MARSH & McLENNAN COMPANIES

FIREEYE | MARSH & MCLENNAN **CYBER RISK REPORT**

2017

CYBER THREATS:

A perfect storm about to hit Europe?

FireEye

SPECIAL REPORT / JANUARY 2017

CONTENTS

Executive summary

Cyber storm clouds are gathering over Europe on three fronts.

First and foremost, the cyber threat environment is intensifying dramatically. Concerns about the misappropriation of financial and personal data — while important — have been supplanted by the spectre of an even larger and more devastating threat. Cyber attacks on critical infrastructure — manufacturing plants, power stations, aviation systems, transportation networks, water systems and even nuclear facilities — are the new reality in Europe. And new vectors of attack are being launched against political parties and electoral systems as national elections loom in France, Germany and the Netherlands in 2017.

Second, while this dynamic is unfolding, the regulatory environment in Europe is about to change profoundly. The European Union has adopted a sweeping General Data Protection Regulation (GDPR) that will impose significant new obligations on industry and its handling of personal data. The Rapporteur assigned by the European Parliament to lead the final negotiations on the EU GDPR, Jan Albrecht, announced upon its passage in the summer of 2016: **"The GDPR will change not only the European Data protection laws but nothing less than the whole world as we know it."**

Third, these two developments beg the question of how prepared businesses are across Europe. To assess their state of preparedness, Marsh conducted a broad survey of 750 European clients. The responses suggest that, while progress has been made, a significant journey remains. If, as we anticipate, cyber breaches begin to fill the headlines of the major European newspapers in 2017, management teams will be pressed, as never before, to address concerns from data protection authorities, supervisory boards and journalists about their state of preparedness. Rather than waiting until 2018, companies must work to confront this looming challenge now.

As trusted cyber advisers, FireEye and Marsh & McLennan — each a leader in its industry — have collaborated to produce this report to help organizations in Europe avoid this perfect storm.

Kevin Mandia
Chief Executive Officer
FireEye

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

...management teams will be pressed, as never before, to address concerns from data protection authorities, supervisory boards and journalists about their state of preparedness.

The dramatically changing cyber threat landscape in Europe

Europe is being forced to confront a growing cyber threat against physical assets. Hackers and purportedly nation states are increasingly targeting industrial control systems and networks — power grids, chemical plants, aviation systems, transportation networks, telecommunications systems, financial networks and even nuclear facilities.

In late 2014, the German Federal Office for Information Security (BSI) reported that a cyber attack had caused "massive damage" to a German iron plant. Utilizing a combination of spear phishing and social engineering, hackers gained access to the iron plant's office network, moved laterally to control the production network and then disabled the shut-off valves on the plant's blast furnaces. In the parlance of the industry, this was a "kinetic" or physical attack against hard assets.

In late 2015, hackers turned their focus to the power industry. In one of the largest attacks of its kind, hackers shut off the power to hundreds of thousands of residents in Ukraine. According to public reports, the attacks that caused the power outage were accompanied by parallel cyber intrusions into Ukraine's train system and TV stations.

In October 2016, the head of the International Atomic Energy Agency at the United Nations, Yukiya Amano, publicly disclosed for the first time that a "disruptive" cyber attack had been launched against a nuclear facility in Germany. This report came on the heels of an analysis by the Nuclear Threat Initiative warning of lax cyber security at nuclear facilities in a number of countries across Europe.

Thus, cyber attacks against critical infrastructure, dubbed a potential "Cyber Pearl Harbor" by US military officials, are no longer the fantasies of Hollywood producers, conspiracy theorists or sci-fi aficionados, but are the reality that governments and businesses across Europe must now confront.

What EU countries are being targeted with the greatest frequency?

Cyber hackers are increasingly opportunistic – smart, savvy, and innovative. Hackers are bypassing traditional defenses by continually engineering new methods of attack. Even sophisticated cybersecurity programs are being thwarted, often by targeting weak links in the chain, including vendors and employees. Due to its advanced economies and important geopolitical positioning, Europe is a prime target for these attacks.

In 2016, hackers most often targeted financial, manufacturing, telecom industries and governments in Germany, Great Britain, Belgium, Spain, Denmark, Sweden, Norway and Finland.

