LOOKING AHEAD:

CYBER SECURITY IN 2018

REPORT

CONTENTS

AN INTRODUCTION BY

Grady Summers

CHIEF TECHNOLOGY OFFICER

One of the greatest aspects of my job is that I get to interface with some of the brightest and most innovative minds in the security industry. As an added bonus, many of these people are from the first and second generation of analysts and researchers and incident responders, so their knowledge and expertise is based on a rich experience that dates as far back as when this whole industry was still referred to as "computer security".

Some of my colleagues, including FireEye CEO Kevin Mandia, were on the frontlines of security in the early to mid-1990s, and they remember when the game was primarily espionage – governments and militaries spying on one another. Many more remember how quickly the game changed a few short years later, when hackers started using Windows NT to carry out cyber crime. And even more remember when we started to see militaries pivot in the mid-2000s and begin hacking the private sector, a sign that the rules of engagement were starting to broaden.

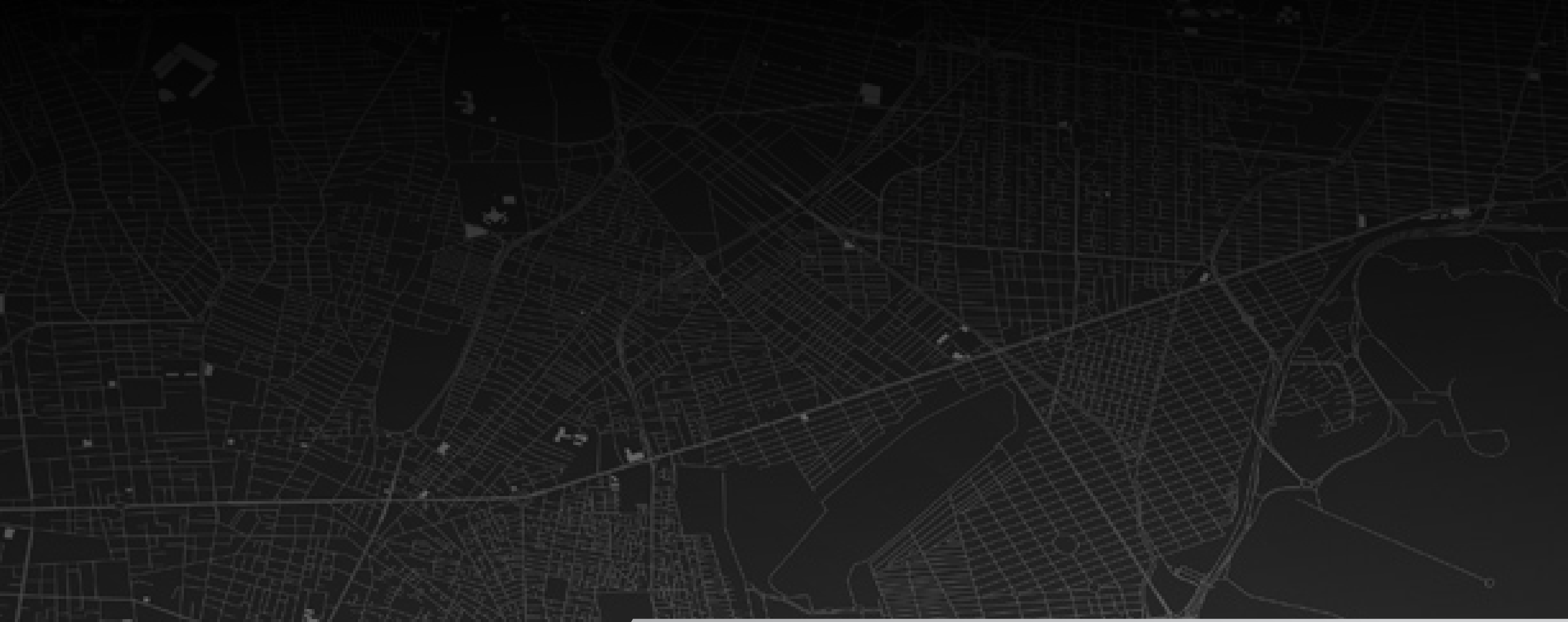
These individuals have experienced decades of evolving cyber security trends firsthand. They've lived through change, analyzed threat and attacker and technology advancements, and have come to understand it all in a way that makes their insights absolutely crucial as we begin discussions about what to expect in the new year.

This year's FireEye security predictions report, Looking Ahead: Cyber Security in 2018, features interviews that I conducted with CEO Kevin Mandia, CTO for Cloud Martin Holste, and CSO Steve Booth about what's to come in 2018. Following those conversations is a variety of insights provided by top experts on our FireEye iSIGHT Intelligence, Mandiant Consulting, and FireEye Labs teams. Then we get a little more specific as we dive into what lies ahead in the EMEA and Asia Pacific regions.

Kevin Mandia

CHIEF EXECUTIVE OFFICER

Predictions for 2018



As we enter a new year, what is top of mind for you?

I can't help but feel that it's a time of uncertainty, but it's also a time of opportunity. There are many challenges being hurled at cyber security practitioners. We have nations that aren't really stable in the rules of engagement. That's a big theme. We at FireEye have a skewed vantage – to some extent – since people don't really hire us to respond to breaches when they're five minutes behind the breach. The majority of breaches we respond to are state-sponsored, or state condoned.

So, we see it firsthand – the rules of engagement that modern nations had locked into from 1993 to 2014 do not exist anymore. Russia has deviated from it. North Korea, Iran and other nations, as well. You can see them testing the waters: "How far is too far? How far can we go?" The challenge is, there have been no risks or repercussions yet. So, every nation is developing a modern offensive capability, and there are no accepted rules of engagement. There is no one nation, five nations, or collection of 20 nations that are holding all nations accountable to abide by any rules of engagement. We need to have some kind of barrier put up, and I'm convinced we will sort it out.

