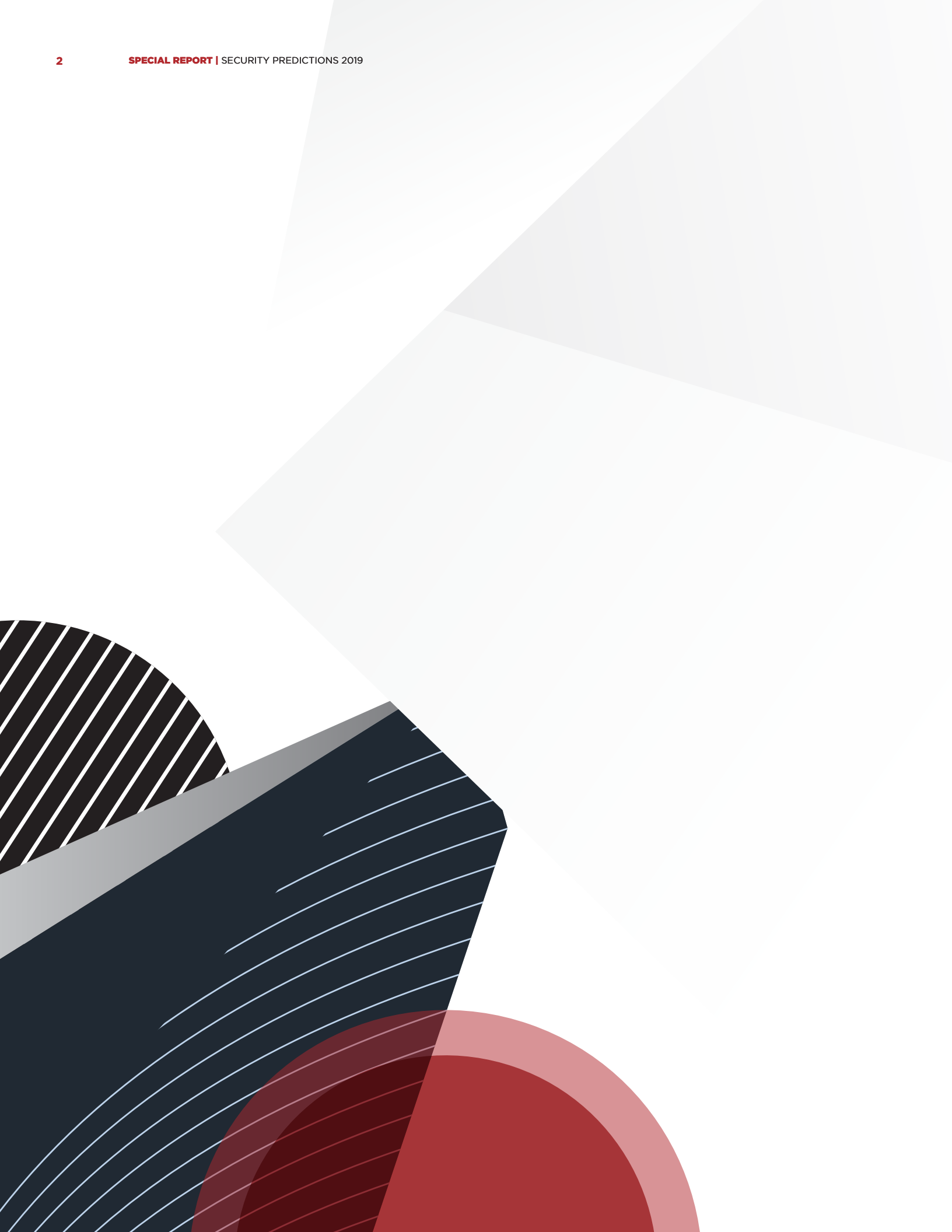




# **FACING FORWARD**

## Cyber Security in 2019 and Beyond





# Voices of FireEye

<b>Facing Forward</b>	<b>4</b>
<b>Follow the Leader</b>	<b>6</b>
Kevin Mandia, Chief Executive Officer	
<b>Staffing, Cloud and Consolidation</b>	<b>10</b>
Steven Booth, Chief Security Officer	
<b>Intelligence Declassified</b>	<b>13</b>
Sandra Joyce, Vice President, Global Intelligence	
<b>A View from the Clouds</b>	<b>16</b>
Martin Holste, Chief Technology Officer for Cloud	
<b>Leaving on a Jet Plane</b>	<b>20</b>
Christopher Porter, Chief Intelligence Strategist	
<b>From the Files of FireEye Threat Intelligence</b>	<b>22</b>
<b>On Assignment with FireEye Mandiant</b>	<b>26</b>
<b>Under the Lens of FireEye Labs</b>	<b>29</b>
<b>Global Insights:</b>	<b>32</b>
Asia Pacific (APAC)	<b>32</b>
Europe, the Middle East and Africa (EMEA)	<b>34</b>
Latin America (LATAM)	<b>37</b>
<b>2019 and Beyond</b>	<b>39</b>



# Facing Forward

In the cyber security industry, we're so frequently working around-the-clock for days at a time that we often forget when one year ends and another begins. It's a shame, too, because the end of the year is a very important time. It provides a moment to reflect on what we observed and experienced over the past 12 months, and to consider how best to address the challenges we have been facing. Perhaps more critical to our line of work, it offers an opportunity to note what developed into a trend, and what might develop into a trend as we move into the next year and beyond.

