



**THE ROAD AHEAD:
CYBER SECURITY IN 2020 AND BEYOND**



2020

● ● ● The Road Ahead

Introduction

From the Desk of the CSO—

Steven Booth, Chief Security Officer

- The Cloud Has Changed Security
- Proof of Compliance
- Security Hygiene
- Staffing Outside the Box
- Mind the Supply Chain

A View From the Clouds—

Martin Holste, Chief Technology Officer for Cloud

- The Cloud Is Secure, Let's Talk about the Real Threats
- More Clouds, More Complexity
- The Skills Gap Holding Back Cloud Adoption
- Attackers in the Cloud
- Asking the Right Questions

Intelligence Declassified—

Sandra Joyce, Senior Vice President of Global Intelligence

- The Bigger Picture
- Multiple Levels of Security Maturity
- Ransomware Tactics Evolving
- U.S. Elections Bring Rise to Cyber Activity
- Attackers are Innovating

4

6

8

10

In the Customer's Shoes—

Dave Baumgartner, Chief Technology Officer for Americas

- What We Lack Today May Hurt Us Tomorrow
- Struggling to Apply Intelligence
- Cyber Security Done Well
- Bridging the Vendor Gap
- Solving a Bigger Problem

12

Emerging Roles: General Counsel—

Alexa King, EVP and General Counsel

- The General Counsel and Cyber Security
- Allies of the General Counsel
- Privacy
- Privilege
- Practice, Practice, Practice

14

Miscellaneous Musings

- Targeted Ransomware
- China's Belt and Road Initiative
- Geopolitical Tensions, Espionage and Disruptive Threats
- Developing Information Operations
- Criminal Operations Expanding Tactics

16

2020 and Beyond


18



Introduction

The end of the year is an important time. In our personal lives we have plenty of holidays to celebrate and we get to spend extra time with those who are most important to us. In our professional lives—and in the cyber security industry, in particular—we get a chance to pause and think about everything that happened throughout the year, what might happen in the coming year and what we could begin doing now to prepare ourselves for any obstacles we may face going forward.





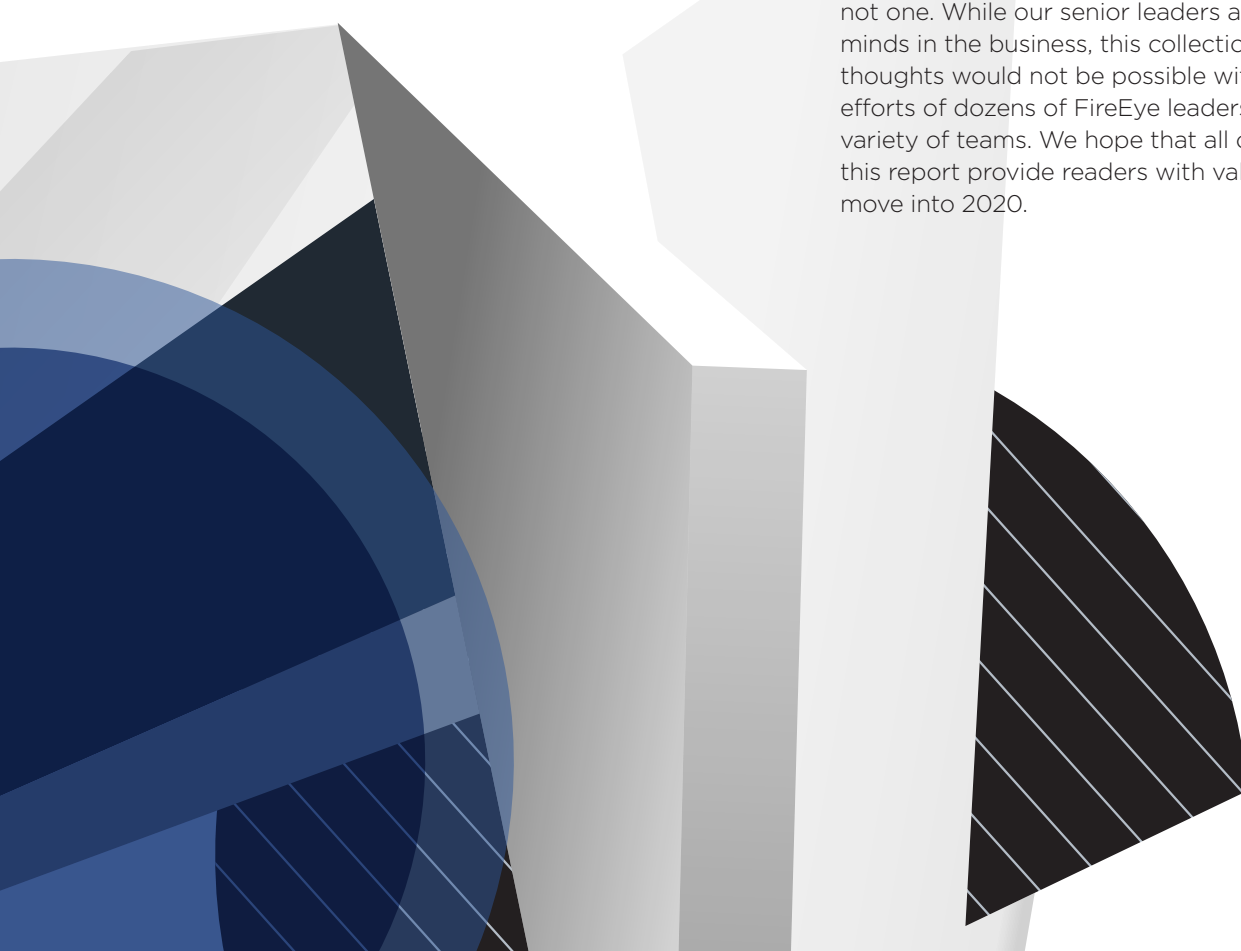
While each security professional is encouraged to stop and think, cyber security is the job of many. Painting a comprehensive picture of the things to come in the industry requires feedback from hundreds or even thousands of individuals.

