-to-end performance of the cybersecurity operations function by assessing performance against the established standard.

Source: Marsh analytics

employee's affiliation with the company and improves retention. Additionally, many of the recognized certifications in the cybersecurity field, as in other fields, require continuing education and training to maintain the certification. Including career path definitions into the workforce development strategy can also improve motivation and retention.

In a field in which qualified workers are in high demand, compensation is a major factor in attracting and retaining staff. Ongoing market research on compensation trends is essential.

Personnel reliability is another important consideration for cybersecurity operations personnel. Cybersecurity operations personnel, as custodians and administrators of enterprise data and systems, literally can possess the "keys to the kingdom," the most valuable enterprise information. Major news stories of trusted IT insiders disclosing highly-classified government information should put all enterprises on notice that the integrity and reliability of their IT people are critically important.

Two: Establish Performance Standards

To achieve a high performance operational capability, setting up a closed-loop "set the standard/train to the standard/evaluate to the standard" construct is a well-established practice across many industry sectors. There is a need to establish performance standards for cybersecurity professionals. This should be aligned with the knowledge skills and abilities outlined in the *National Cybersecurity Workforce Framework*, but needs to go beyond the Framework in terms of specificity.

With standards formally defined and in place, then it is time to implement a program of regular evaluation. The cybersecurity operations practitioners' skills should be measured on a regular basis to assure they are meeting the standard. This can be integrated with the day-to-day job, and technology tools are available to help.

Three: Train and Develop Staff

In addition to what has been previously discussed, continuous changes in technology require this limited pool of staff to be retrained not only on technology, but threat techniques, methods, and vectors, and related changes in organizational policy.

Training requirements for cybersecurity operations staff should include other proficiency training that supports current operations and future growth. One

capability that many organizations have developed internally or that is available through many cybersecurity training organizations is live cyber ranges that offer superb training opportunities in a representative network environment. However, these capabilities and training opportunities come at a cost that organizations and cybersecurity leaders must identify, plan, and budget for as a part of their overall strategy. At a minimum, it includes training of key cybersecurity operations staff on:

- The organization's enterprise IT networks and systems that underpin the business model
- Specific technology related to the organization's cybersecurity controls architecture
- Changes in cybersecurity threat techniques, vectors, and methods targeting the business

Four: Evaluate Performance Against the Standard

Managers should work with existing and new staff to develop an annual cybersecurity proficiency scorecard or assessment to ensure that they are evaluated on and proficient in the specific tasks that their role supports. A detailed description by role should identify the required knowledge, skills, and abilities.

Performance validation testing should be used to assess the end-to-end effectiveness of the organization's technology solutions and the associated human performance. This type of testing can identify gaps or weaknesses in cybersecurity controls implementation and cybersecurity operations and, properly implemented, can improve staff proficiency through hands-on learning in a simulated adversary environment.

CONCLUSION

Cybersecurity is recognized as one of the most important operational risks to enterprises today. The cybersecurity operations workforce is the essential strategic resource on which the effectiveness of enterprise security measures depends. It must be managed accordingly. ♦

Jim Holtzclaw is Washington, D.C.-based Senior Vice President and **Tom Fuhrman** is a Washington, D.C.-based Managing Director, Marsh Risk Consulting.

CHIEF **HUMAN RESOURCES** OFFICER

WHY YOUR EMPLOYEES ARE YOUR STRONGEST – AND WEAKEST – LINK IN YOUR CYBER DEFENSES

Elizabeth Case

An unattended laptop, a lost mobile phone, or a client document that is visible on a commuter's iPad: Like it or not, any of these can be a corporation's worst nightmare when it comes to cyber risk management. Because effective cybersecurity often begins and ends with employee behavior, the Chief Human Resources Officer (CHRO) plays a major role in preventing cyber incidents.

Employees, after all, are a common source of data breaches or business interruption, whether through human error related to information technology (IT), a vendor that had login credentials compromised, or an employee's inadvertent click on a rogue email. According to the *IBM Security Services 2014 Cyber Security Intelligence Index*, human error was cited as a contributing factor in more than 95 percent of the cyber incidents investigated.

As a head of HR, you work to keep employees abreast of incidents that can affect worker safety or morale. Educating them about cyber threat intelligence is no different.

ENGAGING EMPLOYEES TO BE CYBER VIGILANT

The following five preventive steps can help you work with employees to prevent and mitigate cyber attacks:

1. **Monitor your company's bring-your-own-device (BYOD) program.** One of the biggest challenges is how to enforce password protections while conducting business on personal devices.
2. **Put cyber awareness campaigns into place.** HR and IT should work closely to inform employees about cyber threats.
3. **Create policies and procedures around data security when employees leave the company.** Too often, departing employees' credentials are not cancelled in a timely manner, allowing them to retain access to sensitive data.
4. **Educate employees about spear phishing attacks.** It's important to develop live exercises in conjunction with IT to determine employee responses to spear phishing.
5. **Keep abreast of change.** A continuous effort is needed to educate employees about evolving cyber risks.