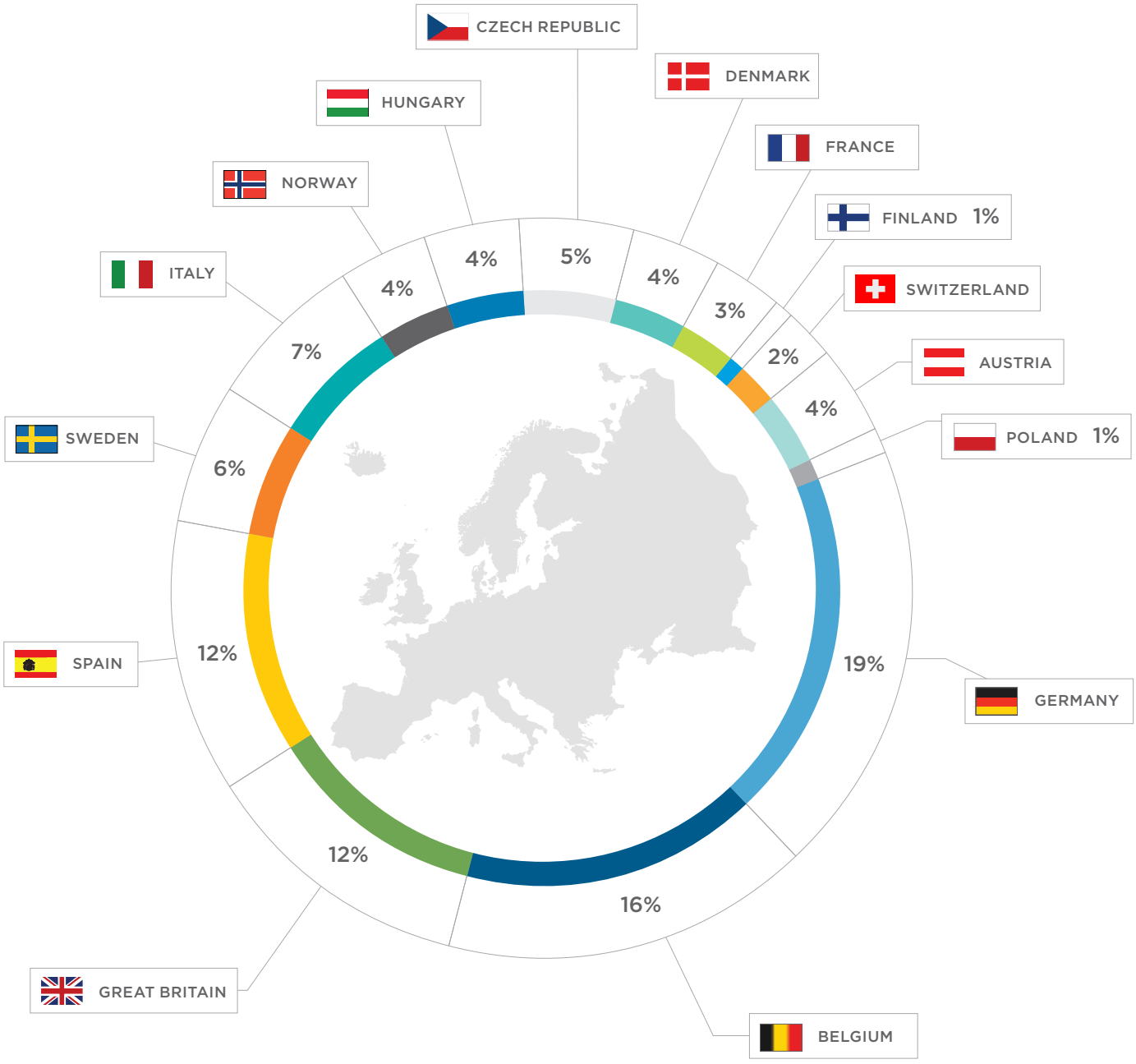


Figure 1. **Illustrates targeted malware detections from January 2016 to September 2016**

Targeting of EU countries

Europe's largest economies remain the top targets, but the focus ranges broadly across the continent. Figure 1 shows targeted malware detections from January to September 2016 for all EU nations except Turkey and Russia. (Nations not represented on this chart received little or no malware assessments from FireEye.)

Had Turkey been included, it would far overshadow the EU nations represented. Turkey accounted for a whopping 77 percent of all targeted malware detections by FireEye in Europe.

Germany powerfully demonstrates the changing cyber environment. Last month, Thyssen Krupp, a large German industrial conglomerate, disclosed that "technical trade secrets" were stolen in a cyber attack that dated back almost a year. The company filed a criminal complaint with the German State Office for Criminal Investigation and stated publicly, "It is currently virtually impossible to provide viable protection against organized, highly professional hacking attacks."

The type of data being stolen in these attacks is particularly revealing. While sensitive personal information like financial or health records remains a key focus, hackers are increasingly targeting higher value data relating to infrastructure systems. Based on FireEye's research, 18 percent of the data that was exfiltrated through cyber attacks in Europe in 2016 related to companies' industrial control systems, building schematics and blueprints, while a further 19 percent related to trade secrets.

The federated nature of Europe also increases the potential cyber risk across the continent. Each EU member state has a different cybersecurity maturity. As more and more components of infrastructure are connected to the Internet and the Internet of Things explodes in popularity, certain countries within Europe may lack the capabilities needed to assess and implement a sophisticated cybersecurity framework to defend against these emerging threats. As a result, hackers can take advantage of the disparate architecture across the EU.

What specific industries are being targeted and how?

