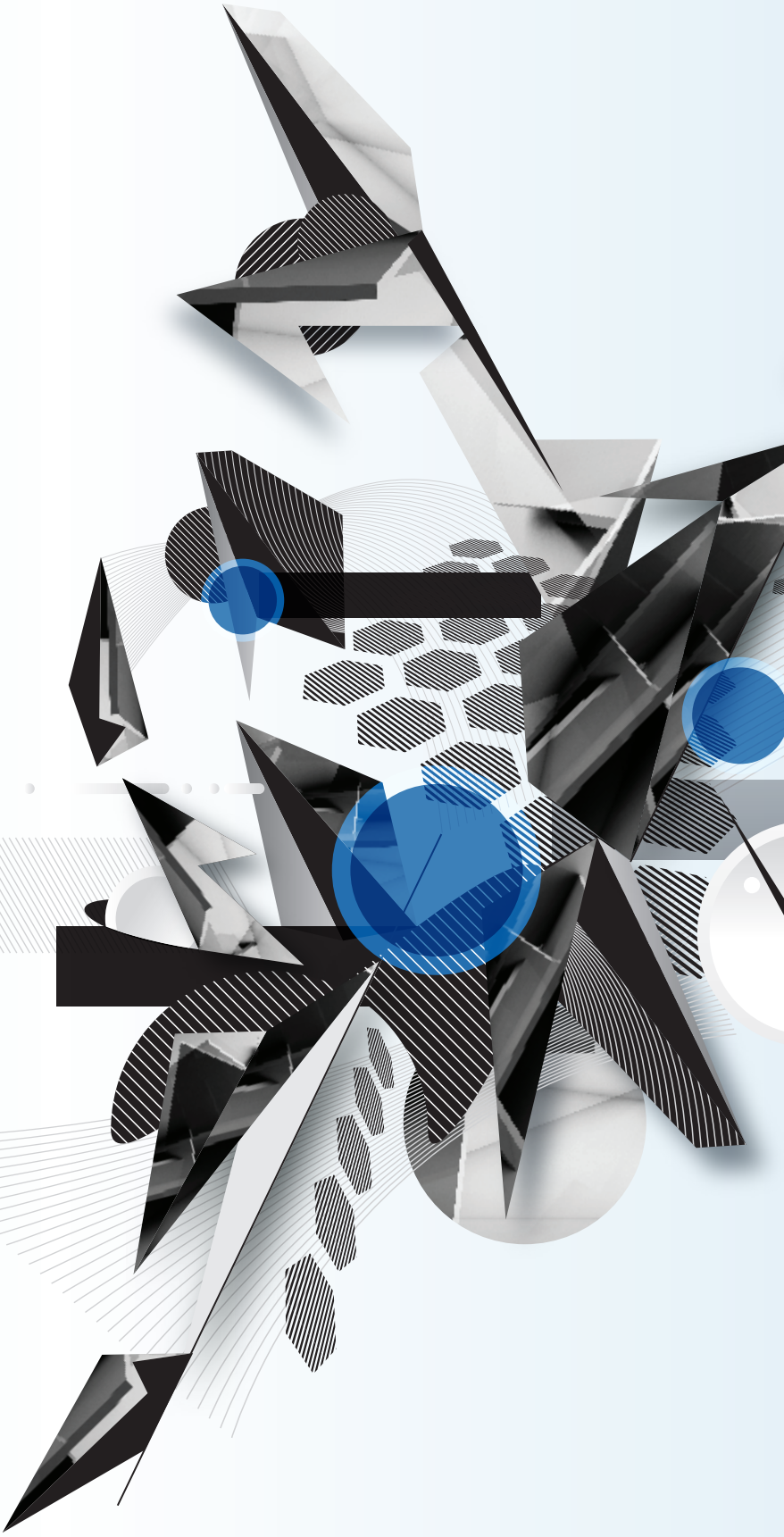
MARSH & McLENNAN COMPANIES

CYBER:

The Stakes Have Changed for the C-Suite



FireEye®

REPORT | JANUARY 2018

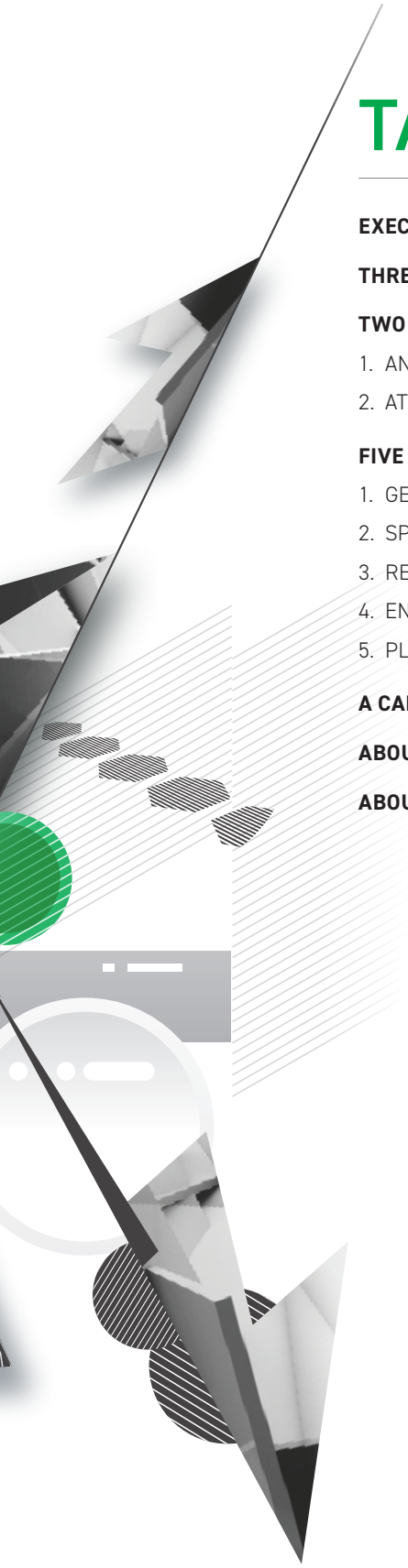


TABLE OF CONTENTS

EXECUTIVE SUMMARY

The cyber stakes changed for the c-suite in 2017. Nation states targeted private companies. Corporations lost billions in market capital. CEOs were toppled from office.

This is the new cyber reality.

In 2018, two emerging trends will complicate this dynamic even further—tough new regulations and frightening new vectors of attack.

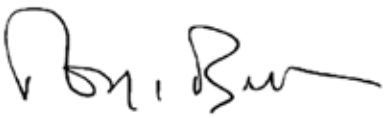
FireEye and Marsh & McLennan, both leaders in our respective sectors, have collaborated to produce this cyber white paper specifically for c-suite executives and public company board members.

Executives and board members start on unfamiliar terrain in two ways. First, with limited exceptions, we are digital immigrants — not digital natives. We are more likely to have studied humanities in college than computer science. IT executives at our companies brief us, but, unlike so many other operational or financial areas, we may not have an intuitive feel for the right answer.

Second, throwing more money at the problem will not make this issue go away. Most companies can double their IT security budgets and still be exposed. The recently disclosed "Meltdown" and "Spectre" vulnerabilities — potentially impacting computers around the globe — highlight this point.

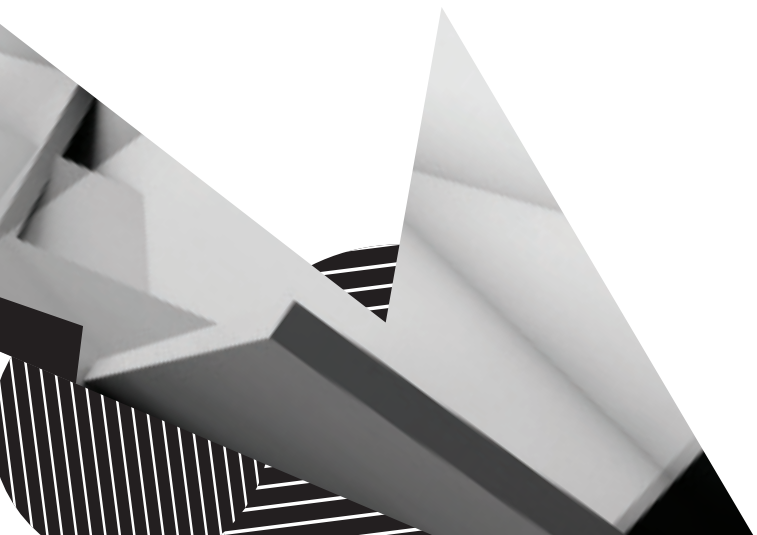
So we are all engaged in a race without a finish line. In this report, we share five tangible, and practical, suggestions for your consideration. Our collective objective is enhanced cyber resilience—not perfection.

Kevin Mandia
Chief Executive Officer
FireEye



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

THREE EVENTS IN 2017 THAT CHANGED THE CYBER LANDSCAPE



Three events in particular changed the **cyber stakes** in 2017.