DEPENDING ON THE MOTIVATION FOR A BREACH, ALL SORTS OF EMPLOYEE INFORMATION CAN GO ASTRAY IN THE MIDDLE OF A CYBER ATTACK, INCLUDING PERFORMANCE RATINGS, SALARIES, AND OTHER PROPRIETARY RECORDS

FACTORING IN LIABILITY

Depending on the motivation for a breach, all sorts of employee information can go astray in the middle of a cyber attack, including performance ratings, salaries, and other proprietary records. And it can be costly. Personal data can potentially be sold on the "dark web," where health records, for example, generally command a higher price than credit card information.

The loss of data can also lead to significant employment practices liability claims against corporations. For example, leaks about salaries or management compensation strategies could lead to claims.

CONCLUSION

As a CHRO, you have a unique opportunity to engage employees about cybersecurity and help them protect themselves and the company. The more active a role you play, the better protected your firm and its people will be. ♦

Elisabeth Case is the National Commercial E&O Practice leader in Marsh's Chicago office.

FURTHER READING

BENCHMARKING TRENDS
Operational Risks Drive Cyber
Insurance Purchases
2016

Analysis of trends in cyber insurance
purchases of US-based companies.

**CONTINENTAL EUROPEAN
CYBER RISK SURVEY**
2016 Report

Survey of risk and finance professionals
in large and medium-sized corporations
across Continental Europe on cyber risk
management approaches and process.
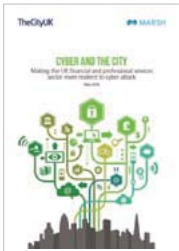
CYBER AND THE CITY
Making the UK financial and
professional services sector
more resilient to cyber attack
May 2016

Recommendations for financial services
firms to improve cyber resilience in
partnership with the government,
regulators, supervisors, police and
intelligence services.
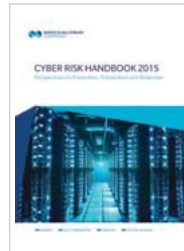
CYBER HANDBOOK 2015:
Perspectives on Prevention,
Preparation and Response

A 2015 collection of includes articles,
report extracts, and perspectives
from business leaders across
Marsh & McLennan Companies as
well as outside experts.
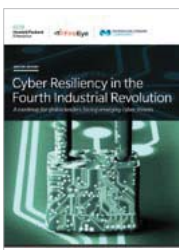
**CYBER RESILIENCY IN
THE FOURTH INDUSTRIAL
REVOLUTION**
2016

Provides a roadmap for global leaders
facing emerging cyber threats in the hyper-
connectivity in of the Internet of Things,
and the Internet of Services.

**EVOLVING CHALLENGES IN
CYBER RISK MANAGEMENT**
Protecting Assets and Optimizing
Expenditures 2016

Overview of shifting cyber threats and how
companies should prepare themselves.

EXECUTIVE BRIEF: REWARDING THE RISK PREVENTERS:
Getting Cyber Staffing Right

Overview of cyber talent needs, the skills and experiences employers seek, and the efforts underway to retain personnel.

GLOBAL RISKS REPORT 2016

The 11th edition of the Global Risks Report identifies top risks and interactions over the next decade, including cyber threats.

PETER BESHAR'S TESTIMONY TO US COMMISSION ON ENHANCING NATIONAL SECURITY
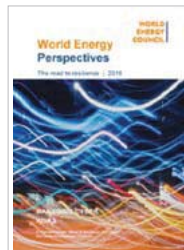
THE ROAD TO RESILIENCE
Managing Cyber Risks
2016

Recommendations to improve cyber risk management for the increasingly digitized and interconnected energy infrastructur

TEN DIGITAL IDEAS
2016

A collection of articles exploring how leaders in financial services, manufacturing, transportation, healthcare, retail, energy, and logistics industries are capitalizing on digital innovations.

UK CYBER RISK SURVEY REPORT
2016

Survey of risk and finance professionals in large and medium-sized corporations across the UK on cyber risk management processes.

ABOUT

Marsh & McLennan Companies' Global Risk Center draws on the expertise of Marsh, Mercer, Guy Carpenter, and Oliver Wyman, along with top-tier research partners from around the world, to address the major threats facing industries, governments, and societies. We highlight critical risk issues, bring together leaders from different sectors to stimulate new thinking, and deliver actionable insights that help businesses and governments respond more nimbly to the challenges and opportunities of our time. Our global digital news hub, BRINK, provides up-to-the-minute insights and informed perspectives on developing risk issues; our Asia Pacific Risk Center and BRINK Asia news hub focus on risk issues relevant to the Asian market.

Marsh & McLennan Companies (NYSE: MMC) is a global professional services firm offering clients advice and solutions in the areas of risk, strategy, and people. 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 of $13 billion and approximately 60,000 colleagues worldwide, Marsh & McLennan Companies provides analysis, advice and transactional capabilities to clients in more than 130 countries. The Company is committed to being a responsible corporate citizen and making a positive impact in the communities in which it operates.

Visit www.mmc.com for more information and follow us on LinkedIn and Twitter @MMC_Global

MARSH & McLENNAN
COMPANIES