The vertical industry analysis below reveals which sectors are being targeted with the greatest frequency. The three industries that draw the greatest attention in Europe are:

- Financial services
- Manufacturing
- Telecommunications

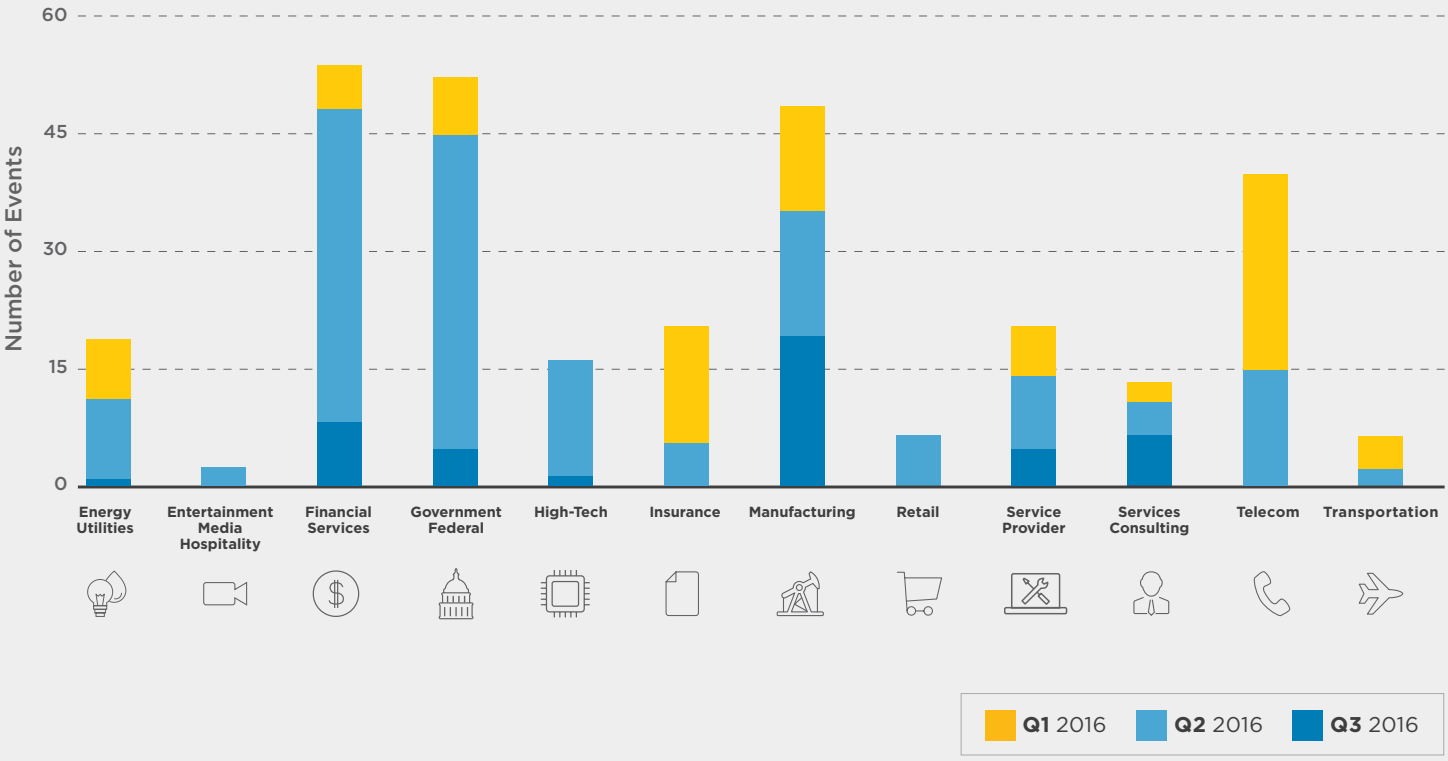
In the third quarter of 2016, threats accelerated in particular against manufacturers and telecom operators. Conversely, retailers, a key focus of cyber attacks in the United States, are virtually at the bottom of the list in Europe.

In addition, governments are a primary target for hackers across Europe. Indeed, aggregating attacks against national, state and local governments into a single category makes government the number one target in Europe.

To date, there has been an underreporting of cyber incidents in the EU. Nonetheless, a handful of public reports reveal significant cyber incidents across the continent. In 2016, cyber hackers stole more than $75 million from a Belgian bank and $50 million from an Austrian aircraft parts manufacturer through fraudulent emails mimicking legitimate communications to fool companies into transferring money to a hacker's account.

In sum, no sector of the economy is immune from attack — not industry, not government and not even the not-for-profit sector. Accordingly, we need a mindset, particularly between government and industry, that we are all in this together.

Figure 2. **Targeted malware detection across Europe during January - September 2016**



...no sector of the economy is immune from attack — not industry, not government and not even the not-for-profit sector.