Each of us can take some time to ponder, but at the end of the day a single individual cannot sort it all out. It takes thousands of individuals — providing detailed insight from their various areas of expertise — to adequately assess the current state and future shape of the cyber security industry as a whole. It takes a full team to develop informed, well-reasoned and defensible security predictions.

For this year's security predictions report, *Facing Forward: Cyber Security in 2019 and Beyond*, we tapped into FireEye's deep well of leadership and expertise to pull together a wide range of thoughts about what's to come in 2019 and beyond.

As we enter 2019, our senior leaders, including CEO Kevin Mandia, CSO Steven Booth, intelligence authority Sandra Joyce, cloud guru Martin Holste and aviation expert Christopher Porter are thinking about:

- Nations developing offensive capabilities
- Breaches continuing due to lack of attribution and accountability
- The widening skills gap, and less trained experts to fill security roles
- Lack of resources, especially for small and medium-sized enterprises
- Supply chain as a weakness
- Attackers eyeing the cloud, since that's where the data is headed
- Social engineering, considered by many to be the most dangerous threat
- Cyber espionage, cybercrime and other threats to the aviation industry

Our senior leaders have a fantastic top-down view of the cyber security industry, but it's just as important to get a detailed look from the frontlines, so for that we've turned to experts from three of our major teams: FireEye Threat Intelligence, FireEye Mandiant and FireEye Labs. Our specialized analysts and researchers discuss a variety of topics, including:

- Restructuring of Chinese cyber espionage
- Increase in Iranian threat activity against U.S.
- Use of publicly available malware by major threat actors
- Abuse of legitimate services for command and control
- Sights set on e-commerce rather than point of sale
- Online banking portals in the crosshairs
- Reduced use of Flash and Java to improve security
- More business email compromise as initial attack vector
- Emerging technologies used to evade detection

Many of these predictions come from FireEye experts based in the United States, so we closed out this year's report by discussing some major predictions for regions outside of North America, including Asia Pacific (APAC), Europe, the Middle East and Africa (EMEA), and Latin America (LATAM).

This year's security predictions report would not be possible without the efforts of several dozen FireEye leaders and experts. We hope their contributions to this report provide readers with valuable insights as we move into 2019.



# Follow the Leader

Kevin Mandia, CEO



Without a deterrent, **attackers are going to keep targeting networks** and getting through.

**My career in cyber security started in 1993 at the Pentagon. I recall meeting with a colonel, and we discussed different options for my role with the 7th Communications Group. One option was JPL programming, while another was to work on the Program Objective Memorandum. I did not find either of these opportunities particularly interesting. Finally, the colonel got to the very last option: I could be a computer security officer. This was by far the most interesting position we discussed — and he stated there was only one spot left. So I took it.**

Today, as CEO of FireEye, I see cyber security much differently than I did in the mid 1990s. And this is true for others as well, from the average consumer on up to our legislators and elected officials. There are three key trends that I believe are impacting the current state of cyber security:



More nation-state  
offensive activities



No risks or rules of  
engagement for attackers



A lack of security  
resources

In my travels, I have the privilege of meeting with government officials from around the globe, and in nearly every conversation I inevitably get the same question within the first 10 minutes. Whether it be in the Middle East, Europe, Asia or North America, they ask how they can develop an offensive capability for their own nation.

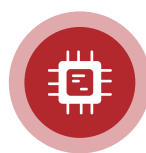
In 2019 and beyond, we expect to see more nations developing offensive cyber capabilities. There are people that claim nations should not do this, but in the halls of most governments around the world, officials are likely thinking their nation needs to consider offensive operations or they will be at a disadvantage.

We are also seeing deteriorating rules of engagement between state actors in cyber space. I have spent decades responding to computer intrusions, and I am now seeing nations changing their behaviors. As an example, we have witnessed threat actors from Russia increase their targeting and launch cyber operations that are more aggressive than in the past. Today, nearly every nation has to wonder: “What are the boundaries of cyber activities? What can we do? What is permissible? What is fair game?” We have a whole global community that is entirely uncertain as to what will happen next, and that is not a comfortable place to be. We must begin sorting that out in the coming years.