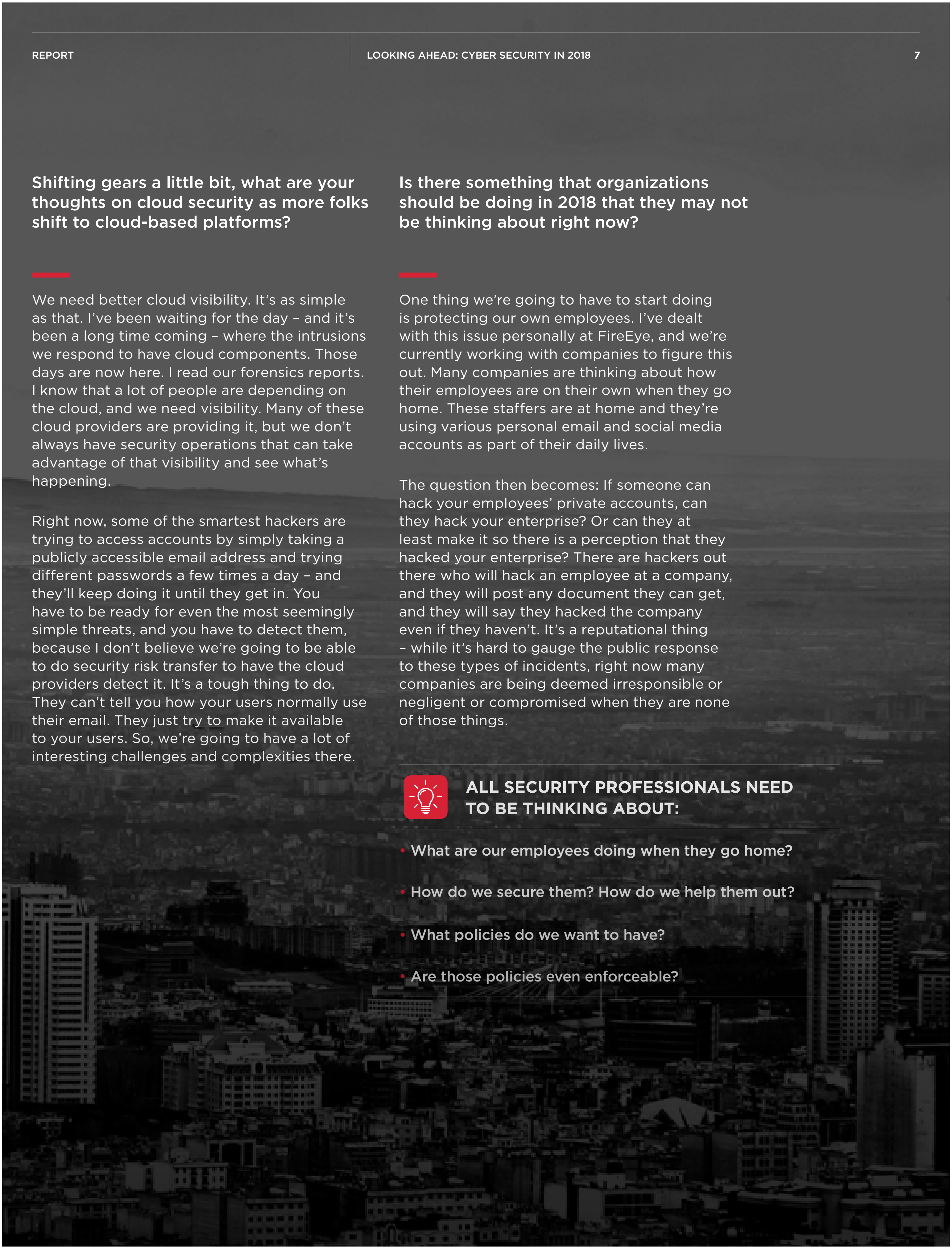
You said there is a bunch of challenges being hurled at cyber security practitioners – what else?

Another thing we have to do is change the game on identity. The idea that you can get someone's date of birth, and their Social Security number or state ID number, and steal their identity and do fraudulent tax refunds, or try to get a loan or credit card – that has to change. Now, you're seeing a lot of modern nations and sovereign nations start doing digital identification. This has to happen. Otherwise, every five months, we're going to have a huge breach, and all we are going to do is go to the victim companies – companies that are doing the best they can do to protect themselves, companies that employ 10,000 people that depend on that job – and we're going to crucify them. And that's all that will happen time and time again, so we have to figure out a better way to do identity.

Also, we're going to have to deal with international privacy issues. You look at this world of people who have essentially been prisoners of geography for 10,000 years, and suddenly we're all connected globally. We're international. Companies can connect to each other and work globally more than ever before based on the advances in communications we have made. As a result, we're going to have to fix some privacy issues that stem from there.

Speaking of international challenges, what nation-state activity do you expect in 2018?

We talk about Russia, we talk about China, we talk about North Korea – for me, I've got my eyes on Iran. In 2017, Iran really started acting at scale, and I think to myself, "Just how big is that scale?" We don't know if we are seeing five percent of Iran's activities, or 90 percent – although I'm guessing it's closer to five percent – but they're operating at a scale where, for the first time in my career, I'm not convinced we're responding more to Russia or China. It feels to me that the majority of the actors we're responding to right now are hosted in Iran, and they are state sponsored. Recently we did a report on APT33, a threat group out of Iran. They're primarily targeting the kingdom of Saudi Arabia, the United States, and Israel. Those nations tend to pop up on Iran's radar when it comes to targeting. It's game on for them.



Shifting gears a little bit, what are your thoughts on cloud security as more folks shift to cloud-based platforms?

We need better cloud visibility. It's as simple as that. I've been waiting for the day – and it's been a long time coming – where the intrusions we respond to have cloud components. Those days are now here. I read our forensics reports. I know that a lot of people are depending on the cloud, and we need visibility. Many of these cloud providers are providing it, but we don't always have security operations that can take advantage of that visibility and see what's happening.

Right now, some of the smartest hackers are trying to access accounts by simply taking a publicly accessible email address and trying different passwords a few times a day – and they'll keep doing it until they get in. You have to be ready for even the most seemingly simple threats, and you have to detect them, because I don't believe we're going to be able to do security risk transfer to have the cloud providers detect it. It's a tough thing to do. They can't tell you how your users normally use their email. They just try to make it available to your users. So, we're going to have a lot of interesting challenges and complexities there.

Is there something that organizations should be doing in 2018 that they may not be thinking about right now?

One thing we're going to have to start doing is protecting our own employees. I've dealt with this issue personally at FireEye, and we're currently working with companies to figure this out. Many companies are thinking about how their employees are on their own when they go home. These staffers are at home and they're using various personal email and social media accounts as part of their daily lives.

The question then becomes: If someone can hack your employees' private accounts, can they hack your enterprise? Or can they at least make it so there is a perception that they hacked your enterprise? There are hackers out there who will hack an employee at a company, and they will post any document they can get, and they will say they hacked the company even if they haven't. It's a reputational thing – while it's hard to gauge the public response to these types of incidents, right now many companies are being deemed irresponsible or negligent or compromised when they are none of those things.

ALL SECURITY PROFESSIONALS NEED TO BE THINKING ABOUT:

- What are our employees doing when they go home?
- How do we secure them? How do we help them out?
- What policies do we want to have?
- Are those policies even enforceable?

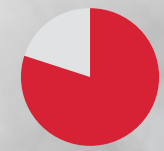
Martin Holste

CHIEF TECHNOLOGY OFFICER FOR CLOUD

Predictions for 2018

80%-85%

THE PERCENTAGE OF OUR CUSTOMERS MOVING TO CLOUD



What cloud trends do you expect to see as we move into 2018?

This past year was something of a turning point for public cloud adoption – not just with regard to traditional public cloud providers such as Amazon and Azure, but also with software as a service. This means people are really starting to put critical data into the cloud. We saw that some of the largest companies are starting some really major cloud initiatives where they may have one or two absolutely critical applications that they've successfully migrated.

In 2018, I think the floodgates are really going to open as organizations see and feel the lower costs for running in cloud, and that they can move more quickly. Those kinds of things will continue to encourage cloud adoption for the majority of businesses. However, there are a few sectors where they're still – for various reasons – not as interested in the cloud, but I would say between 80 percent to 85 percent of our customers are moving significant workloads.

What does that mean for attackers?

That means attackers are going to follow that data into the cloud, regardless of what the data is – be it credit cards or medical records or something else. Attackers won't say, "Well, I'm not really interested in doing cloud stuff. I'm going to stick with on-prem." They'll certainly move to trying to get to the IP that's in the cloud.

On one hand, stuff that goes into the cloud is generally harder to hack. You can most certainly exploit things in the cloud; however, it's all newer technology, which means you don't have as many instances of older, more vulnerable things running. It's a little bit easier to keep an eye on from an asset-management standpoint. On the flipside, if at any point somebody gets phished, suddenly credentials can be much more powerful than they used to be. So, keeping track of who is logging in and from where has never been more important than it is today. Making sure that you have full visibility into all the actions that are occurring starts to move some of the traditional defenses from things like exploits into a little bit more of the business logic layer. Still, vulnerable is vulnerable, so ensure everything running in the cloud is secure.

Do you expect to see more nation-state activity targeting the public cloud?

We've certainly had no lack of drama in geopolitics in 2017, so I think that will be even more prevalent than it has been as we move into 2018. I think one problem is that nation-states are so good at phishing, and we will see that take its effect on cloud operations. Security is all about people, and people are often the weakest element. I don't blame the victims – this happens to everybody. There are things you can do to try to reduce the amount of damage that happens with leaked credentials, but you shouldn't pretend like you're always going be able to prevent that from occurring.