DWELL TIME UNTIL A COMPROMISE IS DETECTED

469

DAYS IN **EUROPE**

146

DAYS
GLOBAL AVERAGE

SOURCE OF DISCOVERING COMPROMISES: EMEA VS. USA

12%

EXTERNAL DISCOVERY
IN EMEA

53%

EXTERNAL DISCOVERY
IN USA

Companies in Europe take 3x longer to detect cyber intrusions

FireEye found that companies in the European Union take three times longer than the global average to detect a cyber intrusion. The region's mean "dwell time" — the time between compromise and detection — was 469 days, versus a global average of 146 days.

The delay in identifying intrusions has profound consequences. At a basic level, the notion that hackers are rooting around in companies' networks undetected for 15 months is sobering, as it allows ample opportunity for lateral movement within IT environments.

Equally important, dwell times of this length allow hackers the opportunity to develop multiple entry and exit doors. When a company does detect an intrusion, the natural first impulse is to shut down its system to "stop the bleeding." Numerous stakeholders then press the organization and its management team to get back online and operating.

In this dynamic, FireEye has found that hackers compromised many organizations in Europe a **second time within months** of the initial breach. Repeated breaches most often result from the use of unsuitable techniques to hunt initially for attacks within their environment. Many companies still opt for a traditional forensic methodology, only analyzing a handful of machines or systems. On average, however, hackers in Europe have infected approximately 40 different machines in any given company during the length of their cyber intrusions.

So, what can be done to reduce the average dwell times?

Unlike in the United States and other parts of the world, it is quite rare in Europe for external actors, including government agencies, to notify a company that its systems have been breached. In fact, companies in Europe learn of breaches in their systems from external parties only 12 percent of the time. This lack of external notifications could also allow for speculation that a large number of intrusions remain undiscovered.

By contrast, this has become fairly commonplace in the US. As a result of outreach by the Federal Bureau of Investigation, the Secret Service and cybersecurity companies, more than half of all US companies (53 percent) learned that their information systems had been hacked by external parties.

This is a critical place where governments can help enhance the cyber resilience of industry by sharing threat and actual breach intelligence in real time. This type of cooperation from national governments and organizations like Europol and sector specific information sharing & analysis centres (ISACs) will reduce average dwell times and thereby bolster cyber resilience across the continent.

How are motives and tactics changing?

Hackers come in many forms and differing degrees of sophistication. In addition to attacks against critical infrastructure, EU cyber threats are dominated by two distinct groups: hackers with political goals and hackers with financial motives.

Is politically motivated hacking on the rise?

In 2016, FireEye observed numerous nation-state or nation-sponsored intrusions against EU governments, and specifically against foreign or defense ministries of member states. Recently, nation-state sponsored threat actors have shown strong interest in extending these attacks into the political arena.

In September 2016, politicians and employees of political parties in Germany were targeted with a series of spear phishing e-mails, purportedly from NATO headquarters, regarding a failed coup in Turkey and the earthquakes that hit Italy's Amatrice region. The links to these spurious e-mails contained malware. Arne Schoenbohm, the head of the German BSI, responded swiftly by warning political parties across the spectrum in Germany that the country needed to learn the lessons from the recent elections in the United States.

In December, the focus shifted to France. France's National Cybersecurity Agency, known as the ANSSI, summoned representatives of all political parties to a detailed cyber briefing about the threat posed by cyber attacks.

Prior to the recent attacks in the US, few would have considered political parties and voting machines as part of a nation's critical infrastructure. With national elections looming in the Netherlands (March 2017), France (May 2017) and Germany (late 2017), however, the risk posed to the integrity of the electoral process is all too real.

... the notion that hackers are rooting around in companies' networks undetected for 15 months is sobering, as it allows ample opportunity for lateral movement within IT environments.

As more criminals successfully carry out ransomware attacks, others are enticed to try this growing type of malware attack.

This is not a message that you want to see on your network.