Unfortunately, the attacks that lead to breaches do not appear to be slowing down. One reason why is that there are still no risks or repercussions for those who are conducting the breaches. The attackers are not waking up fearful that they are going to get arrested for stealing email or extorting someone for a certain amount of cryptocurrency. Without a deterrent, attackers are going to keep targeting networks and getting through. Another challenge is that most cyber attacks exploit human trust. So long as the internet allows us to communicate via email or text, there will be an avenue of vulnerabilities. An attacker will always find a way to get a victim to click on a link or execute something malicious.

A third challenge involves the lack of effective security resources, as well as the means to scale defensive resources. Big companies that are well-resourced are able to have a mature security program with lots of tools, lots of processes, and lots of trained people who have practiced their tradecraft against red teams – and they still get breached. Then there are the small to medium-sized businesses that do not have the people or the resources. As a result, they are simply unable to build the security programs required given today’s threat landscape. The “smalls” are the softer targets, and they comprise the supply chains for the larger organizations. If these softer “smalls” end up getting compromised, the supply chain will be compromised, and that results in a backdoor into the larger enterprises with the mature security programs. These are the struggles we are seeing in 2018, and we must start addressing them in the year ahead.

What should we do about all this? There are three areas we can pursue to improve our security posture as a global community:



**Technology**



**People**



**Diplomacy**



On the technology front, we at FireEye will continue to focus on our innovation cycle. I still believe it is critical for anyone who creates software to recognize that software is the automation of human processes. What we get to do on the frontlines every day when we are responding to breaches is see exactly how the common safeguards we all use get circumvented. Then, we create an innovation cycle that addresses those evasions. That is part of FireEye's mission. What we learn from being on the frontlines is being pushed into our solutions to automate human processes, so we can offer greater scale and better defenses for all. Technology must help, so we will do everything we can to automate Tier 1 and Tier 2 security operations center (SOC) operations. We might not take humans completely out of the loop, but we can scale with software and automation and focus human involvement on the most critical decisions.

The second action is to build capacity through knowledge sharing. We must train each other, learn from each other, discuss what the bad guys are up to, and discuss which solutions and services work and which solutions and services do not work. We must get everyone in the industry to elevate their skillsets and, perhaps more importantly, get the next generation of security practitioners developed as well.

The final priority is diplomacy. Cyber security is a global problem, and we are all in this together. The fact that a lone attacker sitting in one country can instantaneously conduct an operation that threatens all computers on the internet in other nations is a problem that needs to be addressed by many people working together. We need to have conversations about rules of engagement. We need to discuss how we will enforce these rules of engagement, and how to impose risks on attackers or the nations that condone their actions. We may not be able to reach agreements on cyber espionage behaviors, but we can communicate doctrine to help us avoid the risk of escalating aggression in cyber space. And we can have a global community that agrees to a set of unacceptable actions, and that works together to ensure there exists a deterrent to avoid such actions.

# Staffing, Cloud and Consolidation

Steven Booth, Chief Security Officer



A lot of innovation in 2019 is **going to deal with consolidation.**

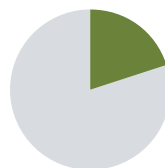
---

**When I think about how the cyber security industry will shift and evolve as we move into 2019, I see several key areas that security professionals and organizations will (and will need to) focus on, chief among them: staffing, cloud and consolidation.**

Let's start with staffing. According to various industry estimates, there are two or three million cyber security jobs that will go unfilled by the year 2020. While the numbers vary by study, the point is that if you take every single person in every computer science major in the U.S., that's still not enough to fill every open cyber security position. And we know most of those people will choose another field and won't end up working in cyber security.

We haven't quite hit the critical meltdown point when it comes to staffing. The good news is that the pain is there, and the thinking is changing. Can you take that employee working the service desk and train them how to respond to a security event? I believe you can. Can I get security value from non-security personnel? The potential is there. Sometimes the dynamic nature of life makes this inevitable. If you have a firewall person who has done extremely well, but now you're moving most of your business to the cloud, now that firewall person needs to set policy for their AWS environment for the first time. This is where leadership counts. If you're not giving employees new responsibilities and providing them with the training to enhance their skills, you're missing an opportunity and will likely lose those employees. If you invest in your people, you develop and attract the best people.

Another thing that really concerns me for 2019 is cloud, and cloud problems. Everyone in the industry is seeing huge migrations to the cloud, but most companies are not doing anywhere near as much work as they need to be doing to protect the cloud the way they used to protect their data centers — and the bad guys know this. There is a reason why roughly 20 percent of the incident responses and breaches we are working involve the cloud. The bad guys go where the money is, and throughout 2019 there will be an increasing number of opportunities for attackers in the cloud. With cloud, there's a whole chunk of attack surface that doesn't have advanced technology to detect evil. The good news is there is a big surge of innovation in the industry as to how to address those things. The bad news is that means organizations end up with more solutions, more events, more workload — more complexity. But that's never going to change. There is always going to be more — more events, more devices, more detection platforms, more things to look at, and more technologies that your security people have to understand.