That is why for this report, *The Road Ahead: Cyber Security in 2020 and Beyond*, we sought insights from FireEye senior leaders across the entire company, including CSO Steven Booth, cloud guru Martin Holste, intelligence expert Sandra Joyce, technology expert Dave Baumgartner, and head of legal Alexa King.

As we move into 2020, our group of senior leaders has a lot on their minds, including:

- How increasing use of the cloud continues to change security
- The skills gap and thinking outside the box when it comes to staffing
- Threats such as ransomware and weak spots such as supply chain
- Cyber activity during the upcoming U.S. elections
- How organizations and vendors need to start thinking about security
- The emerging role of the general counsel
- The continued evolution of information operations
- Geopolitics as a driver of cyber activity
- Increasingly sophisticated cyber criminal operations

We cannot overstate that cyber security is the job of many, not one. While our senior leaders are some of the brightest minds in the business, this collection of forward-looking thoughts would not be possible without the additional efforts of dozens of FireEye leaders and experts on wide variety of teams. We hope that all of their contributions to this report provide readers with valuable insights as we move into 2020.





From the Desk of the CSO

Steven Booth, Chief Security Officer

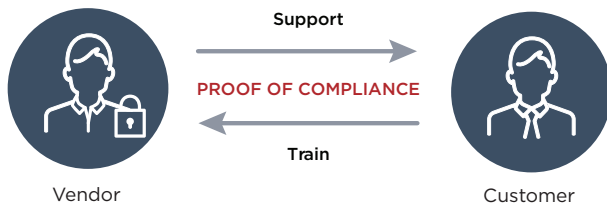
In 2020, vendors and security providers will need new, expanded and **renewed thinking** on how to **collectively** approach security.

The Cloud Has Changed Security

Cloud adoption has fundamentally changed the IT landscape and will continue to do so as we move into 2020. While this may sound obvious, the reality is that it impacts what we do as security professionals in fundamental ways that are not always obvious. We no longer manage many of our core infrastructures, applications or even services, and as customers of cloud providers we need to understand the contract terms that delineate and isolate the platform vendors' responsibilities versus those of their customers. Apart from ensuring the

service availability levels, capabilities and utility of their service, nearly all other the responsibilities fall on the organizations that use those services. More specifically, customers retain the responsibility of ensuring they operate the cloud offering in a way that maintains their own security requirements, that they follow all best practices and—more broadly—that their use of these solutions also meets and can address all applicable regulatory compliance and audit requirements. That is a very tall order, and in 2020 it will require new, expanded and renewed thinking on how we (vendors and security providers) collectively approach security.

Compliance is a two-way street.



Proof of Compliance

In 2020 there will be a broadening push on providers to offer more proof of compliance to industry regulations and customer requirements, with clear ways for their customers to validate that vendors are doing what they say they are doing. This is a two-way street—as cloud and other offerings mature, they must incorporate and grant better facility to support the reporting capabilities we have grown accustomed to in our security and risk programs. We have a responsibility to train the vendors to understand that they have a part to play in ensuring we should grant them our trust and our data.