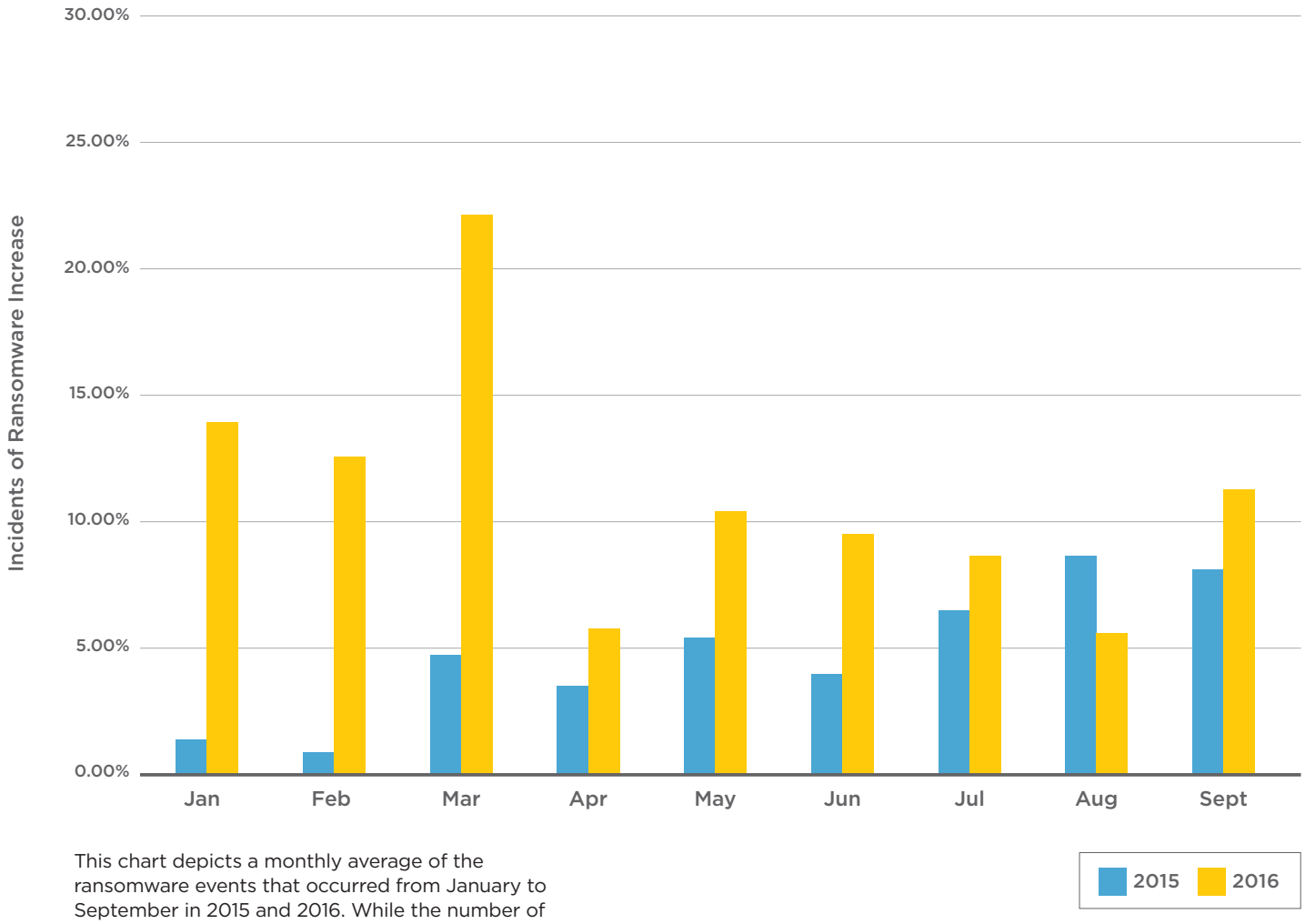
Criminal hackers still a dangerous threat

Cyber criminals continue to target organizations and private citizens across Europe to steal information, stage cyber extortion attacks, and steal money through fraudulent transactions.

The use of "ransomware" spiked significantly in 2016. Victims are asked to pay a ransom in the form of "bitcoins." Utilizing malware with names like Cryptolocker, TorLocker and Teslacrypt, hackers encrypt your files and then demand a ransom to unlock them. In one recent example, a ransomware variant called "Locky" targeted users in more than 50 countries — many of them in Europe. Locky utilized exploit kits and mass e-mailing campaigns, often seen with spam. The campaign enticed recipients to open e-mail attachments that appeared to be invoices but instead contained malware. Victims are asked to pay the ransom to obtain a decryption key that will then unlock their systems. As more criminals successfully carry out ransomware attacks, others are enticed to try this growing type of malware attack. This form of attack has been particularly prevalent in the health care space, with one report contending that 88 percent of ransomware attacks target the healthcare industry.[1]

1 Solutionary's Security Engineering Research Team Quarterly Threat Report, Q2 2016.

Figure 3. **Ransomware evolution: Europe**



This chart depicts a monthly average of the ransomware events that occurred from January to September in 2015 and 2016. While the number of events varied, the increase in events in 2016 over the prior year is significant — and worrisome.

In addition, there has been an increase in targeting of corporate executives across Europe to carry out a scam known as "CXxO fraud" or "Business E-mail Compromise." Cyber criminals typically mimic a small- to mid-size enterprise with international supply chains requiring regular wire transfer payments. Hackers compromise legitimate business e-mail accounts and then request unauthorized transfers of funds.


"The GDPR will change not only the European Data protection laws but nothing less than the whole world as we know it."

The regulatory environment in Europe is about to change — and profoundly

As European organizations encounter a rapidly changing cyber threat landscape, what about the regulatory environment?

While the front pages of the Wall Street Journal, USA Today and the New York Times regularly feature reports of breaches against US-headquartered companies, the situation appears on the surface to be blissfully different in Europe. It is exceedingly rare that Der Spiegel, Le Monde or Corriere della Sera carry accounts of high-profile breaches against large European companies.

Why is that? The fundamental difference in the two continents is that in the United States, more than 50 federal, state and local laws mandate disclosure of cyber breaches to regulators or affected consumers. Until recently, the regulatory regime in Europe was far different.