**20%**

There is a reason why roughly 20 percent of the incident responses and breaches we are working involve the cloud.

I think that a lot of innovation in 2019 is going to deal with consolidation. You can only have so many categories of things that your security people can focus on. And you can't afford it, either. You have to get the job done with the people you have, and anybody should be able to do it. That's the part that is hopeful. If you can come up with a way where non-security employees can deal with some of the threats that come in, that's a huge benefit.

In the cyber security market, people tend to think of things as: What is the magic technology? Unfortunately, there is none. The question should be: What is the overlapping system of controls and capabilities that you have, and how do you use them? There is a large number of people — many who have my title — that have purchased various tools and technologies, but they don't have anyone that knows how to use them. They're staring at consoles at what events are firing the most, but not what is the most important.

Most of the people in my type of role have gotten over the antiquated idea that if I have a firewall then I'm safe. But if you're thinking you bought a bunch of technologies and you're safe, then you're wrong. You need to ask yourself: What is it that I'm trying to control? One way to approach that question is to accept that you can't protect everything equally. You have to be treating the new cloud infrastructure that stores the crown jewels of the organization as higher priority than the laptop belonging to one user who just clicked a malicious link. You need to have significantly different controls, and a large part of that simply boils down to: Do you know what your assets are? Do you actually know what you're trying to protect? This is a tougher question than it seems, but in 2019, you need to have it figured out. And once you build an ability where you can say, "I have a pretty solid architecture to protect this asset," then you can reuse and adapt that ability. You now have a set of controls that are reliable, and that can possibly be repurposed for different needs.



...remain skeptical  
about what you read,  
**especially on the  
internet.**

# Intelligence Declassified

**Sandra Joyce,**  
VP and Head of Global Intelligence Operations

---

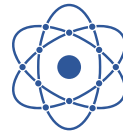
**As we move into 2019, one concern of mine is supply chain attacks. Last year, we observed at least five software supply chain compromises, and to us that's a huge increase over what we had been seeing in the past. The supply chain can offer attackers access to multiple high value targets so that they can capture a wide range of information. Plus, if the threat actor is targeting deep enough in the supply chain, there's a good chance that they can operate unnoticed.**

We have also seen industrial control systems (ICS) attacks become more sophisticated. Most notable is the TRITON malware we recently shared with the public — malware that was actually attacking the safety systems of a critical infrastructure organization. That's particularly disturbing because it is not a reconnaissance play in this case, but someone actually attacking the safety systems. It's worth noting that while the type of persistence and resources it takes to conduct these sorts of attacks would traditionally indicate more of a nation-state actor, we are seeing the knowledge gap for ICS attacks closing. Intrusion and attack tools are increasingly being made available in underground marketplaces. This is a big shift. It's not an immediate cause for alarm, but it is certainly something to keep a close eye on as we move into 2019.

One additional area of concern going into 2019 is an increased use of mobile malware. Mobile malware isn't anything new; however, we're seeing increased capability in this area. As cyber threat actors emerge from developing countries in southeast Asia, Africa, and the Middle East where citizens rely primarily on mobile, we expect to see this trend increase even more.

When it comes to these threats, all industries are at risk and no one can rest easy. That said, one notable industry to keep an eye on in 2019 is manufacturing — everything from firms assembling cars to pharmaceutical companies making medicine. The primary reason for this is that manufacturing operations have a very broad attack surface, especially with an expanding Internet of Things (IoT) increasing connectivity every day and reliance on the supply chain in manufacturing processes. Plus, adversaries simply have plenty to gain from breaching organizations involved in manufacturing, making the industry an even more attractive target.

It won't be an easy fight. The biggest problem facing all organizations is the dearth of expertise. Organizations may have every intention of addressing the security gaps and mitigating breaches, but many simply don't have the manpower. One thing FireEye is working on for 2019 is being able to offer expertise on demand, which will allow organizations to address problems without needing to hire 20 or 30 people. They can simply tap into FireEye's expertise as they need it and as the situation warrants. This type of assistance is going to be a huge help to all organizations in the future, especially those that don't have the resources to fully build out their security teams.



## 5 to 20 Years

The other technology is quantum computing. The estimates for when quantum computing (and quantum key distribution, which is already going on) will really take off range anywhere from 5 to 20 years from now.

Longer term in 2019 and beyond, there are two major technologies that everyone knows about, but that many people don't take very seriously. One is artificial intelligence, which has been a buzzword for a while. This really is going to change the threat landscape. Imagine artificial intelligence being used to not only probe, but to specifically tailor attacks against organizations and other targets. We're already seeing some of this with deep fakes, the ability to copy the voice and mannerisms of a person to create something that looks and sounds as though the real person said it.