Security Hygiene

Hygiene is one of those topics that cause many to roll their eyes in disdain; however, it is fundamental to security and must again be brought to the forefront and addressed as we expand the services we use. As organizations move more of their development environments natively outside their perimeter, they must be diligent in ensuring they protect their development and staging environments at the same level as their operation environments, and should never keep them available longer than required to perform necessary tasks. This year we saw a situation where a long-time, early cloud adopter exposed access to years of development, test and staging environments, which resulted in a significant breach. This is a high value and relatively low risk approach for attackers because these systems tend to be monitored with less voracity. I expect to see many more organizations in 2020 exposing real data, sensitive data, configurations and trusted security components due to the mismanagement of their off-premise development, staging and testing environments.

Staffing Outside the Box

We are now firmly in the midst of a security staffing shortage that demands a rethinking of what is actually required to do the jobs we have available. What are the high-value skills that are hard to develop, versus the skills that a dedicated individual can learn over a reasonable amount of time? Critical thinking and data synthesis are among the skills that are developed over many years and are not easily teachable, whereas various other technical skills that some may think require years of training can actually be acquired in a shorter period of time. As security leaders we have to think outside the box—we need to reconsider our notions of what makes a great security candidate by looking beyond the typical security certifications if we are going to have any chance to protect our environments the way our employees and customers expect.

Mind the Supply Chain

Not all vendors automatically merit a high level of confidence. The lack of visibility into the details of an offering can lead to unexpected exposures if it was relied on to perform a specific security function or if it grants a previously unavailable or undocumented capability or data access if it was compromised. Much of the code used in on-premise and cloud environments is built using open source components, and many of the basic building blocks are rarely—if ever—vetted beyond checking that others have used this same code, thereby making an assumption that someone must at some point have taken the time to review it for possible issues. We have seen a number of situations in the past few years where software components in automatic updates were corrupted or poisoned with malicious code. In 2020 and beyond, this will become a greater risk as we see more threat groups building capabilities aimed at impacting software supply chains. While it is a practical impossibility to review every bit of code provided by all vendors or service providers, one way to monitor possible exposures includes using brand and digital threat monitoring services.



A View From the Clouds

Martin Holste, Chief Technology Officer for Cloud

The number one thing an organization has to do after email security is get **visibility** into all their different cloud environments to know which cloud they're in, what assets are there and **exactly who's doing what**.

The Cloud Is Secure, Let's Talk about the Real Threats

It's been roughly 20 years since we first saw cloud computing emerge as a service for enterprises; now we can confidently say cloud computing is fundamentally secure. It's time to focus resources on how to properly secure the cloud, work with cloud platforms and address the skills gap that's increasing our risk when we use the cloud improperly.

More Clouds, More Complexity

The major cloud platform providers recognize the security of their platform is core to earning trust with customers. We've seen significant investments in security since the beginning, and today we're seeing cloud vendors add even more security capabilities.


On the security provider side, they are doing a much better job of understanding that customers are moving to the cloud, and not just one cloud but multiple clouds. That's something that will continue into 2020. It's not just a single cloud provider that a customer will use—they're going to have multiple clouds that they have to protect, and that really adds up quickly. Cloud providers are doing a much better job of making security simpler, but at the

same time there's more cloud being used, and more types of clouds being used, so the job of any security professional is only going to get more challenging because there's just that much more work to do.

As security practitioners, we have to understand this complexity, match our security programs to meet the needs of the business and be thinking about these challenges ahead of our business partners. We've also seen platform vendors recognize the need for different accounts. As organizations get more into cloud, making sure that they are separating out duties across different account IDs is important. And that is much easier now with some of the things cloud providers have done in the last few years. I see that trend continuing, of making the cloud easier to use and more secure by default.

The Skills Gap Holding Back Cloud Adoption

Even the most mature security operations centers (SOC) struggle with moving to the cloud. They're still having to do all the work that they've been doing to secure their on-premises assets, and that's not going away any time soon. It takes years and years to migrate for most companies. Even the companies that do it the best—with the strongest mandates—are still taking about a year and a