On May 12, 2017, the Wanna Cry ransomware attack cascaded across the globe, and we watched as a self-perpetuating "worm" jumped across networks and infected more than 300,000 computers in 150 countries. In the United Kingdom alone, more than 80 National Health System hospitals were impacted, resulting in cancelled surgeries and diverted ambulances.[1] Tom Bossert, the homeland security advisor to President Donald Trump, attributed the attack to North Korea: "North Korea has acted especially badly, largely unchecked, for more than a decade . . . WannaCry was indiscriminately reckless."[2]

A month later in June 2017, the NotPetya virus was launched in Ukraine and rapidly spread across the world. NotPetya's "wiper" malware was even more nefarious than the WannaCry ransomware because the infected data was destroyed rather than merely held hostage. Consumer goods manufacturers, transport and logistic companies, pharmaceutical firms and utilities reportedly suffered over $1 billion in economic losses in the aggregate[3].

The summer of cyber woe peaked in August when a well-respected consumer credit reporting agency reported the loss of personal records for almost 150 million people. The reaction was swift and severe. Within days, the market cap loss exceeded $5 billion. The Federal Trade Commission and both houses of Congress launched investigations. The company's chief information officer, chief information security officer, and later, chief executive officer, all stepped down in the aftermath of the breach[4].

So, in our opinion, 2017 goes in the record books as the worst year in cybersecurity history.

---

[1] "Ransomware attacks leave insurers and businesses exposed," by Patricia L. Harman. (PROPERTYCASUALTY360.COM, June 1, 2017). (accessed at http://www.propertycasualty360.com/2017/06/01/ransomware-attacks-leave-insurers-and-businesses).

[2] "It's Official: North Korea Is Behind WannaCry," by Thomas P. Bossert, WALL STREET JOURNAL (Dec. 18, 2017). (accessed at https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537).

[3] See NotPetya Ransomware Attack Causes $375M Loss for Pharma Giant Merck, Approaching $1B In Total Damages," (SNIP.COM 11/2/2017). (accessed at https://www.snip.today/post/notpetya-ransomware-attack-causes-375m-loss-pharma-giant-merck-approaching-1b-total-damages/).

"Shipping Company Maersk Says June Cyberattack Could Cost It Up To $300 Million," (CNBC Aug 16, 2017). (accessed at https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html).

"NotPetya's Cost to FedEx: $400 Million and Counting," (THE SECURITY LEDGER, Dec. 22, 2017). (accessed at https://securityledger.com/2017/12/notpetyas-cost-fedex-400-million-counting/).

[4] "Retail Upheaval, Data Breaches and Tech Innovations." (WSJ, Dec. 2017). (accessed at https://www.wsj.com/articles/retail-upheaval-data-breaches-and-tech-innovations-1513703018).

"The GDPR will change ... the whole world as we know it."

TWO EMERGING TRENDS IN 2018

Two trends will emerge with force that will make this dynamic far more challenging.

1. An Array of New Cyber Laws, Particularly the GDPR

Governments are adopting new laws that impose elevated, and exacting, standards on the business community. The most significant of these new laws is the European Union General Data Protection Regulation, which will take effect in May. Jan Philipp Albrecht, a member of the European Parliament from Germany and the Rapporteur for the GDPR, aptly captured the ambitions of European policymakers saying, "The GDPR will change not only the European Data Protection laws but nothing less than the whole world as we know it.[5]"

The GDPR will bring about a sea change around the public reporting obligations of companies handling data in Europe. For the first time, companies will be required to disclose cyber breaches to regulatory authorities and, where the threat of harm is substantial, to affected consumers. The penalties for non-compliance are steep, at up to four percent of revenues.

Numerous other national and local governments have adopted new cyber laws. For example, the New York State Department of Financial Services now requires regulated companies to adopt certain controls, including multi-factor authentication and encryption at rest, or explain why adoption is not feasible. Senior executives are required to "certify" their organization's compliance with the regulation. China, Japan, Australia, Israel, Singapore, and other countries around the world have recently adopted sweeping new cyber laws.

2018

The year the General Data Protection Regulation (GDPR) goes into effect. It was adopted in April 2014 and is effective as of May 25, 2018.

GDPR

The GDPR is a sweeping reform of EU data protection legislation. It will impose significant new obligations around cyber breach disclosure.

€2.3 BILLION

The amount the EU estimates businesses will save by having identical data protection laws.[6]

[5] "How the GDPR Will Change the World," by Jan Philipp Albrecht (March 2016). (accessed at https://edpl.lexxion.eu/data/article/10073/pdf/edpl_2016_03-005.pdf).

[6] "What is GDPR? Everything You Need to Know before the 2018 Deadline," by Dale Walker, Joe Curtis. (Dec. 2017). (accessed at http://www.itpro.co.uk/it-legislation/27814/what-is-gdpr-everything-you-need-to-know-8/page/0/1).