Do you see any particular industries that will be more targeted in 2018 versus others?

I don't think the cloud is going to affect specific industries that are targeted. I think that there is going to be essentially the same threat that existed before. I think the cloud just offers a different way to deliver that same threat to a victim, and it represents an evolution of the overall game plan of attackers. I don't think that what they're choosing to attack is changing because of the cloud itself, so don't expect too much variance in who is being targeted as we move into 2018.

That said, I think that if there's one industry that's going to see an uptick in threat activity, it's going to be entertainment – just because we have already seen a fair amount of targeting there and the reasons for that targeting aren't going away. The entertainment industry is suddenly realizing that they really need to worry about security.

> “I think the cloud just offers a different way to deliver that same threat to a victim, and it represents an evolution of the overall game plan of attackers.”
>
> **Martin Holste**
> CTO for Cloud
> FireEye

What should organizations be doing in 2018, as they move to the public cloud, to stay in front of threats and vulnerabilities?

First, organizations must know everything that’s going on. What I mean is, they must have situational awareness, and visibility’s the name of the game. Incident responders should be able to identify all key assets. Do you have data in Dropbox? What data do you have in Salesforce? These days, it is extremely rare for organizations to have this level of visibility – to have a window into all the different places where their critical data sits. This is a bad sign.

Second, organizations must be natively protecting their cloud environments. That includes making sure the organization has hooks into things such as artifacts that are being transmitted. For instance, do you have places where documents are getting uploaded and then going into your back office? That’s a good place to ensure there is some high-grade detection, beyond an antivirus scanner. Because you essentially have unauthenticated input going directly into the key parts of your organization.

In the public cloud, visibility in some ways can be easier because there's so much native visibility built into cloud environments. But organizations have to be doing something with it, right?

Right. Each cloud provider will sort of give you their own specific console so you can go and ask really specific questions. The problem is that asking a SOC or an incident responder to log in to 30 different consoles is too much. You need to make sure you can bring all that back into one place so they can say, “All right, show me everywhere that this user logged in,” or, “Show me all the logins that we’ve seen from this time period.”

And that’s just the beginning. You then want to be able to say, “What are the anomalous things that're occurring across all of this stuff?” And being able to correlate all those things is really important as well. Just saying that, “Okay, well, I have an administrator login, so I can go figure out who logged in recently on this one cloud provider” – that's not going to cut it day-in and day-out for running a SOC, or for doing an incident response. There are just too many things to triage and it’s going to take too long. Moreover, you are not going to be able to do any of what I would call the “real security” of it, which is to actually notice when those sorts of anomalous things occur across providers or across time – the things that an individual cloud provider won’t build in directly.

What do you see in terms of innovation for defenders of public cloud environments in 2018? Anything new coming, or anything that organizations should be taking advantage of?

Following up the previous question, the first thing is being able to pull all that data into one place. We've been working on our own FireEye products to be able to do these types of tasks. Next is being able to integrate into those native platforms to make sure that organizations don't have to sort of bolt on their cloud security, and that it’s all directly working with the cloud provider’s native hooks. And as such, we have products coming out that will accommodate that need as well.

Steve Booth

CHIEF SECURITY OFFICER

Predictions for 2018

Steve, you're tasked with defending, of all companies, a cyber security company. I feel that's one of the toughest jobs in the world. That said, let's just start with a general question: What do you think the threat landscape will look like in 2018?

I'm sure there's going be yet another round of fun, new, interesting attacks, but I think the uglier ones are going to be modified versions of current attacks. For instance, for attacks targeting employees, first it was phishing and then it was spear phishing. In 2018, we'll be seeing more attacks targeting social media accounts and more attacks targeting personal email accounts. This is where organizations could get into trouble because, as a company, they may not even know that have to defend against attacks targeting those personal accounts.

Compromising employees to cause damage – there are all kinds of other new and creative ways of doing that. We're working on something right now that gets into malicious publishing of applications, where an employee clicks "Yes" on their phone just once and now they have a malicious app that can do SAML assertions as them.

The other side of it is that we always live sort of the hygiene side of things, and that's important, but the world is more complex. There could be 800 different places you can set permissions – or "mis-set" permissions – using a popular platform such as Amazon, for example. Any single one of those platforms can become an attack surface.

It seems we are observing more groups using techniques traditionally associated with other groups – basically, threat actors are borrowing and stealing the best techniques out there...

Yes, that's right. And sometimes they'll even just buy the technology. So, either they are acquiring the skills based on what they're learning from certain individuals or reading from various message boards, or they are just saying, "Forget it, why exert the effort? I'll just go buy some commercially available piece of malware and have at it."

Speaking of threat groups, what about nation-state threat activity in 2018?

From the nation-state activity that we see and that we see our customers coming up against, we've observed that these actors are not just sticking to traditional espionage. Sure, there is a sizable chunk of APT groups that literally have to fund their country's government – groups that are looking to steal military technology, for example – but that is just part of it. Now you have nation-state adversaries targeting supply chain and more.

The other part of it that ends up being particularly interesting for me is that there are no norms for this – there are no rules of engagement. If a nation were to take a bunch of soldiers and steal money from the banks of an adversary, that would be an act of war. However, if they do it with computers, it's not. And then you're simply left asking, "Is it not an act of war, or has it simply not been declared an act of war yet?"

Should any specific industry be on high alert in 2018 that perhaps hasn't been in the past?

Pretty much every industry needs to be on high alert these days. The better way to ask that question would be, "Name an industry you think is safe." A few years ago, you may have said, "Well, they only generate power; what could anybody ever want from them?" But now everyone is talking about the energy industry. Or you may hear from a company that, "We only make locomotives." The truth is that there are petabytes of data created on that locomotive, and someone out there can benefit from access to it. It's not even just a matter of destruction or theft – some attackers may want to manipulate the data, some may want to just embarrass the organization, and some may want to affect business. With that thinking, any company can come in the crosshairs of attackers.

> "To stay ahead of threats and minimize risk, we need to focus on the current wars we're fighting – not the battles we've already lost – and keep innovating at the speed of or faster than attackers."
>
> **Steve Booth**
> CSO
> FireEye

What should organizations be doing in 2018 to stay ahead of these threats?

The answer has always been to get the job done for real. There is the basic upkeep and hygiene and those kinds of things, but that alone won't stop the determined attacker. Unfortunately, we see more organizations submitting to that mentality: "Why bother? They're going to get in." We can't have that mindset. To stay ahead of threats and minimize risk, we need to focus on the current wars we're fighting – not the battles we've already lost – and keep innovating at the speed of or faster than attackers.

Internally, in my group, we have ended up with this kind of maniacal focus on: "What are the things we should abandon and put truly zero security time on?" For instance, I don't have any conversations with my server group telling them what they should patch this month. That would be a waste of security time. My teams knows what they have to patch. They have their jobs and they have to get their jobs done – and they do get them done.

Shifting gears a little bit to regulation. I get asked all the time about GDPR. How do you see that changing anything? And do you expect any other changes in the security and regulatory nexus?