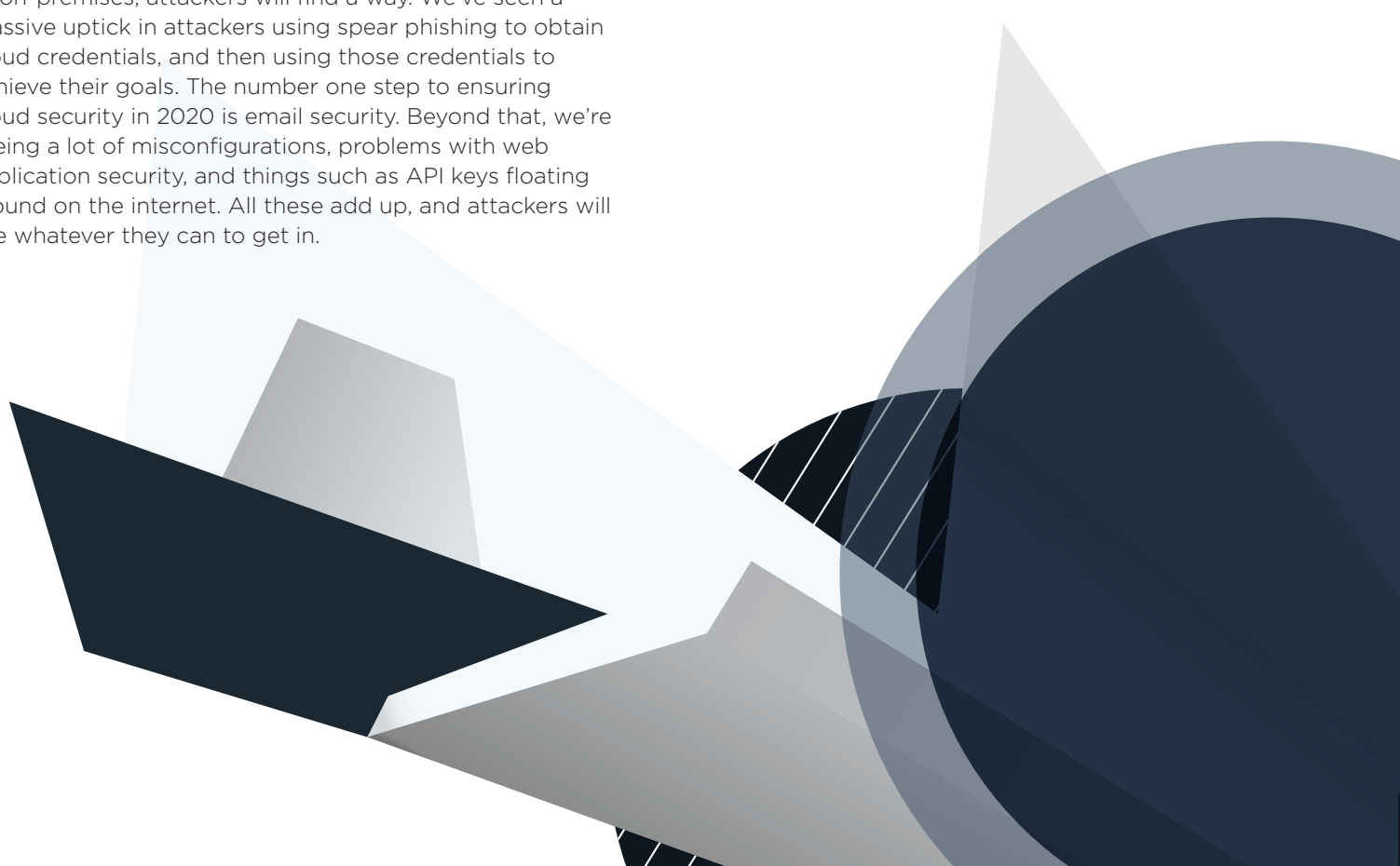
half to move everything into the cloud. And that SOC has to protect everything that's still on-premises, on top of the new stuff going in. The less security mature organizations at least know that they have a really big problem to start with, and they seek assistance immediately. However, the lack of skilled workers isn't helping, and now you have staffing issues for specific areas such as cloud. Finding cloud expertise is hard—finding cloud security expertise is even harder. Cloud environments have different processes around monitoring, identity, configuration and encryption processes. Customers trying to transfer an on-premises security program to the cloud will find a new set of challenges. Be aware of the differences, focus on developing cloud security skills and ensure you have regular security reviews of cloud environments.

Attackers in the Cloud

Any given cloud or any given service offered in the cloud is generally pretty secure. The problem is that attackers don't care. They will go around whatever protections are put in place. Whether an organization is in the cloud or on-premises, attackers will find a way. We've seen a massive uptick in attackers using spear phishing to obtain cloud credentials, and then using those credentials to achieve their goals. The number one step to ensuring cloud security in 2020 is email security. Beyond that, we're seeing a lot of misconfigurations, problems with web application security, and things such as API keys floating around on the internet. All these add up, and attackers will use whatever they can to get in.

Asking the Right Questions

The number one thing an organization has to do after email security is get visibility into all of their different cloud environments—make sure that they're well aware of not only which cloud they're in and what assets they have there, but exactly who's doing what. This becomes a bit of a business logic problem at the end of the day, trying to figure out: "Was an application doing what it was supposed to be doing?" or "Was a user doing what they were supposed to be doing?" And that requires a lot higher level knowledge from your SOC than just looking at an alert and deciding whether it is a true positive or not. The job of the SOC is really changing, and we're seeing them having to learn a lot more about the business to understand what's normal.