The other technology is quantum computing. The estimates for when quantum computing (and quantum key distribution, which is already going on) will really take off range anywhere from 5 to 20 years from now. With that technology, the scaling of computations goes up dramatically, to the point where the time needed for breaking traditional encryption would shrink to weeks, or maybe even minutes. This means breaking some of the foundational encryption we see in use today such as RSA. Currently, physicists and mathematicians are looking at quantum resistant algorithms to try to stave off the threat, but if you think about it, whoever gets there first will have the opportunity to defeat encryption for not just the things they're looking at now, but all of the legacy encryption protecting historical information. It provides a tremendous informational advantage to whomever develops quantum technology.

Today, many countries around the world are making huge investments into quantum computing, and there is a race to get there first. This may not be for another 20 years and may not be a critical item right now, but one thing we do know is that some of the same adversaries we see conducting cyber attacks and cyber espionage today are also heavily invested in this technology. They're already using a related technology — though not the same — called quantum key distribution, which is essentially an encryption that is unbreakable at this time. Countries such as China are already heavily invested in it, so if we're looking out to the horizon, this is a technology to prepare for now.

One final thought as we move into 2019: remain skeptical about what you read, especially on the internet. Historically, when we would think about influence operations and the ability to influence the way people think (either through social media or through some other type of manipulation campaign), Russia would come to mind. Russia has been conducting influence operations for a really long time, and not just in the cyber realm. They're very skilled. We're seeing other threat actors learning from Russia's success in cyber influence. For example, we recently uncovered several Iranian inauthentic accounts being used to propagate a social agenda that was pro-Iranian. We're going to increasingly see these cyber operations from more nations than just Russia, and now Iran, as nations realize how effective this tactic can be. The upside of social media is that everyone can be part of the conversation, but that can clearly be a downside as well.

# A View from the Clouds

**Martin Holste**, Chief Technology Officer for Cloud



Do you have visibility for the things that are going on in the cloud, and are you able to set up your security operations center (SOC) to be able to respond to something that happens?



**There have been a lot of cloud-related challenges throughout 2018 and we expect to see those continue and evolve as we move into 2019. First, a lot of data is moving to the cloud and the attackers are going right along with it. We're seeing a massive uptick in the number of incidents that involve cloud, and that's really just attackers following the data. It's not really about cloud being more or less secure. I talk about that a lot with customers — that attackers will always go where the data is. We've seen a lot of advanced attacks involving cloud, and we've seen some not-so-advanced attacks. Either way, the attacks are happening and that means organizations need to be vigilant. Really, the question you should be asking is: Do you have visibility for the things that are going on in the cloud, and are you able to set up your security operations center (SOC) to be able to respond to something that happens?**

The big challenge of the cloud is that the attack surface is everything. Organizations still have a lot to do when it comes to cloud security, and in 2019 they really need to be asking the right kinds of questions. Do you know who is logging into your infrastructure right now? Do you know who is accessing it? If someone downloads a file, do you know if they were supposed to download it? There is less of a focus on the bits and bytes — things such as buffer overflows — and a lot bigger focus on the business logic, and understanding: Are the things that are happening supposed to be happening? Is there anything anomalous? Also, does your security operations center have time to investigate these things? And that gets into automation. You need to be able to automate easier tasks for cloud, to say, we can do vulnerability management, we can do firewall rules, we can do all the easy things that need to happen so our security operations can focus on finding unusual activity and making sure everything is normal.

A lot of the attacks that are happening in the cloud just happen to be happening in the cloud. As in, it's a virtual machine that could be running on-premises yet happens to be running in the cloud. Sometimes an attacker will infiltrate an on-premises network and then move into the cloud from there, and sometimes vice versa. That's something to be mindful of in 2019 — monitoring connections between your hybrid data center that's on-premises and your cloud is really important.

Perhaps the number one thing for cloud security is email security, because phishing is just so hard to defend against. That's the number one way that attackers are coming through, and we don't expect that to change in 2019. By default, cloud is a lot more secure for things such as buffer overflows and SQL injection. Many of the tried and true attacks of five years ago don't work very well in the cloud. On the other hand, calling up tech support and pretending to be someone works really well, and we will continue to see that tactic. Attackers are starting with

credentials and moving laterally from there. That's why visibility is so important, and automating what you can is so important, because it takes a real investigation to decide whether something that happened was supposed to happen — versus looking for a known malicious pattern.

I think the big innovation we are going to see as we move into 2019 is a focus on business logic and visibility. It's the idea of needing to know who's doing what at all times if you want to be able to defend against a bad actor. Organizations need to be aware of what's going on within the business, and that doesn't just mean financial aspects, it means files that are being downloaded, virtual machines that are being booted, and even use of two-factor authentication.