SURVEY OF 1,300 CORPORATE EXECUTIVES

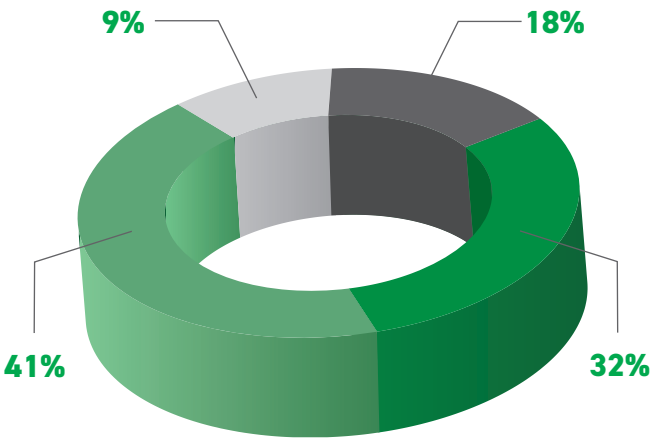
To gauge the state of readiness of the business community to meet the new requirements of the GDPR, Marsh recently conducted a global cyber risk survey. More than 1,300 corporate executives from around the world participated in the survey, including over 500 from organizations that offer products and services in Europe.

So, what did we learn?

Organizations offering products/services in continental europe

2016

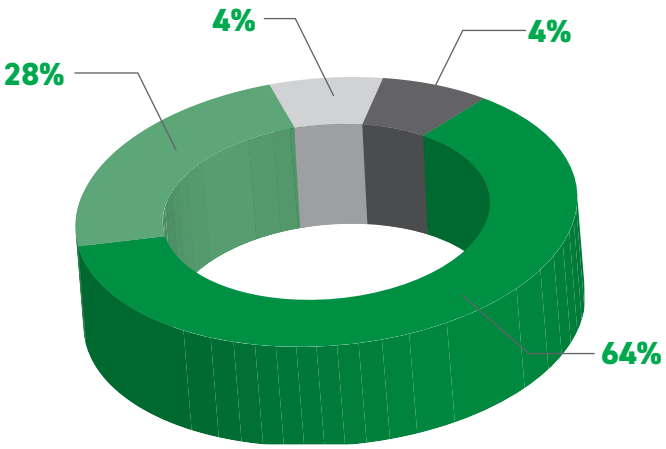
Where does cyber risk feature on the corporate risk register?



- A top five risk
- A risk, but not in the top five
- Cyber risk does not feature on the corporate risk
- My organization does not have a corporate risk register

2017

Among my organization's risk management priorities cyber risk is....



- A top five risk
- A risk, but not in the top five
- Cyber risk is a low priority/not a priority for my organization
- I don't know

CYBER AWARENESS IN EUROPE HAS DOUBLED

First, some good news. In our survey, 64 percent of respondents who offer products or services in Continental Europe now consider cyber attacks as a Top Five risk for their organizations. In a similar survey Marsh conducted in Continental Europe in 2016, only 32 percent of companies rated cyber as a Top Five risk.

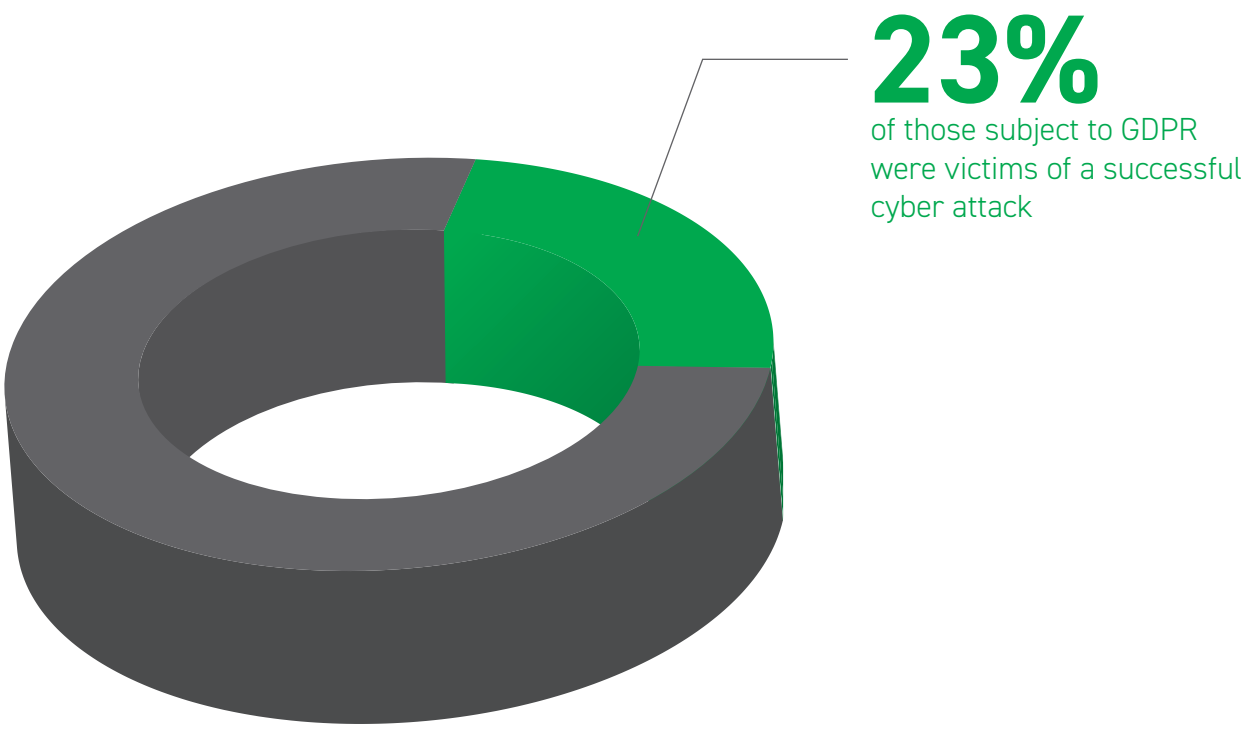
Starting this May, many cyber incidents that previously remained below the surface will become public events.