Intelligence Declassified

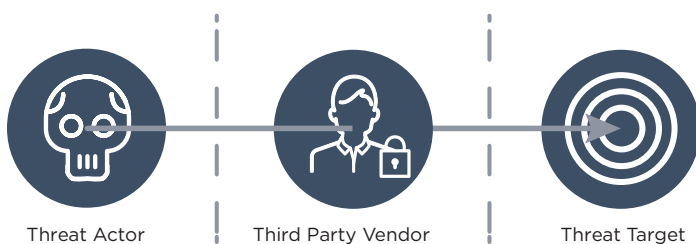
Sandra Joyce, Senior Vice President
of Global Intelligence

What organizations need to really think about
in 2020 is that the **innovation** has to come
from **the good guys**.

The Bigger Picture

One important takeaway for next year is that every organization is somehow related to a possible target. Even if an organization is small or seemingly insignificant to threat actors, it's likely a supplier, third-party vendor, or in some way connected to a bigger, larger target. Organizations need to be cognizant that they could be the critical node—they could be the weakest link. Organizations should consider themselves in a broader context. It's not just what's happening between a target and a threat actor—the entire ecosystem that they're a part of matters. The best thing organizations can do going into 2020 is understand where they sit in the threat landscape, but that's easier said than done. Those that are trying to use intelligence are now seeing that it's quite a large task to really understand their threat profile.

If you work with a high-value target, you're probably also a target.



Multiple Levels of Security Maturity

What intelligence providers in particular need to be aware of as we move into 2020 is that there are multiple levels of security maturity in the market space. Some organizations are extremely mature when it comes to using intelligence to make decisions and to improve their security postures, whereas other organizations are just starting out and need good advice about how to use intelligence in the best way possible to prioritize their spend and put the technology they have to good use. Leaders of organizations implementing an intelligence program have the benefit of understanding what is likely to happen, and what threats are targeting them and others in their industry. However, other leaders haven't had to think about what is going on beyond their network until now.

Ransomware Tactics Evolving

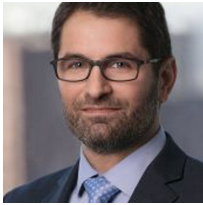
In 2020, defenders need to be looking out for new techniques involving ransomware. What we've been seeing in the underground is threat actors advertising their access to organizations, no matter what industry, and trying to find partners who have ransomware that they can deploy deep in those networks in a very customized fashion. We've also seen some of the most sophisticated criminal intrusion operations shift to this type of ransomware deployment, away from other tactics. This very targeted ransomware technique is leading to increased ransomware demands and putting organizations at a high risk of losing intellectual property. While many criminal actors avoid targeting governments to reduce exposure, we have even seen a major increase in the targeting of state and local government organizations, most likely because they have fewer resources than the federal government.

U.S. Elections Bring Rise to Cyber Activity

As we go into a very important election year in the United States, we expect to see an increase in not just cyber espionage and cyber influence operations targeted at the electoral systems, but also candidates being impersonated on social media and other types of information operations designed to target the voters themselves. In an effort to support election security, FireEye recently launched an [election security resource center](#) where we have a lot of information that should help defenders during this critical time.

Attackers are Innovating

Unfortunately, what we're seeing is great innovation and progress on the part of the threat actor. They're becoming more creative and more sophisticated. We're seeing cyber criminals have the sophistication level of nation states. Organizations need to ensure in 2020 that innovation comes from the good guys; we cannot let the bad guys have the lead. In order for us to defend, we need to get ahead of the threat.



In the Customer's Shoes

Dave Baumgartner, Chief Technology Officer
for Americas

One reason that organizations struggle with cyber security is a **lack of experience** having **seen it done well**.

What We Lack Today May Hurt Us Tomorrow

Strength in cyber security is very fragmented, meaning across multiple industries—retail, hospitality, finance, government, transportation, energy—you have a significant disparity between those that do cyber defense well, and those that are unable to for a plethora of reasons. It could be the fact that they don't have enough experienced individuals within their team to understand how to effectively or adequately detect potentially anomalous conditions, or it could be that they have great skills and great potential, but are unable to fund all the necessary investments to up their game consistently. This is a trend we've been seeing and something we expect will continue as we move into next year. Organizations need to start identifying their weaknesses if they're going to be prepared in 2020.