That is about to change profoundly. With the recent passage of the European Union's General Data Protection Regulation (GDPR), companies will soon be required to publicly disclose data breaches to national data protection authorities and, where the threat of harm is substantial, to affected individuals. Failure to do so could result in fines of as much as four percent of a company's global turnover — a staggering sum.

This sea change in the public reporting obligations of companies will carry significant ramifications for governments, businesses and consumers across Europe.

In addition, the Network Information Security Directive, adopted by the EU in July 2016, will place further demands on governments and the operators of critical infrastructure.

EU General Data Protection Regulation

Jan Philipp Albrecht, a member of the European Parliament from Germany and the Rapporteur for the GDPR, captured the awesome aspirations of European policymakers in approving this new regulation: "The GDPR will change not only the European Data protection laws but nothing less than the whole world as we know it."

Albrecht's comment reflects the strength of the belief in Europe that privacy constitutes a fundamental human right.

With the growth of Internet-related technology, companies have accumulated troves of personal data. Business procedures have typically been focused on aggregating broad categories of data gleaned from consumers. Fearing the impact to the privacy rights of individuals, the European authorities are now strengthening privacy law to control, limit and expose the sweeping collection and use of data by many organizations.

Once implemented in May 2018, the GDPR will introduce a seismic shift in how companies retain and utilize personal data of individuals subject to the EU's jurisdiction. To prepare for implementation, companies must begin assessing the current state of their operations and the sweeping breadth of the new requirements.

While the regulation is nearly 90 pages long, there are four broad themes that are worth emphasizing:

- Individuals will have enhanced rights.
- Companies will be forced to reassess the manner in which they process and retain data.
- Companies will need to review their contractual arrangements with a host of third parties.
- Companies will be held to far stricter accountability and sanctions.

Figure 4. **Components of GDPR implementation**

Sweeping jurisdiction

The GDPR purports to extend its reach far beyond the borders of the European Union to any organization that might collect or process "personal data" of an individual subject to EU jurisdiction (known as "EU data subjects"). Extending data protection beyond EU borders reflects the EU's view that data privacy protections should apply wherever data may travel. In practice, the broad jurisdictional provisions signal a clear hope that the GDPR's complex regulations will have a global impact.

Privacy impact assessments

Businesses can expect both regulatory authorities and individuals to make inquiries about how data is being processed. Individuals can object to any data collection made without an adequate basis and can demand correction of inaccurate information. Organizations must perform so-called "data impact assessments" prior to collecting data.

The GDPR provides guidance on practices to protect data, such as de-linking data from identities ("pseudonymisation"), encryption, regular assessments of technical controls, and incident response plans that account for maintaining the confidentiality and integrity of data.

Affirmative consent and the right to be forgotten

The GDPR makes clear that no company may collect personal data without first notifying users of how their data will be stored, protected and shared with third parties. In order to collect data, the company must first obtain the individual's "freely given, specific, informed and unambiguous" consent for the collection. The GDPR will require users to give consent by affirmatively clicking on a consent notice or opting for specific technical settings that allow for the data collection.

Lastly, the GDPR codifies "the right to be forgotten." Already recognized by European courts and some member states, the right to be forgotten allows data subjects to demand that their personal data be erased and no longer used for processing.

Businesses can expect both regulatory authorities and individuals to make inquiries about how data is being processed.

So that is the dramatically altered regulatory regime that will begin to take effect in early 2018. What insight do we have about how sweeping its impact will likely be?

The Dutch "mini-GDPR"

This is where the Dutch "mini-GDPR" comes into play. After a series of cyber attacks in 2015, the Dutch Parliament passed a Personal Data Protection Act, known as the Wet Bescherming Persoonsgegevens ("WBP"), in late 2015. In the time since the Dutch "mini-GDPR" took effect on January 1, 2016, companies have already notified the Dutch authorities of more than 5,500 cyber "incidents." Extrapolating these figures across the EU gives a glimpse of what management will likely confront in response to inquiries from regulators, supervisory boards and the press.

Network Information Security Directive

To enhance focus on the specific vulnerabilities regarding critical infrastructure, the EU separately enacted the Network Information Security (NIS) Directive. Also scheduled to take effect in 2018, the NIS Directive will impose additional obligations on EU member states and infrastructure operators to raise the baseline of their cybersecurity capabilities. For example, the NIS Directive will require all member states to have a cybersecurity strategy, a national competent authority, and national cybersecurity incident response teams.

Several EU nations have already demonstrated early leadership. For example, Germany announced the creation of a mobile Quick Reaction Force as part of its Federal Office for Information Security.

Cyber preparedness in the EU is improving, but the journey has just begun

With the threat environment intensifying and the regulatory environment about to change profoundly, the question becomes whether industry and even government are ready for these changes.