23 PERCENT REPORTED BEING SUCCESSFULLY HACKED

On a less positive note, 23 percent of these executives revealed that their organizations were the subject of a "successful" cyber attack in just the past year. This answer was significant, particularly given the GDPR's public reporting obligations.

Starting this May, many cyber incidents that previously remained below the surface will become public events. As a result, supervisory boards, the press, consumers, and regulators will scrutinize management's response.

Has your organization been a victim of a successful cyber attack in the past 12 months?



2. Attacks Against Safety Control Systems

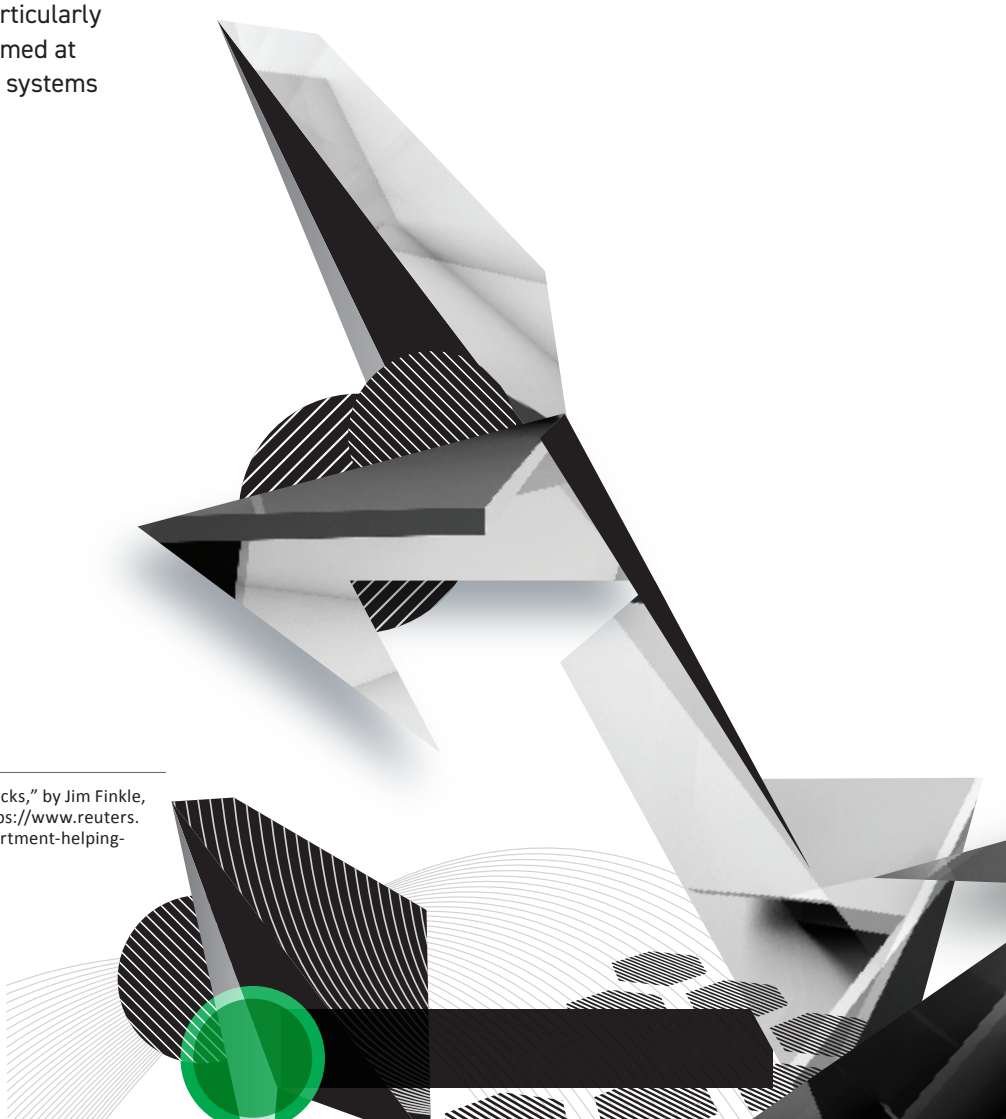
The second major trend that will accelerate in 2018 is the emergence of new vectors of attack, particularly against critical infrastructure.