Struggling to Apply Intelligence

One of the biggest challenges facing companies today is they don't necessarily have an appreciation for just how difficult it is to maintain a pace of awareness to adversary activity. Basically, everyone now thinks they know what threat intelligence is, but most often when they describe how they consume and process intelligence it becomes obvious they are not maximizing its full potential. They may solicit content from two or three different threat

intelligence providers and think that's good enough, or they may belong to an industry sharing consortium and feel like that's good enough. Realistically, that's not going to cut it. What organizations need to start doing in 2020 is figuring out how to take that content and map it to how they actually run their business and use it to proactively instrument detection in a continuous manner.

Cyber Security Done Well

One reason that organizations struggle with cyber security is a lack of experience having seen it done well. To become more security mature in 2020, organizations need to understand how they're potentially susceptible to an attack and what the implications of those attacks may be, so they can ultimately determine how to best defend themselves. They have to actually understand their assets. They have to understand their technology, know where their applications live, know where their infrastructure lives, understand their third-party risk, be capable of determining where all of their egress points are, and so on. Unfortunately, most companies today lack one or more of these things and that leaves them open to attack from the bad guys. They simply don't have a comprehensive perspective of what they are trying to protect, and that has to change as we move into next year.

A deep understanding of critical topics can help mature your security.



Bridging the Vendor Gap

From a vendor perspective, I think we're working with a customer base today that has more broad awareness than ever about the problems they're facing, and that has probably grown more frustrated about their inability to see the promises that vendors and professional services firms have made to them come to fruition over the past few years. More specifically, I think their expectations of integration between disparate technology is greater than it ever has been before. What we will continue to see moving into 2020 is security vendors forced out of necessity to become a bridge between multiple technologies that might previously have been considered competitors. I think that's critically important.

Solving a Bigger Problem

Realistically speaking, I don't think anything is going to change any time soon, especially when you continue to see what we see, which is the growth and explosion of new attack techniques, while at the same time the things that we stopped talking about and that people assume aren't a big deal anymore are also increasing. A good example is how denial of service, which people don't really talk about anymore, is up about 150 percent in 2019. Business email compromise, which people are concerned about yet often prioritize behind other investments, is now a criminal enterprise bringing in billions of dollars each year. I don't think it's necessarily going to get better in 2020. I don't think it's going to get better until we as a global community determine that we're going to get serious about holding actors accountable, and unfortunately in many cases that means holding countries accountable. That's a very complex issue that I do not see being solved in 2020.



Emerging Roles: General Counsel

Alexa King, EVP, General Counsel



The number one thing that GCs should be doing—if they're not already—is running **tabletop crisis exercises** to prepare for breach scenarios.

The General Counsel and Cyber Security

The role of the general counsel (GC) in an organization's cyber security program—from beginning to end—has evolved and greatly increased, and it will continue to do so as we move into 2020 and beyond. General counsel today and going forward need to be front and center in

any corporation's cyber security program, partnering very closely with several key individuals, focused very strongly on educating the board and working with the board and executive management to prepare for the inevitable breach. Cyber security is not something that is going away in terms of GC priorities and agenda.

Allies of the General Counsel

The first and foremost ally of the general counsel is the board of directors. The board's fiduciary duties have evolved to absolutely include cyber security. They are becoming more interested in learning what their duties are, and the GC is the person who should be advising them. The general counsel must also work with various other people across their organization.

I work very closely with our CSO and CIO. I additionally work quite closely with HR and Marketing, and with our sales force as well. One reason for this is that the people on these teams are controllers of data. They're going to know what we have, how we access it and how we use it. Furthermore, if an incident occurs, these are the people that I will be partnering with when it comes to executing the communications plan, the customer support plan, and all of the things that our company needs to do in the middle of a crisis.

Privacy

One thing that I focused on a great deal over the last year or two is privacy. I hired our data privacy officer, and I partner very closely with him. In large measure this focus on privacy was because we were preparing for enactment of General Data Protection Regulation (GDPR) and more recently we were preparing for California Consumer Privacy Act (CCPA), which was just signed recently by the California governor. We've done a lot of work together around understanding where our data is held and what types of customer and employee data we collect and/or hold—both internationally and now, with CCPA coming up, here in California. The knowledge we've built up translates very well into the work that I do around cyber security. It helps me understand, again, what data we have, where we keep it, what's most vulnerable, what I should be worried about from a privacy perspective and what I need to safeguard from a cyber security perspective.

Privilege

As we know, particularly in the United States, most cyber breaches result in litigation, and litigation is best prepared for when all of the steps that are taken by a company before, during and after a breach go through the general counsel's office and therefore are privileged. The attorney-client privilege enables companies to prepare, investigate and do everything they need to do in the most transparent way possible without worrying about what a plaintiff's lawyer may or may not use against them, especially if it's out of context. In order for me and our executive team and our board to have the most open conversations about opportunities, vulnerabilities and next steps, we need to be confident that those conversations aren't going to be somehow taken out of context and used against us. We want to do the best we can for our employees, for our customers and for our shareholders, and the attorney-client privilege helps us to do just that.