Marsh surveyed the cyber practices at more than 750 of its clients across continental Europe in the fall of 2016.[2] The study found that while high-profile events, government initiatives, and legislation have pushed cybersecurity to the forefront, far more work needs to be done.

For example, Marsh found that the percentage of companies indicating that they assessed "key suppliers" for cyber risk actually decreased from 23 percent in 2015 to 20 percent in 2016. As numerous attacks in the US and elsewhere have shown, hackers often gain access to larger organizations by initiating attacks against smaller vendors that provide services like air conditioning or takeout food.

2 Continental European Cyber Risk Survey: 2016 Report

General awareness of the risk posed by cyber attacks, while increasing, remains low. The percentage of companies that report having a strong understanding of their cyber posture increased from 21 percent in 2015 to 31 percent in 2016. Similarly, companies that regard cybersecurity as a top-five risk increased from 17 percent in 2015 to 32 percent in 2016, and the percentage of organizations that did not even include cyber on their risk register dropped from 23 percent in 2015 to 9 percent in 2016.

Despite this progress, European companies, like their counterparts around the world, have a long way to go to keep pace with the dramatically changing threat and regulatory environments.

31%

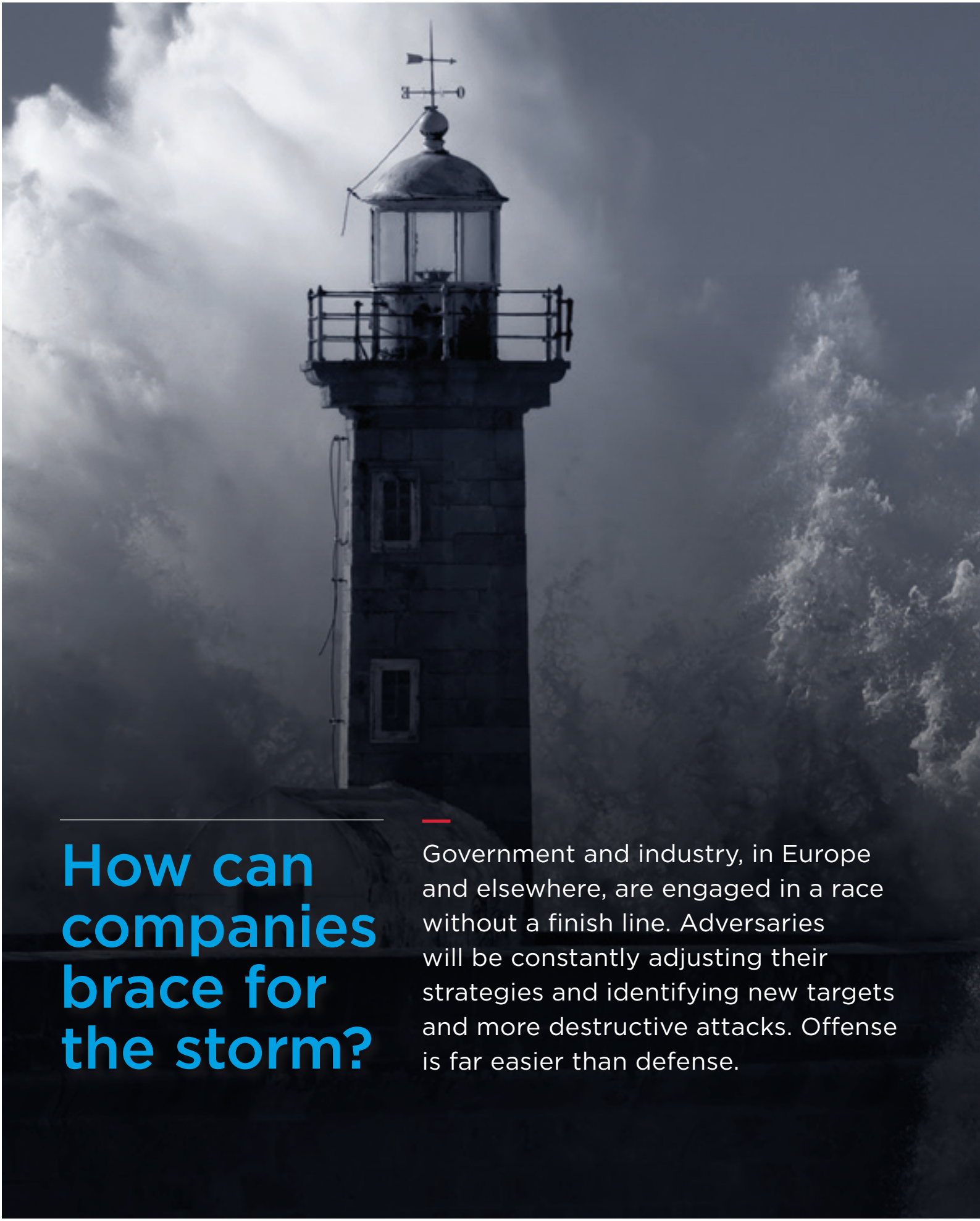
COMPANIES THAT HAVE A **STRONG UNDERSTANDING OF THEIR CYBER POSTURE**

32%

COMPANIES THAT REGARD **CYBERSECURITY AS A TOP-FIVE RISK**

9%

ORGANIZATIONS THAT **DID NOT EVEN INCLUDE** CYBER ON THEIR RISK REGISTER



How can companies brace for the storm?