In the past few years, hackers have increasingly targeted organizations that operate industrial control systems. For example, the US Department of Homeland Security and the FBI released a joint bulletin last year warning that hackers had targeted the Wolf Creek nuclear power plant in Kansas.[7]

FireEye recently responded to an incident at a facility where an attacker deployed malware designed to manipulate industrial safety systems. The targeted systems provided emergency shutdown capability for industrial processes.

This is one of a small but growing number of particularly troubling attacks we are aware of specifically aimed at industrial control systems. Safety instrumented systems monitor processes and trigger alarms if hazardous levels are reached. Think of emergency shutdown systems at a nuclear plant or a chemical facility.

This development is doubly significant from a cyber perspective. To date, cyber attacks have largely occurred in the digital, rather than physical, world. As more physical processes come online, nation states are increasingly turning their sights toward chemical facilities, energy platforms, transportation networks, manufacturing plants, pipelines and water systems. If attackers can reprogram safety instrumented systems, the ramifications could be profound both in terms of physical damage and loss of life.



[7] "U.S. Energy Department Helping Power Firms Against Cyber Attacks," by Jim Finkle, Scott DiSavino, and Timothy Gardner. (July 2017) (accessed at https://www.reuters.com/article/us-usa-cyber-energy-nuclearpower/u-s-energy-department-helping-power-firms-defend-against-cyber-attacks-idUSKBN19S27Z).

FIVE PRAGMATIC ACTION ITEMS

While the challenges are indeed daunting, here are five practical, action-oriented suggestions to consider:

1. Get Your Arms Around the Cloud

The cloud computing dynamic is here to stay. FireEye estimates that 80-85% of its customers are migrating to the cloud.

For companies of any size or history, the cloud offers powerful benefits ranging from scalability, flexibility, enhanced collaboration, disaster recovery and reduced IT capital expenditures. There is a reason why cloud computing is now a massive business with revenues in the hundreds of billions.

So, how can you migrate to the cloud securely? As a starting point, you should ask your CIO or CTO how much of your data is now stored in the public cloud (hosted by third-party providers) versus the private cloud (operated by your own IT departments)?

Once you have a handle on the amount — and nature — of your data stored in the cloud, there are three key areas that warrant close consideration — governance, audit rights and breach rights.

GOVERNANCE

Migrating to the cloud does not mean abdicating responsibility for your data and systems. Rather, cybersecurity becomes a shared responsibility between the cloud provider and your company. Accordingly, it is crucial that the respective roles and responsibilities of vendor and customer are clearly defined. The primary tool for doing so is a "cloud service agreement." Where will your data be physically housed? If the cloud provider decides to move your data to another location, is there any obligation to notify you? Will your data be fully segregated, or isolated on separate servers, from the data of other customers? If this is arguably one of the most important contracts for your organization, has your general counsel, or outside counsel, reviewed it?

AUDIT RIGHTS

In the words of President Reagan, a good operating philosophy is "Trust but verify." The prevailing wisdom is that cloud providers offer greater security than individual companies. For most enterprises, that is likely accurate. In one form or another, however, customers should have the right to audit a cloud provider's security measures and system of controls either by reviewing independent assessments of the cloud provider or by conducting their own reviews.

BREACH RIGHTS

At a minimum, cloud providers should be required to provide prompt notice to affected clients in the event of a breach.

2. Spend Time on Patching

Most successful cyber attacks, including Wanna Cry, exploit vulnerabilities that were not patched with the latest software fixes.

The process of patching known vulnerabilities is something of an Achilles heel, particularly for large organizations with complex legacy IT environments. After software is installed at your company, software providers and outside IT experts regularly identify flaws or bugs that need to be patched. Commentators, and occasionally regulators, assert that failure to patch a known software vulnerability is akin to leaving your back door open for thieves to enter.

While certainly colorful, this metaphor does not take into account the complexity of the task. The process for patching software, which involves inserting and then testing code in your operating environment, is not simple. Moreover, both the volume and criticality of new patches identified every week by software providers and IT experts are rising exponentially. This is a frustrating combination for IT professionals.

WHAT SHOULD YOU DO?

First, get briefed on the volume and criticality of unpatched software vulnerabilities at your organization.

How many do you have? How many of these vulnerabilities have the highest criticality?