Practice, Practice, Practice

Breaches are inevitable, so what is the course of action when it happens? I'd say the number one thing that GCs should be doing—if they're not already—is running tabletop crisis exercises to practice. We do that regularly here at FireEye. As always, I partner with our CIO and our CSO, but it has top-down support. I have the CEO in the room, as well as the CMO and the CFO. The reason for this is that, should a breach occur, these people cannot spend valuable time coming up with a plan. I would say as GCs, tabletop exercises are the best thing we can do to prepare. Work with the CMO in advance to think about: What is our communications strategy? Work with the CFO in advance to think about: How do we want to think about investor relations? The more we can do in advance, the better.



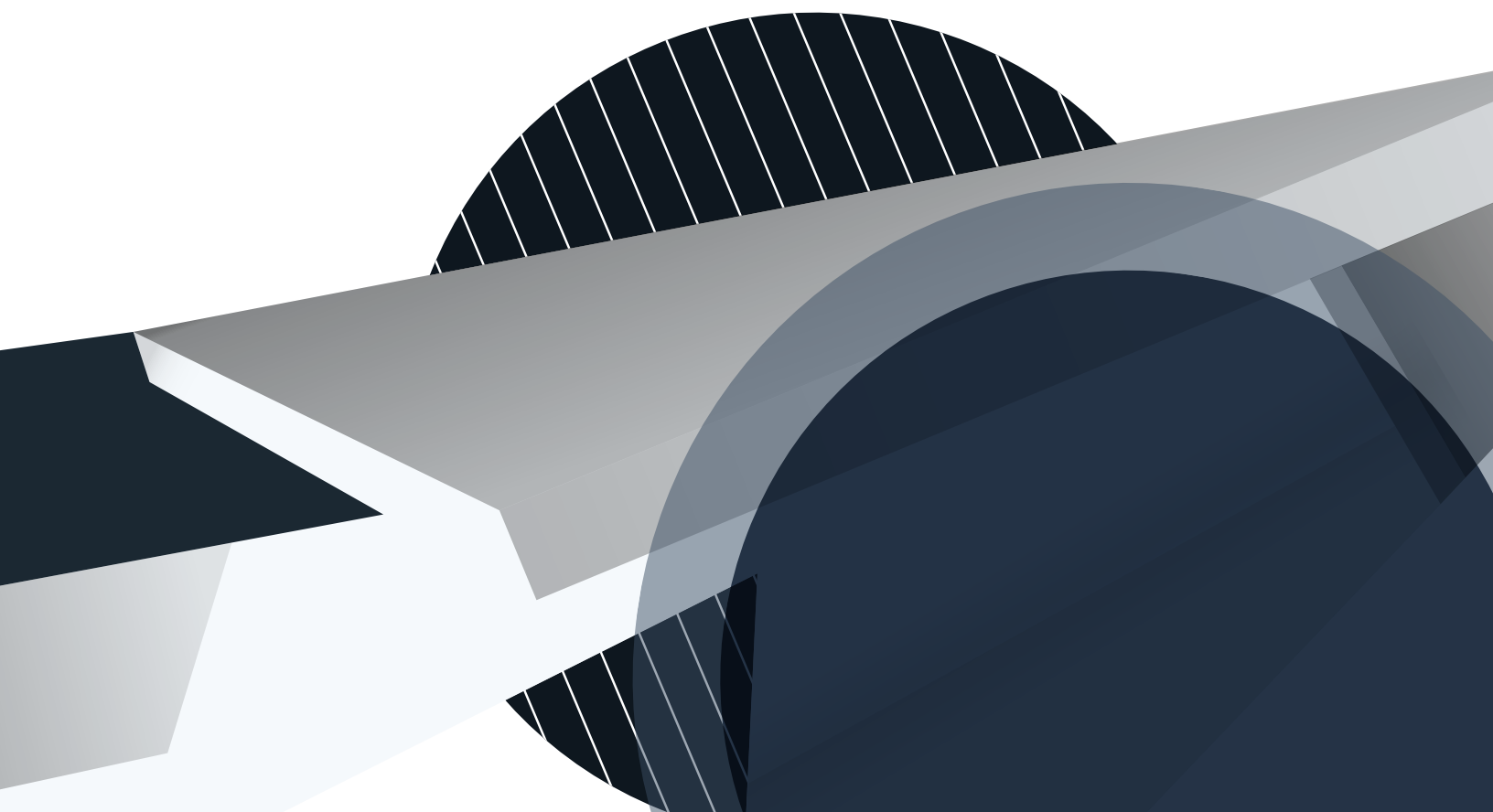
Miscellaneous Musings

Targeted Ransomware

Malicious actors will maintain a high pace of deploying ransomware in a targeted manner against specific environments. These attacks have commoditized highly disruptive tactics that historically were more limited to politically-motivated attackers. They impact a wide variety of organizations, are not limited to any particular sector or region, and cause victims significantly more pain and loss than the non-targeted ransomware attacks popular in the past. Based on the success of these operations observed to date, we expect them to persist through 2020.