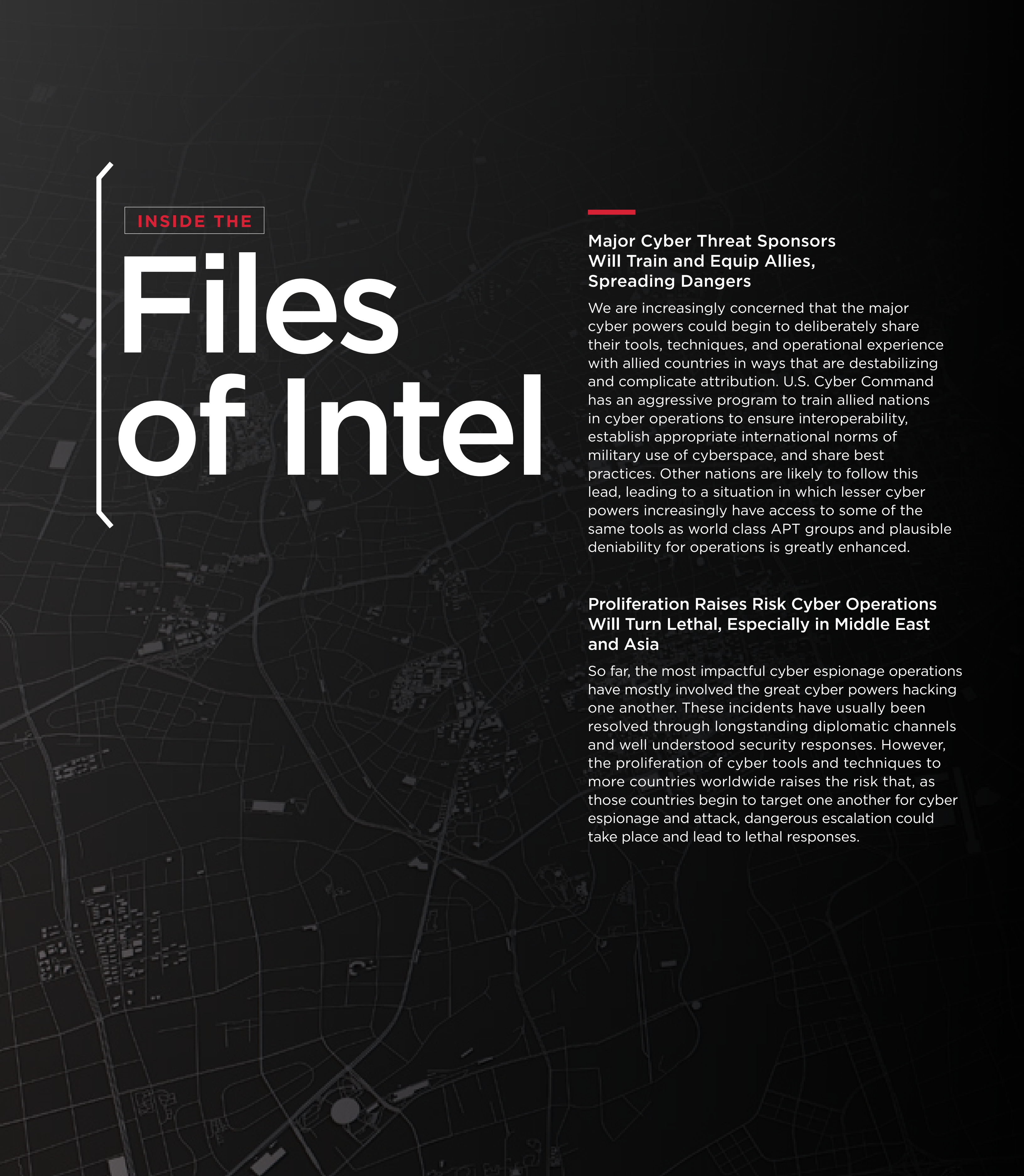
One of the obvious changes is that everybody seems to have their own regulation. They have them not only per country or per region, but also per state. There is even a per industry inside individual states. GDPR (General Data Protection Regulation) is interesting because it does change the rules quite a bit. Some folks are onboard and others not so much. I think GDPR has the potential to become similar to a Sarbanes-Oxley, although perhaps without the freaking out. You go through and you do all of the assessments, privacy impact analysis, and those kinds of things. I think GDPR is really going to get down to how people become compliant. As in, do you just sort of have one figurehead data protection officer that covers everything? Or do you have one per business unit, or per product silo, in order to do it for real? Some of this stuff hasn't been tested in court yet, so it will be interesting to see how it all turns out.

FireEye operates one of the largest private cyber intelligence gathering operations in the world.

We have a comprehensive view of adversaries that is comprised of victim intelligence from our Mandiant investigations, machine generated intelligence from our global MVX cloud, and adversary intelligence from our FireEye iSIGHT analysts deployed around the world.

The following predictions come from top experts on our FireEye iSIGHT Intelligence, Mandiant, and FireEye Labs teams.

Mandiant is a leader in helping organizations respond to and proactively protect against advanced cyber security threats. The FireEye iSIGHT Intelligence team produces actionable intelligence that arms global enterprises with rich contextual information about the motivation and intent of adversaries, their campaigns and technical indicators, the malware they use and the vulnerabilities they exploit. And FireEye Labs is the threat research and analysis division of FireEye that continuously monitors and analyzes threats detected by millions of network and endpoint sensors deployed across dozens of countries.



INSIDE THE Files of Intel

Major Cyber Threat Sponsors Will Train and Equip Allies, Spreading Dangers

We are increasingly concerned that the major cyber powers could begin to deliberately share their tools, techniques, and operational experience with allied countries in ways that are destabilizing and complicate attribution. U.S. Cyber Command has an aggressive program to train allied nations in cyber operations to ensure interoperability, establish appropriate international norms of military use of cyberspace, and share best practices. Other nations are likely to follow this lead, leading to a situation in which lesser cyber powers increasingly have access to some of the same tools as world class APT groups and plausible deniability for operations is greatly enhanced.

Proliferation Raises Risk Cyber Operations Will Turn Lethal, Especially in Middle East and Asia

So far, the most impactful cyber espionage operations have mostly involved the great cyber powers hacking one another. These incidents have usually been resolved through longstanding diplomatic channels and well understood security responses. However, the proliferation of cyber tools and techniques to more countries worldwide raises the risk that, as those countries begin to target one another for cyber espionage and attack, dangerous escalation could take place and lead to lethal responses.

Chinese Economic Cyber Espionage Threat Will Continue to Change Shape While Diplomatic Agreement Holds

From our vantage point, it appears that the Chinese Government has complied with the terms of the September 2015 “Xi Agreement” to cease using its state-backed hackers to steal U.S. intellectual property for commercial purposes. The Trump Administration renewed this deal, further indicating that Beijing is not in large-scale violation of the agreement. However, since that time other forms of espionage – targeting both U.S. and Asian government networks – and collection of business intelligence on the activities of U.S. companies has increased. Additionally, Chinese groups are in the midst of an ongoing surge of cyber espionage campaigns targeting U.S. businesses that provide services to other businesses, such as cloud providers or law firms, probably to enable Beijing to collect intelligence on a wide variety of targets with less chance of discovery.

Because China has been successful gaining access to wide swaths of U.S. data – telecommunications, healthcare records, business-to-business services, etc. – we assess they may be willing and able to violate the Xi Agreement on select, high priority cases while minimizing the risk of diplomatic blowback. Already we have observed some groups preparing what could be operations targeting revolutionary technologies, such as artificial intelligence and advanced batteries, which would provide such an extreme economic and military advantage to whichever country takes the lead in those fields that Beijing would risk upsetting the current status quo in cyber operations. There has been no evidence of such theft in other high priority scientific fields, such as genetics and biotechnology, since the Xi Agreement was reached, indicating that such operations by China are probably still in the preparatory phase or being conducted on a small scale.

Targeting Inherent Trust in the Software Supply Chain

Malware authors are increasingly taking advantage of inherent trust between users and software providers. Users inherently trust software developers to provide updates for their products that would add new functionalities or fix security bugs, and they don’t expect the updates to be tainted with malicious code. In supply chain attacks, cyber threat groups target the build servers, update servers and other parts of development environment. The hackers can then inject malware into software updates and software releases, thus potentially infecting users through trusted official software distribution channels.