Second, figure out who has primary responsibility for applying the patches.

Is it managed at a corporate level or in individual business units?

Third, track and report to senior management on your progress.

A goal near zero, in our judgment, is simply not feasible. Rather, focus on establishing a sound protocol for prioritizing — and then steadily reducing — the overall volume of critical patches.

3. Rethink The Human Element

Despite all the technical jargon about Trojan horses, cryptoworms and botnets, human behavior lies at the core of any sound security strategy. Indeed, most successful corporate strategies require an equal measure of focus on people, processes, and technology.

The statistics are daunting. It has been reported that 91%[8] of ransomware infections reportedly start with an employee clicking on a spearphishing email, and 95% of all security incidents involve human error.[9]

WHAT SHOULD YOU DO?

First, think of creative ways to reinvent your employee training.

Today, IT staff at most companies attempt to raise employee awareness with repeated email campaigns. A sizeable percentage of employees – often between 10 percent and 30 percent - click on inappropriate attachments or links. Interestingly, fictitious LinkedIn job postings consistently receive the highest click rates! IT security staff then train the same employees a second time — and click rates remain stubbornly high.

Might gamification and a system of incentives, rather than penalties, change this dynamic? A handful of companies are experimenting with gamification tools that reward employees who spot spearphishing emails or social engineering attempts with Generation Y or Millenial titles like Ninja Level III Warrior.

Second, reduce your company's attack surface by disabling access to personal web mail from company computers.

Hackers are increasingly attempting to penetrate company networks through phishing attacks on the personal email accounts of employees. Because many personal email providers use encryption, it is difficult for companies to detect malicious code that may be entering company networks via this route. Accordingly, companies increasingly are precluding employees from accessing personal email accounts from corporate systems.

[8] "91% of Cyberattacks Start with a Phishing Email," by Steve Zurier. (Dec. 2016) (accessed at https://www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704?).

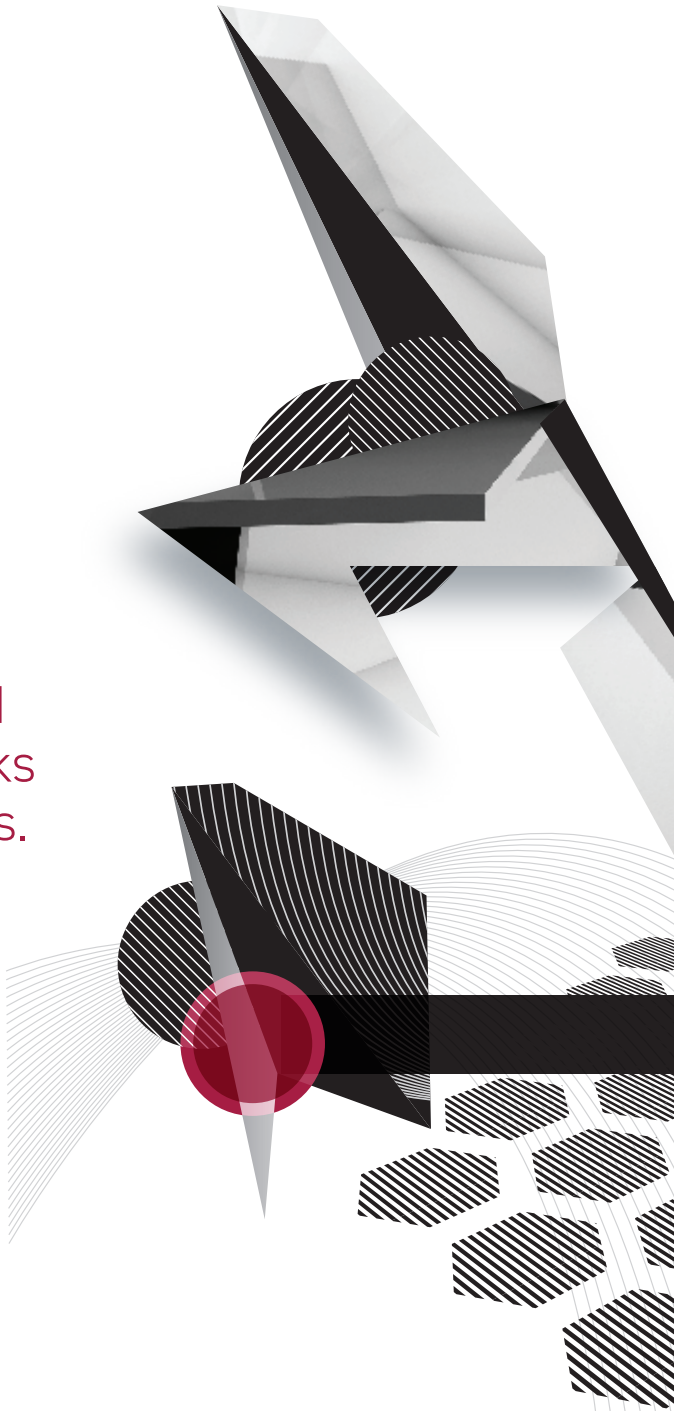
[9] "The Role of Human Error in Successful Cyber Attacks," by Fran Howarth. (Sept. 2014). (accessed at https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/).