China's Belt and Road Initiative

China's Belt and Road Initiative (BRI) will drive espionage throughout multiple regions: Europe, the Middle East, and Asia. The BRI is a large-scale project to develop China's trade and influence. Recent cyber espionage activities believed to be related to the BRI have targeted governments at the national and regional level, transportation, extractive, energy, defense, space, media and telecommunications sectors. Simultaneously, we have seen Chinese espionage activity evolve to be more deliberate and covert amidst a restructuring of the country's intelligence apparatus.



Geopolitical Tensions Driving Espionage and Disruptive Threats

Geopolitical tensions are, regardless of the inciting issue, often a significant driver of intrusions and disruptive attacks. Currently, we are seeing Western tensions with Iran accelerate the tempo of Iranian cyber operations, and we anticipate this issue to continue if tensions persist. We have seen activity from several Iranian groups—including APT33, APT34, and TEMP.Zagros—against financial services, media and entertainment, retail and other sectors. In addition to exfiltrating sensitive information, it is possible that Iranian groups could leverage compromised access they establish for disruptive and destructive cyber attacks to retaliate or impose costs against adversaries.

Developing Information Operations

Nation-state influence activities at the intersection of cyber threats and information operations will continue developing. FireEye has observed information operations linked to Russia, China, Iran, Venezuela, and other countries developing and maturing as these have received public exposure. While not limited to issues around elections, we often observe these activities to be particularly intense around elections. Some of the elections that may drive this activity in 2020 will take place in Taiwan, South Korea, France, Poland and the United States.

Criminal Operations Expanding Tactics

Sophisticated intrusion operators that have conducted point-of-sale (POS) breaches will perform more diversified operations, threatening organizations that have secured their POS environments and those outside the retail space. Because many organizations in the United States especially have continued operating POS environments vulnerable to data theft, we have continued to see sophisticated intrusion operators targeting these environments for compromise, despite the rollout of EMV. As U.S. organizations have improved their security stance, though, we also see these operators—FIN6 and FIN7, for example—diversifying into other tactics such as compromising ecommerce websites and deploying targeted ransomware. This diversification means these sophisticated operators pose broader threats to a wider scope of organizations.



2020 and Beyond

We made great strides in 2019 and should feel very proud of the work we accomplished. However, attackers won't let up, so as defenders, we must continue to dedicate ourselves to cyber security in 2020.

On the cloud front, we're confident it is secure, but attackers are still finding success using email and other tactics that work just as well against an on-premise environment. While cloud providers, security vendors and customers all need to come to an understanding over who is ultimately responsible for what when it comes to security, customers need to be particularly vigilant since they have the most to lose: the crown jewels and primary drivers of business.

In the United States, 2020 marks an election year and we expect to see an uptick in threat activity in the months leading up to the big vote. Not only are the actual voting machines at risk, but those with an agenda will more than likely take to social media and other similar platforms to spread misinformation in an attempt to sway voters. In today's heated political climate, voters owe it to themselves to remain skeptical. They should be stopping to think about where they are getting their news and if it's a trusted source.

One person that should be a primary player in any organization's security program is the general counsel. The general counsel can ensure that the board and other senior leaders are prepared for the inevitable breach by holding tabletop exercises and other activities. They can also ensure that their organization is compliant with any national and international legislation, notably as it pertains to data. And since many of today's intrusions result in litigation, the general counsel can ensure that organizations are protected and prepared to deal with any related fallout.

There is a lot more, but unfortunately no quick fix for everything. If there was, there would be no need for the millions of cyber security professionals across the world helping to fight the good fight, and there would be no skills gap and shortage of trained workers. Part of the solution is developing the right technology, which would automate easy tasks and allow security personnel to follow-up on critical alerts. We also need to hold attackers accountable if we want to see threat activity decline, which will only happen when we start pursuing attribution and make sure we're getting it right.

It's a tricky road ahead, but we at FireEye will stay the course and look forward to leading the charge in 2020 and beyond.

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

FireEye, Inc.

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

© 2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. F-EXT-RPT-US-EN-000238-01

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.