In 2017, FireEye iSIGHT Intelligence observed at least five cases of advanced threat actors compromising software providers for follow-on intrusions into targets of interest. While targeting trusted partners – such as law firms or accounting firms – has long been a favored approach by some cyber espionage groups, this activity represents an expansion that might be more difficult to detect. Ensuring trusted partners employ resilient and proactive cyber security practices will assist in mitigating this business risk.

SEVERAL OF THE MOST ECONOMICALLY DAMAGING CYBER ATTACKS OF THE PAST FEW YEARS

have been provoked by Western or U.S.-led sanctions, and we expect many cyber powers in the future to respond to newly imposed trade and economic sanctions with cyber attacks targeting U.S. companies. Some countries targeted for Western sanctions, such as Russia and North Korea, have demonstrated that they can respond to such actions with cyber attacks that potentially pose a systemic threat to the global economy.

WE EXPECT SOME SMALLER COUNTRIES,

eager to bolster their control over information and public opinion, will learn from their larger counterparts in conducting offensive cyber sovereignty operations to achieve their goals. So far, the international community's lack of coordinated or meaningful responses to offensive cyber sovereignty may embolden these smaller actors into gaining outsize benefits for a comparatively low cost. Smaller countries that perceive significant threats to their cyber sovereignty may take more aggressive action in the form of Virtual Private Network (VPN) destabilization, border gateway protocol (BGP) hijacking, attacks on ICANN and the DNS, or malicious manipulation of social media accounts to steer narratives.

ON ASSIGNMENT WITH

Mandiant Consulting

Increased Activity from Nation-States and APT Groups

Given the current political landscape, we expect to see increased cyber offensive operations from North Korea. We also expect to see increased activity from China, Russia, and Iran. Iran will be recognized as a country with a broad offensive capability and will continue destructive operations in the Middle East, but operators may moonlight and conduct disruptive operations (extortion and/or public shaming, for example) in the Western world. Russia will continue to engage in offensive operations against countries that they are in conflict with, including Ukraine. China may become more active as it attempts to spread its influence in Asia, Africa, and Latin America.

The changing geopolitical situation in the Asia Pacific region will see Chinese APT groups shift their focus, instead going after countries and groups that are seen as a threat to China's access to and influence over global markets. India and Hong Kong are likely to attract maximum activity from Chinese APT groups. Additionally, we observed an increase in non-Chinese and non-Russian APT groups in 2017, and expect to discover more in 2018.

A Shortage of Skilled Workers Paves the Way for Automation

Attacks will continue to be effective through an increase in sophistication, but they will also be successful due to the challenges organizations face in recruiting and retaining skilled cyber professionals. These skill shortages are partly to blame when it comes to recent widespread attacks that leveraged unpatched applications and operating systems.

With no foreseeable end to this skills shortage as we enter 2018, the security industry will begin to see more automation, machine learning, and artificial intelligence used to combat cyber attacks. The most sophisticated organizations have automated intelligence sharing, and are putting those intelligence feeds directly into security controls without a human ever touching a keyboard. We will see this type of automation spread to the masses next year, increasing preventative controls and decreasing the time to detect attacks.

New Regulations Will Help Organizations Better Protect Data

Breaches at major organizations are attracting the attention of regulators and legislators around the globe. The recently introduced General Data Protection Regulation (GDPR) and New York State Department of Financial Services (DFS) regulations have extremely aggressive notification requirements – 72 hours and 48 hours, respectively. To give these new laws some teeth, we may see fines being issued for failure to notify. Meanwhile, other countries such as China, Singapore, and Canada are also racing towards implementing their own laws to protect their citizens and critical infrastructure.

GDPR in particular will be a major topic of discussion throughout 2018, as it applies to all organizations that process EU data. GDPR stands to become the de facto worldwide standard for data privacy, and organizations should see it as an opportunity to focus the board's mind on privacy and information security. Ultimately, GDPR should help organizations understand what data they possess, where that data is located, why they have the data, and how it is being protected.

72
HOURS
GDPR

48
HOURS
DFS

More Organizations Will Test Their Capabilities and Perform Security Assessments to Minimize Potential Damages

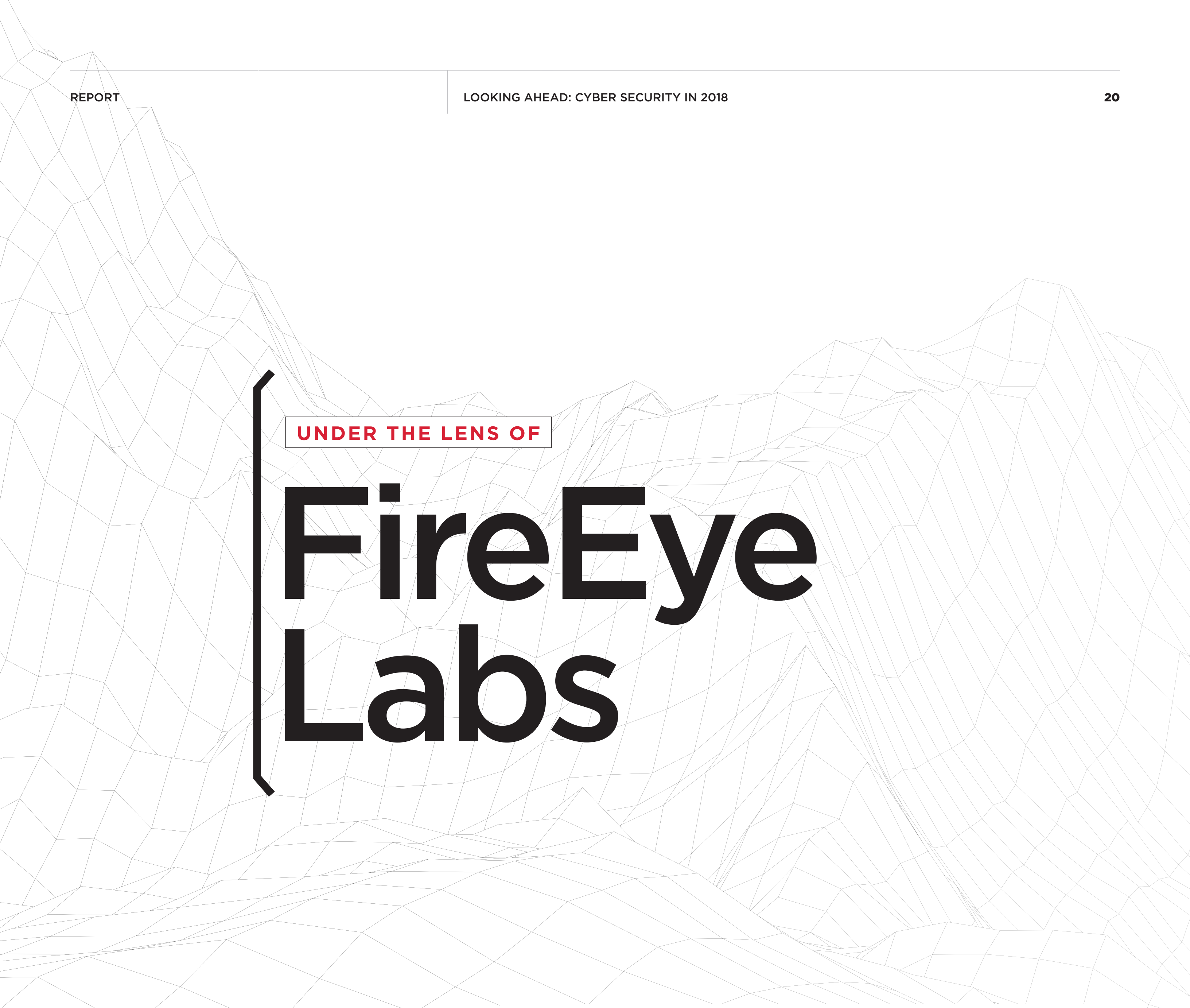
In 2018, organizations will spend more time thinking about and testing their ability to detect security incidents in their environment with their tools. This will lead to the development of actionable plans to quickly respond to and contain security incidents. The ability to respond to a security incident in hours or days, instead of weeks or months, translates to whether the organization has a small issue or a large data breach that could eventually become public.