**...the number one thing for cloud security is email security,** because phishing is just so hard to defend against.

One technique we've seen attackers use to bypass two-factor authentication is SIM card spoofing. When you get a new phone, the clerk will stamp out a new SIM card with your phone number on it. If you can convince someone to stamp out a card that doesn't have your phone number on it, then you can bypass a lot of two-factor that way. We've seen this tactic being used to steal social media accounts, where attackers will figure out the phone number of someone who owns a sought-after account, and they are able to gain access to and later sell the account. These attackers go through the effort of going into a boutique store, and they use social engineering to get a new SIM card, or there is an employee on the take who will create it.

As organizations continue migrations to the cloud in 2019, they need to ask the right security questions. I hear organizations saying, "Well, I want to make sure I have the same security that I had on-premises in the cloud." That's not really the right way to think about it. It's a good place to start, but you need to be asking the extra question,

which is: "Okay, cloud is different, it's a lot more about who is doing what, so can I do things like understand why a box was booted? Can I know whenever an admin logs in? And who's checking on that on a regular basis?" Enabling your operations center to answer those questions requires automating out all the less interesting stuff so they can focus their time on the real human side of the investigation.

Analytics are going to be a good way to automate simpler tasks, but you are never going to automate away the human component — some activities require a phone call. It's really hard to get a machine to do everything right all the time, and having a human to follow up is critical. However, it works in conjunction with artificial intelligence (AI) because AI can take you to weird and interesting things. But it's going to take a human to sort them out. And that's one of my biggest concerns — that SOCs aren't spending enough time making sure that all those hunting activities are actually occurring.



# Leaving on a Jet Plane

**Christopher Porter**, Chief Intelligence Strategist



Due its pervasive nature, **the best defense against cyber espionage is rapid, detailed information sharing with context.**

**On Sept. 6, 2018, I had the opportunity to testify before the House Homeland Security Committee and share FireEye's insight into threats to America's aviation sector. It was a great honor to be invited and a lively conversation with Committee Members and their staff who posed some tough and important questions to me and my fellow panelists. Our goal was to "right size" the threat — to point out areas of real concern for the United States and the aviation sector, but also to reign in alarm that persists in some corners though is not supported in fact.**

First, to answer the question at the front of everyone's mind: Can someone hack a plane? I have learned to never say never, and the most sophisticated cyber threat groups have repeatedly generated technical and operational surprise across many sectors, including disabling threats to physical systems. But this question is outside FireEye's expertise. We defend airports, aircraft manufacturers' development and production networks, and federal agencies tasked with regulating and protecting the aviation sector. We do not currently defend the aircrafts themselves, so on this one I defer to the experts at DHS, who found in a study made public in 2017 that such a threat was at least technically feasible.

While we should stay attuned to cyber-enabled physical threats to aircraft and supporting systems, a far more common threat that security teams in the aviation industry must be prepared to defend against is cyber espionage. Due its pervasive nature, the best defense against cyber espionage is rapid, detailed information sharing with context. FireEye pushes alerts to customers in real-time, and industry groups share information between peers because, as we have learned, a threat to one is often a threat to all.

Aviation is one of our nation's leading export industries, and China in particular is harnessing all aspects of national power to displace the U.S. as a military and economic power in Asia and worldwide. Despite a successful U.S.-China agreement to halt intellectual property theft, I predict that, as defense competition between the two countries intensifies over the next decade, so will cyber espionage. It is safe to expect targeting of U.S. aerospace researchers, manufacturers and aviation operations more generally.

Cyber criminals likewise pose an economic threat to the aviation sector and its customers. For years we have seen airlines and third-party ticket sellers exploited so that illicit tickets could be resold for profit on the dark web. Because airlines are trusted by their customers with a wide variety of sensitive personal data, they are also frequently targeted by cyber criminals looking to gather data to enable other types of fraud.

In the last two years, our devices have detected a sharp increase in the use of ransomware to temporarily disable airline ticketing and support operations. Air travel is a time-sensitive business, and cyber criminals know that they can extort quick payment from airlines that are unable to move passengers until their systems are decrypted.

When airports themselves are the victims, it can be unclear which entity is responsible for responding to the threat. Some aviation infrastructure is privately owned, and some is owned by states, by local governments or a combination of all three. When the threat is a foreign military-backed threat group, airports might reasonably think that the U.S. military or federal government will be responsible for defending them. I remain concerned not only by the threats that are posed, but by the level of preparedness in the United States to be resilient in the face of cyber threats to aviation — in part because of the risk of confusion during a time of crisis. When FireEye hosts practice exercises for clients, drawing in a variety of stakeholders to simulate response to a crisis created by a cyber attack is key, but it still isn't common.