Government and industry, in Europe and elsewhere, are engaged in a race without a finish line. Adversaries will be constantly adjusting their strategies and identifying new targets and more destructive attacks. Offense is far easier than defense.

While there are many technological advances that will form part of the solution, potentially including encryption at rest and blockchain, we focus on five non-technological recommendations.

1

Cybersecurity is not solely an IT issue.

The most senior members of a company's management team must engage and be at least conversant with this dynamic risk. In your organization, can the CEO, the CFO or the GC answer the following three questions:

- What are your company's principal cyber vulnerabilities?
- What are your key strategies for mitigating those risks?
- Are adequate resources being devoted to the task at hand?

2

Vulnerability assessments are essential.

Every company should conduct a vulnerability assessment. The best place to start in 2017 is to benchmark your cyber protocols against an established standard. What are your most critical cyber assets? Does your organization primarily rely upon proprietary data or industrial control systems? Have you assessed the true financial consequences of a large-scale breach?

3

Cyber risk is now a board-level issue.

Supervisory boards in Europe will be putting far more focus and pressure on management teams in the coming year. Expect your board to ask questions about patching of software vulnerabilities, implementing multi-factor authentication for user access, and conducting risk assessments of third-party vendors and suppliers. If it takes your organization three times longer to identify a cyber intrusion as other companies, will that be satisfactory for your board?

4

Corporations should engage with external stakeholders.

If the premise is correct that cyber breaches will become a far more public issue for European corporations in the coming 12-18 months, now is the time to prepare by reaching out to build relationships of trust with data protection and law enforcement authorities, policymakers and the press. In addition, have you engaged top-notch security experts to respond to an incident?

5

Governments in Europe must lend a hand to the business community.

Given the particular threat posed to critical infrastructure, governments in Europe should reach out more affirmatively to the business community on two fronts:

- By sharing threat intelligence in real time regarding the latest forms of attack and known malicious IP addresses.
- By promptly alerting businesses that their systems have been breached.

An enhanced level of trust between government and industry will pay dividends in a host of different areas.

A call to action

FireEye and Marsh & McLennan Companies joined together to provide an overview of a fundamental challenge facing the European Union — the evolving threat landscape and questions surrounding the region's ability to address new cyber threats. There are no quick fixes or magic solutions. No sector, in isolation, can solve this issue on its own. Rather, a true public-private partnership is required.

Our goal with this paper is to increase awareness of emerging threats and recommend tangible steps for businesses and government across Europe to enhance their cyber resilience.

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 5,300 customers across 67 countries, including more than 825 of the Forbes Global 2000.

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

About Marsh & McLennan Companies

Marsh & McLennan Companies provide advice and solutions to mitigate cyber risk. As the world's most trusted cyber insurance broker, Marsh, Inc. advises over 1,000 clients regarding network security and privacy issues and has won Advisen's award for Cyber Broker of the Year in 2014, 2015 and 2016.

www.marsh.com/us/services/cyber-risk.html

For more information, please contact:

Europe
Flavio Piccolomini
CEO, Marsh Continental Europe
flavio.piccolomini@marsh.com
39 02 48 53 84 62

Nilay Ozden
Marsh FINPRO Practice Leader
nilay.ozden@marsh.com
44 78 25 22 84 54

Giampaolo Scarso
Head of Client Advisory Services, Marsh Central Europe, Middle East and Africa
giampaolo.scarso@marsh.com
39 02 48 53 82 81

Jean Bayon de La Tour
Marsh Cyber Development Leader
jean.bayondelatour@marsh.com
33 1 41 34 50 05

Corrado Zana
MRC Business Resilience Leader
corrado.zana@marsh.com
39 02 48 53 85 27

United Kingdom
Mark Weil
CEO for Marsh UK & Ireland
mark.weil@marsh.com
44 20 73 57 59 27

Peter Johnson
Marsh UK Cyber Advisory Lead
peter.a.johnson@marsh.com
44 20 7357 3527

United States
Thomas Reagan
Cyber Practice Leader
thomas.reagan@marsh.com
+1 212 345 9452

Robert Parisi
Cyber Product Leader
robert.parisi@marsh.com
+1 212 345 5924

Thank you to our contributors:

FireEye
Tony Cole
Kristi Houssiere
Stuart McKenzie
Jens Monrad
Nick Rossmann
Tony Sapienza
Lynn Thorne
Kristen Verderame

Marsh & McLennan
Devin Beresheim
Ronnie Brandes
Matthew McCabe
Bob Parisi
Tom Reagan
Inna Tsimerman

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

www.FireEye.com