These organizations will also perform regular security assessments to identify weaknesses and maintain a strong security posture. Compromise assessments ensure a clean environment and red team engagements for security operations help improve visibility and speed. Organizations will focus on automating lower priority alerts and will use skilled resources to fix the harder problems. These organizations will implement overlapping controls to secure their most critical systems and data.

IN 2018, we may see an increase in ransom and extortion attacks relating to GDPR (and perhaps other regulations) as attackers seek to capitalize on a potential fear of large fines. An example of this would be an attacker compromising an organization – or even tricking the organization into believing they have been compromised – and promising to keep the breach from going public for the right price.

Threat actors will continue to set their sights on the energy industry and industrial control systems (ICS) in 2018. Financial threat groups are more likely to target the retail and hospitality industries. The technology industry (especially cloud providers), IT service providers, and professional services firms (law firms, accountings/audit firms) will also continue to be targeted due to the amount of concentrated data they hold and, in some cases, the amount of access they have to their clients' environments.

Ransomware distribution has risen dramatically in the past few years, and recent attacks leveraging major vulnerabilities show that attackers are still finding success with the file and system locking malware. We expect to see continued use of ransomware in 2018, especially as administrators are slow to patch and update their systems. Additionally, ransomware will continue to be prolific as long as the ransomware authors continue to find the business lucrative.



UNDER THE LENS OF

FireEye Labs

Increase in Cloud-based Attacks and Evasion Techniques

In recent years, we have seen an uptick in security technologies and infrastructure using cloud services such as Amazon Web Services (AWS), Azure, and more. We have also seen attackers leveraging these cloud services for various purposes, including to host URLs for phishing and to distribute malware. Hosting on known file sharing services and leveraging cloud service providers is useful for attackers because it helps them bypass the initial domain reputation checks performed by most security engines.

Additionally, with cloud offerings becoming more prominent every day, we expect attackers will become more aware of cloud environments and, thus, adapt their behaviors accordingly (traditionally, we have seen malware binaries detecting virtual environments). For defenders, this means either restricting downloads from cloud service provider IP addresses or limiting downloads.

Increase in Internet of Things Attacks by Exploiting Vulnerabilities

We saw many Internet of Things (IoT) attacks in 2017 beyond those involving the popular Mirai, a malware that corralled CCTV cameras and routers into a large botnet by exploiting weak passwords. One such example is Reaper, a malware that exploited vulnerabilities in IoT devices to gain access and spread itself. The end result of these types of attacks is that threat actors can enlist millions of compromised IoT devices to drive largescale attacks, including the distributed denial-of-service (DDoS) attacks that commonly disrupt and take down website, gaming, and other internet services.

With the number of connected devices constantly growing, it is highly likely that attackers will move quickly to exploit newly identified vulnerabilities. This coming year will likely bring a new level of sophistication in IoT-based botnets, and we may also see attackers targeting certain IoT devices (smart refrigerators and home automation, for example) with ransomware. Additionally, we also expect to see more attacks targeting IoT devices at the enterprise level.

Multi-vector Phishing Attacks Involving a Variety of Evasion Techniques

Traditional phishing attacks leveraging PDF files typically involve a PDF attachment containing an embedded URL. When the recipient clicks on the URL in the PDF, they are taken to a phishing website. Currently, many email technologies are able to identify the URLs embedded within a PDF file, extract it, and send it along for further analysis. However, attackers are adapting. One example of this is using an original PDF attachment containing a link to another PDF. This second PDF file is what contains the URL to the phishing page, and could lead to the user being compromised.

Other techniques being used by attackers include URL evasions. We have observed attackers generating URLs that use encoding (hex-based, for example) designed to evade pre-filters used in URL reputation technologies. Another emerging trend is the use of non-HTTP protocols. Phishing attacks are moving from HTTP to non-HTTP protocols such as FTP, which can also be used to evade security technologies. We expect this trend will grow throughout 2018 as it is used in more targeted attacks.

⬆ 186%

We have seen an uptick in use of 'HTTPS' domains for phishing attacks, and we expect that to continue throughout 2018. From early August 2017 to early November 2017, we observed a 186 percent increase in phishing attacks involving HTTPS. These domains could either be legitimate websites that have been compromised for use in attacks (such as WordPress websites), or they could be newly registered domains, or shortened URLs redirecting to phishing websites.

⬆

More recently, we have observed attacks involving vulnerabilities in cryptographic protocols and algorithms, and this trend will most likely continue into next year. We expect to see an increase in the number of weaknesses disclosed in widely used cryptographic protocols and algorithms – primarily SSL/TLS – as we enter 2018.