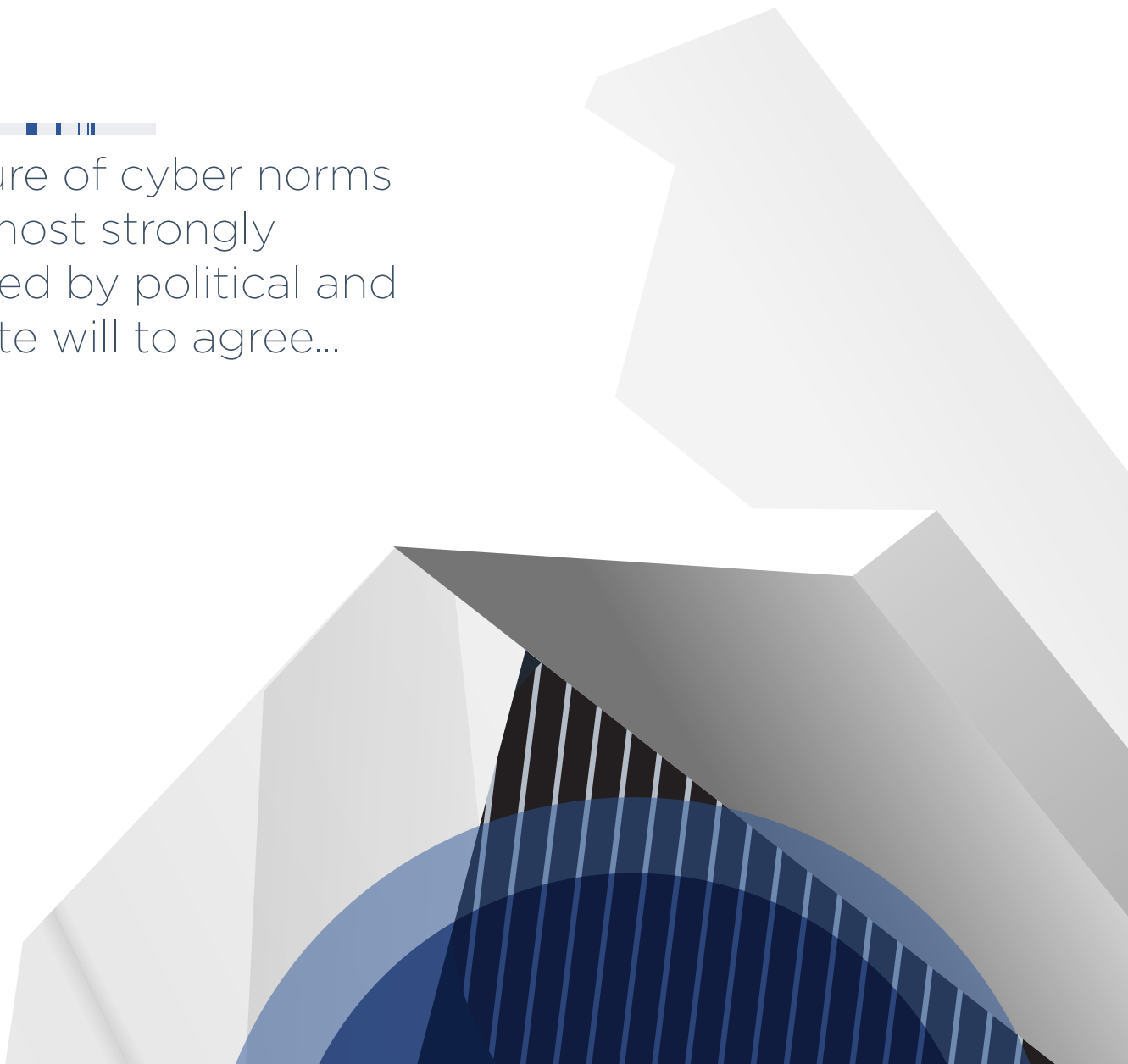
Many aviation systems may even be unintentional targets, where criminals seeking to turn a quick profit instead stumble into causing more serious disruption — exactly what seems to have happened to a British airport the same afternoon as my public testimony. Terrorist groups likewise target aviation for cyber attack, to draw attention to themselves as much as to cause any disruption.

At the end of the day, the primary victims in these situations are members of the public who may wrongly fear that they or a loved one is at risk, or who become increasingly distrustful of flying. Communications are key, and it starts with the public being made aware of the difference between taking down systems that cause inconvenience from those that directly support flight operations and passenger safety.

# From the Files of FireEye Threat Intelligence



The future of cyber norms will be most strongly influenced by political and corporate will to agree...