4. Engage with the Government

Industry and government now need each other more than ever. Given the sophisticated foes that are attempting to penetrate both corporate and government networks, it serves all of our interests to lessen the tensions between the private and public sectors. As governments are going to play an increasingly active role in a company's compliance with cyber laws, take the time to reach out to key agencies.

Moreover, this should not be a one-sided discussion about what more industry alone should do. Rather, the business community should press governments to develop international norms regarding (1) the identification and prosecution of hackers and (2) the setting of limitations on targeting particularly critical resources like water systems or electric power supply. In traditional warfare, there are conventions that limit attacks, for example, on hospitals or the provision of humanitarian relief. While the task is complex, there must be greater levels of deterrence and boundaries in the digital domain. It is simply not realistic to expect private companies to stand alone in defending their networks against determined nation states.

Private companies cannot stand alone in defending their networks against determined nation states.



5. Plan, Plan, Plan

Eisenhower had it right. When preparing for battle, he said, "Plans are useless, but planning is indispensable."

People, particularly strong-willed executives, revert to form when under stress. Whatever dynamic exists within the members of a senior management team or between these executives and the board of directors will be put under severe strain at a time of crisis.

Accordingly, there is no substitute for conducting a mock cyber exercise. Senior business, IT, finance, legal, and communications executives should all be in the room together with outside forensic, communications, and legal advisers.

HERE ARE THREE CORE QUESTIONS THAT YOU SHOULD ASSUME WILL ARISE.

First, when do you possess enough information to make a public disclosure?

The typical dynamic that unfolds is that half the room will urge the CEO to get "in front of the story" and "control the narrative." The other half will say that not enough is known and more time is needed to conduct further analysis. When you do decide to communicate, do you include a specific number of records or individuals that you believe to be affected or do you simply state that a breach has occurred? To put it mildly, every step in this process is fraught with complexity and potential risk.

Second, when you become aware of a significant breach, do you immediately shut down your IT systems?

Your instincts and logic would say absolutely. Stop the bleeding. Given FireEye research that it typically takes 99 days – more than three months – before attackers are discovered and that hackers have built many entry and exit points during that latency period, this is not as simple of an analysis as one might assume.

Third, do you reach out affirmatively to law enforcement?

Many executives are hesitant to do so. One way to approach this analysis, however, is to think of two "Vs" - villain and victim. Companies that suffered breaches several years ago were often depicted as the villains. More recently, certain companies have been portrayed more as victims of sophisticated attacks launched by nation states. The question becomes whether engaging government authorities might result in a credible attribution of the attack to a nation state or a criminal prosecution of the hackers who launched the attack.

It behooves us to spend time thinking through these issues in a moment of quiet reflection rather than chaotic disruption.

A CALL TO ACTION

While the concepts of cybersecurity may be foreign for many executives and board members, protecting your company against risk is not. Great executives understand their limitations and leverage resources to fill the gaps. We will all be grappling with these issues for the balance of our careers.

ABOUT FIREEYE

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye minimizes the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 6,300 customers across 67 countries, including more than 40 percent of the Forbes Global 2000.

For more information, please visit contact **cyberrisk@fireeye.com**

ABOUT MARSH & MCLENNAN

Marsh & McLennan Companies (NYSE: MMC) is a global professional services firm offering clients advice and solutions in the areas of risk, strategy, and people. As one of the four operating companies, Marsh is a global leader in insurance broking and risk management. 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. With annual revenue of $13 billion and over 65,000 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.

For more information, please visit **www.marsh.com/us/services/cyber-risk.html**

If you would like any further information or to request an analysis of your cyber practices, please feel free to contact any of the executives from our two companies listed below.

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

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

Tom Fuhrman
Cybersecurity Consulting and Advisory Services
Marsh Risk Consulting
thomas.fuhrman@marsh.com
+ 703 731 8540

Thank you to our contributors:

FireEye

Peter Beck
Gavin Bradbury
Tony Cole
Christina Jasinski
Sandra Joyce
Tony Sapienza
Andrew Schmidt
Rich Stegina
Lynn Thorne
Lauren White

Marsh & McLennan

Devin Beresheim
Ronnie Brandes
Matthew McCabe
Bob Parisi
Tom Reagan
Inna Tsimerman
Steven Viña

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

www.FireEye.com

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 845 of the Forbes Global 2000.

FireEye®