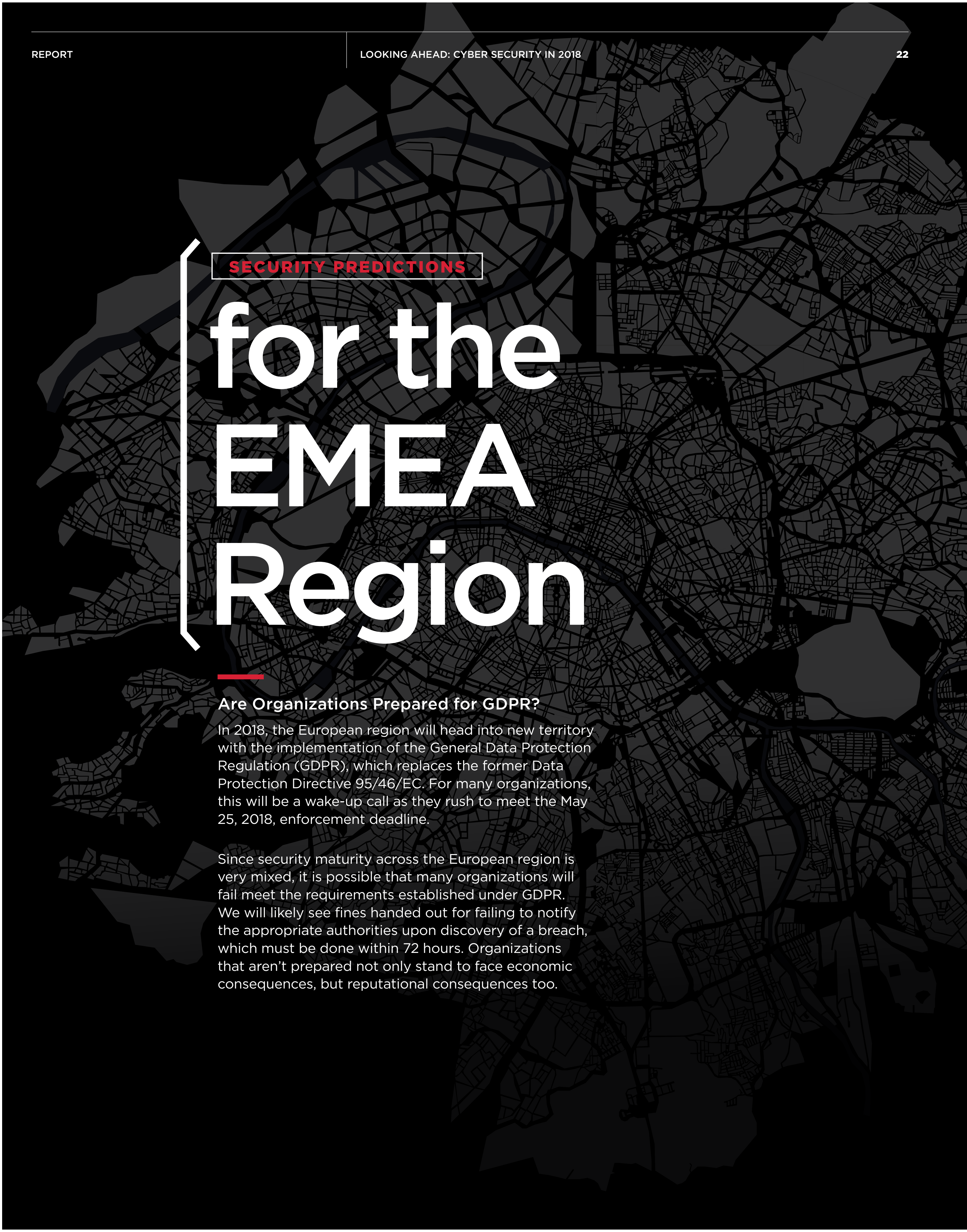
⬆

We expect to see some of the old standards returning in 2018. Social engineering attacks other than just phishing will continue to be used to deliver malware. Of note, we expect attackers will find new methods of luring users through malvertising. Considering the geopolitical climate, we can also expect information theft to continue through the use of surveillance software, as well as via attacks leveraging non-public exploits. Additionally, we expect to see more worms and other commodity malware that can spread rapidly.

⬆

UPDATE

Threat actors will continue to leverage unpatched vulnerabilities in their attacks. Acting quickly, they will carry out attacks involving high-impact vulnerabilities against targets that they expect will not have updated their systems and networks. Organizations and users alike must get in the habit of applying patches quickly, including application and network layer updates. New enterprise solutions should be deployed in ways that will make them more rapidly adaptable for any changes, and easy for security teams to update as needed.



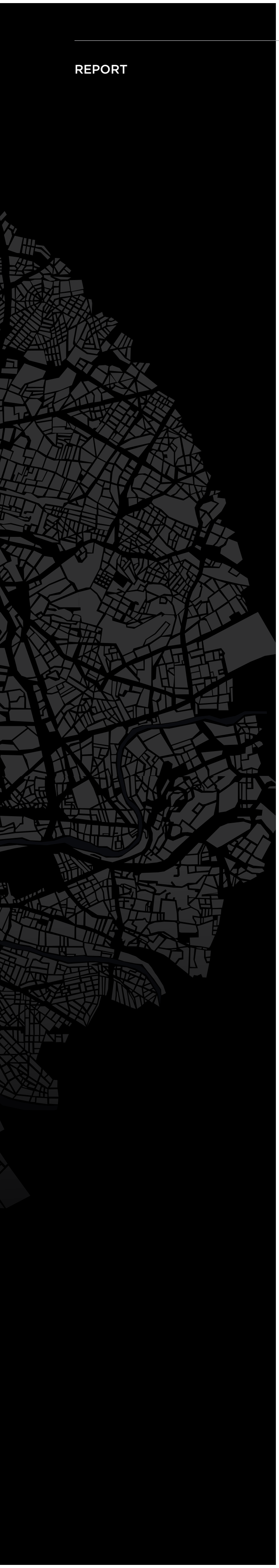
SECURITY PREDICTIONS

for the EMEA Region

Are Organizations Prepared for GDPR?

In 2018, the European region will head into new territory with the implementation of the General Data Protection Regulation (GDPR), which replaces the former Data Protection Directive 95/46/EC. For many organizations, this will be a wake-up call as they rush to meet the May 25, 2018, enforcement deadline.

Since security maturity across the European region is very mixed, it is possible that many organizations will fail meet the requirements established under GDPR. We will likely see fines handed out for failing to notify the appropriate authorities upon discovery of a breach, which must be done within 72 hours. Organizations that aren't prepared not only stand to face economic consequences, but reputational consequences too.



Politically Motivated Cyber Activity

The ability to quickly get messages across in cyberspace will fuel more politically motivated cyber activity across Europe in 2018. Publishing fake news, leaks and other data could help shift the political climate in some regions, thus leading to certain candidates and political parties being unfairly favored over others.

In 2017, we saw reports of cyber attacks occurring up to and during some of the elections taking place throughout Europe, particularly in France and Germany. More recently there have been indications of information operations carried out in the Southern European region, with a focus on the tension in Spain and the Catalonia region. Also, in the last half of 2017, we observed continued targeting of alliances such as NATO and the EU.

We expect these types of activities to continue into 2018 as tensions grow in the region and in neighboring countries. Next year there will be several elections across the EMEA region that we expect will be targeted by threat groups carrying out information operations and other politically motivated cyber attacks.

Increased Cyber Maturity Leads to More Sophisticated Attacks

The offensive capabilities of nation-states in EMEA were considered mixed throughout most of 2017, but nearing the end of the year we began observing these nation-states trying to mature their offensive capabilities through the purchase of zero-day exploits from lawful intercept companies. We expect this trend to continue into 2018, fueling more offensive maturity across Europe. Additionally, since history has shown that nation-states will eventually lose their tools (either because of leaks, poor operational security or compromises), we will likely see more groups other than nation-states beginning to mature, particularly cyber criminals looking to make a quick buck.

“You are Not an Island” – Everybody is Connected

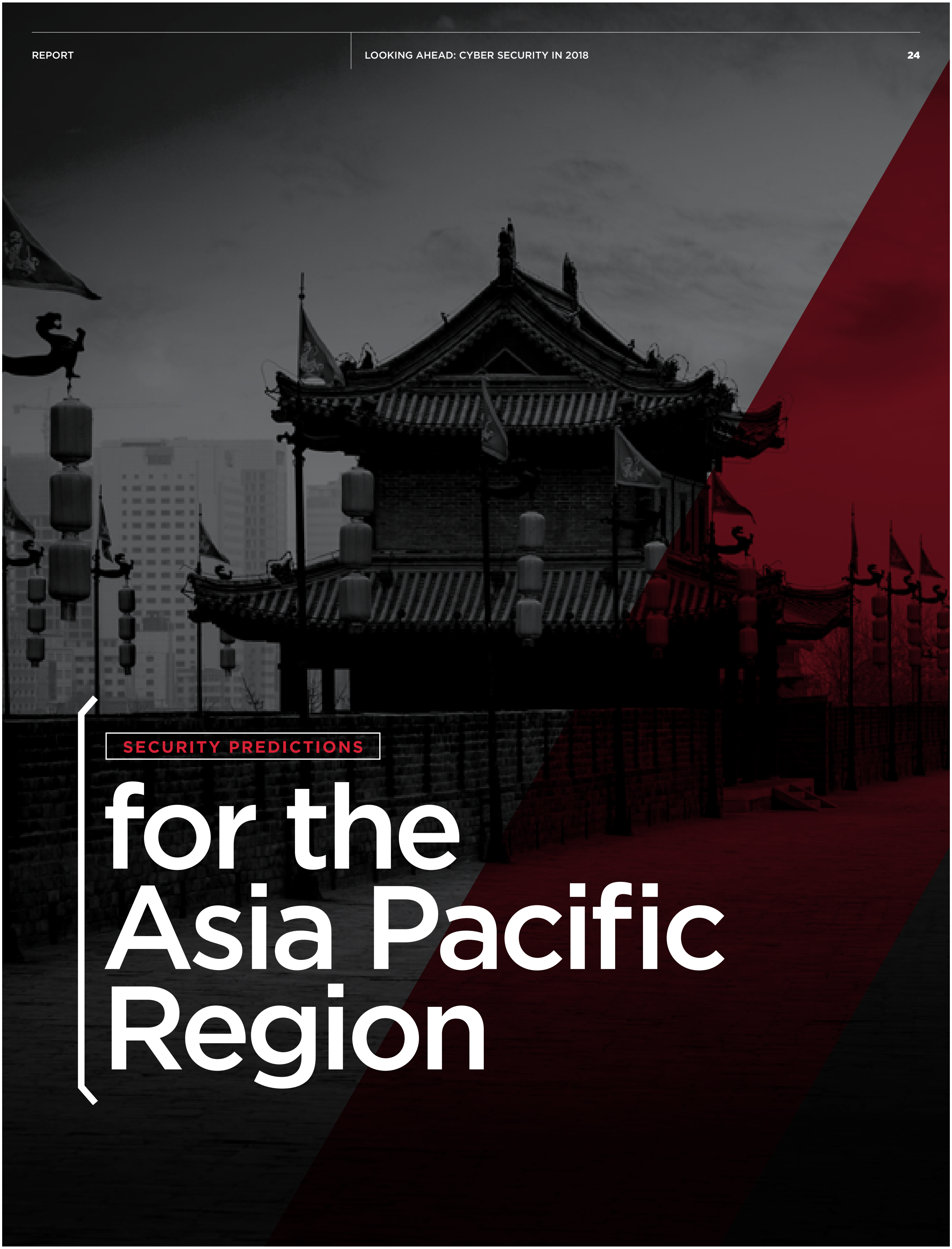
Recent widespread attacks such as EternalPetya (NotPetya), WannaCry and BADRABBIT have taught organizations that even if they are not a direct target, they might be affected indirectly due to connected infrastructure.

Of note, EternalPetya was primarily targeting entities in Ukraine. Any future cyber operations that aim to undermine the functioning of Ukraine’s critical infrastructure could cause substantial collateral damage to neighboring countries and businesses operating in the region. EternalPetya should serve as a warning of the potential for geopolitically motivated cyber operations to cause significant economic damage in the immediate and surrounding regions.

As organizations continue to struggle with visibility, these types of incidents – causing significant economic losses – will continue to make headlines in 2018. Additionally, affected organizations may be further penalized by not complying with laws such as GDPR, and may also experience an increase in insurance premiums and loss of brand value.

A Digital Geneva Convention is Unlikely to Happen in 2018

As we enter 2018, cyber criminals and nation sponsored hackers will continue to operate with little to no risk of repercussion. While there has been a stronger voice suggesting a form of a digital Geneva Convention, this is unlikely to happen in 2018. Nations need to agree on rules of engagement in cyberspace, but the politics surrounding such an agreement will make it unlikely – if not impossible – for something to be developed in 2018. Therefore, attribution will continue to play a crucial part in 2018 to cast a spotlight on threat actors and the nations that are hosting and/or sponsoring them.



SECURITY PREDICTIONS

for the Asia Pacific Region

China Continues to be a Major Cyber Power

Over the past 15 years, China has conducted a wide variety of well-documented activities in cyberspace to advance their national interests, and we expect that to continue as we move into 2018.

Specific to relations with the U.S., while we believe the Chinese Government has complied with the terms of the September 2015 “Xi Agreement”, we also believe that they may be willing to violate it in high priority instances.

A similar agreement was signed between the Australian Government and the Chinese government in April 2017. There was an additional requirement in this agreement, in comparison to that of the U.S., that required each signatory to act in accordance to the norms of responsible state behaviors, as outlined by the UN Group of Governmental Experts on cyber. While this is an important political milestone for the Australian government, we do believe China will continue to undertake cyber espionage activity against Australian interests to achieve its strategic goals.

In the Asia Pacific region, China and neighboring countries are still continuing political disputes, especially with South Korea, Japan, the Philippines, Vietnam, India and other Southeast Asian countries. Therefore, unorganized hacktivism attacks as a response to these political tensions within and against these countries is expected to continue and possibly rise throughout the new year.

Cyber Crime Reaches New Levels of Sophistication

From an incident response perspective, we've seen an uptick in the number of investigations of incidents carried out by financially motivated groups, and we believe this trend will continue upward throughout 2018.

Unlike nation state actors, cyber crime groups are not bound by regional intelligence requirements, only financial gain. Traditionally, the approach for these actors has been comparable to casting a wide net across many people. However, the incidents that we investigated in 2016 and 2017 have more resembled the cyber equivalent of a well-coordinated heist with a focused objective.

This means that any institution handling money or transactions has a good chance of being compromised if they have weak security controls. These cyber crime threat groups are using techniques and attacks more closely resembling what we typically see from nation state actors, and the level of sophistication will only go up in the new year.

Additionally, targeted focus on large hauls of personally identifiable information will continue to occur in 2018. Recent breaches in the region – including one involving tens of millions of phone numbers – highlight the ongoing underground economy commercial demand for personal information and credentials.

More Malware Targeting Cryptocurrencies

As cryptocurrency continues to skyrocket in value and popularity, we expect to see much more malware targeting anonymous currencies such as bitcoin. Previously, we have seen several different types of malware that target systems for mining purposes; however, moving into 2018 we expect to see much more malware actively stealing cryptocurrency from weakly protected wallets, shimming password entry to wallets, stealing offline wallets for brute forcing, or using credentials stolen from the same user. We've already begun seeing instances of this, but with bitcoin valuations spiking and the returns from stealing even a few bitcoins being significant, we expect to see a lot more in 2018.

More Malware Spreading Surreptitiously

Another recent malware trend we've begun noticing is the development of malicious programs that misuse operating system facilities, yet do not look like malware. We expect threat actors will continue to explore this in order to avoid being detected. Additionally, auto-spreading malware leveraging credential theft, pass-the-hash, and more will become increasingly common in 2018. We've already seen several of these cases this year, and the implications for ransomware distributors are significant as it drastically increases the returns.

The Battle Ahead

From innovative attacks and malware, to incoming laws and regulations, to changes in nation-state activity, it's evident that 2018 has the potential to be another event-filled year in cyber security. But while there are many new things to look forward to in the next 12 months, and many different ways to stay prepared, we also cannot sleep on the timeless fundamentals that continue to keep us secure.

As we've said before, so long as consumers remain vigilant and perform basic security hygiene, then they stand to remain reasonably protected. This includes enabling two-factor authentication on all systems and accounts, using password managers to protect those systems and accounts, and automatically backing up data in the event of a ransomware infection or data compromise by a threat actor. The recent mega breaches involving the loss of personal data make it prudent to add credit monitoring and identity theft protection services to this list.

As usual, enterprises have the tougher road ahead. We continue to advise clients to prepare for when attacks happen – not if they happen – and to be ready to respond to and contain incidents. Holding incident response tabletop exercises to simulate typical intrusion scenarios is one way to stay prepared, and an added benefit is exposure of incident response processes and concepts to executives, legal personnel and other less technical staff.

Finally, it's important to simply keep a positive attitude in this industry. Some people think it's all fear, uncertainty and doubt, and that there are no answers, but this is exactly the type of thinking that hampers innovation and ultimately lets the bad guys gain an edge. Remain optimistic – we're going to manage our way through all the uncertainty in the industry. Security is in our DNA, and we are going to fix the problems, or at least treat them in ways where all the promise of our increasingly connected world is going to become a reality.

For more information, please visit
www.FireEye.com

For more information
on FireEye, visit:
www.FireEye.com

FireEye® is the leader in intelligence-led security-as-a-service. 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 5,000 customers across 67 countries, including more than 940 of the Forbes Global 2000.

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

www.FireEye.com

FireEye®