### Restructuring of Chinese Cyber Espionage

We believe notable restructuring in the Chinese cyber espionage apparatus has taken place since at least 2016, resulting in a resumption in the pace of activity. We assess that this reorganization will inform the growth and geographic expansion of Chinese cyber espionage activity through 2020 and beyond. The changes so far have been gradual, and driven by several high-profile events and official motions, including the Obama-Xi agreement shifting Chinese cyber espionage operations away from intellectual property theft, the People's Liberation Army (PLA) consolidating most cyber-related functions under the newly formed Strategic Support Force (SSF), and China beginning initiatives in line with the 13th Five Year Plan (2016-2020), formally shifting national priorities.

Since the decline of observed Chinese cyber espionage activity against the U.S., as cataloged in our **Red Line Drawn report**, we noticed some groups have slowly resumed activity. In most of these instances, the groups have re-emerged with new malware, modified tactics, techniques and procedures (TTPs), and/or different geographic targeting patterns. In other cases, actors who were part of dormant groups may have been reorganized into new operational teams or reassigned to existing known groups.

### China's Belt and Road Initiative to Drive Cyber Espionage Activity in 2018 and Beyond

The Belt and Road Initiative (BRI) is an ambitious, multi-year project across Asia, Europe, the Middle East, and Africa to develop a land (Silk Road Economic Belt) and maritime (Maritime Silk Road) trade network that will project China's influence globally. We expect BRI to be a driver of cyber threat activity.

Cyber espionage activity related to the initiative will likely include the emergence of new groups and nation-state actors. Given the range of geopolitical interests affected by this endeavor, it may be a catalyst for emerging nation-state cyber actors to use their capabilities. Regional governments along these trade routes will likely be targets of espionage campaigns. Media announcements on BRI progress, newly signed agreements, and related development conferences will likely serve as operational drivers and provide lure material for future intrusions.



### **Iranian Cyber Threat Activity Against U.S. Entities Likely to Increase Following U.S. Exit From JCPOA, May Include Disruptive or Destructive Attacks**

Following the signing of the Joint Comprehensive Plan of Action (JCPOA) in 2015, the tempo and nature of Iranian nexus cyber activity changed in two key ways. First, there was a significant drop in destructive and disruptive operations. Second, we observed a reduction in Iranian-nexus activity probing critical infrastructure.

Last year, we reported that should the U.S. withdraw from the JCPOA, we suspect that Iran would retaliate against the U.S. using cyber threat activity. This could potentially take the form of disruptive or destructive attacks on private companies in the U.S. and could be conducted by false front personas controlled by Iranian authorities purporting to be independent hacktivists. While we do not anticipate such attacks in the immediate or near-term, we suspect that initially Iranian-nexus actors will resume probing critical infrastructure networks in preparation for potential operations in the future. Organizations and asset operators across all critical infrastructure sectors in the U.S. should be prepared to defend against Iranian threat groups that have demonstrated a focus on disruptive and destructive attacks.

### **Cyber Norms Unlikely to Constrain Nation-State Cyber Operations in the Near Future**

Norms of responsible state behavior in cyberspace, though still in their infancy, have the potential to significantly affect the types of future cyber operations conducted by nation-states and their proxies in the long term. Norms can be positive or negative, either specifically condoning or condemning a behavior. The future of cyber norms will be most strongly influenced by political and corporate will to agree, and ultimately decisions by particular states to accept or disregard those norms in their conduct of cyber operations.

Various countries active in cyber diplomacy, along with a small number of international corporations, are exploring norms to manage their increasingly complex and crowded cyber threat landscape. However, except for an emerging consensus to not conduct cyber-enabled theft of intellectual property with the intent to provide commercial advantage, no norm has yet found significant, explicit agreement among states. Companies, on the other hand, are increasingly moving forward with several new propositions, including the Charter of Trust and the **Cybersecurity Tech Accord**.



**Publicly Available Malware Usage by FIN and APT Groups**

Although nothing new, we expect to see continued growth in the usage of open-source malware by espionage and financially motivated actors. While there are a variety of reasons why advanced threat actors may choose to use a publicly available tool, the two likely drivers of employment include the intent to frustrate attribution efforts and reduced cost of development. Additionally, the modularity of penetration testing frameworks such as Cobalt Strike allows adversaries some flexibility in the payloads they deploy. Examples of open-source malware that have been observed being used by APT and FIN groups include NETWIRE, TRINITY, GHOST RAT, METERPRETER, ASPXSPY, and others. In recent months, Cobalt Strike and PowerShell in particular are two platforms that are growing in popularity with actors.

**Abuse of Legitimate Services for Command and Control**

Cyber espionage and financially motivated actors have abused legitimate internet services for command and control (C2) purposes during cyber operations since at least 2008. Leveraging legitimate, often whitelisted services makes C2 traffic more difficult to detect and may provide another layer of obfuscation between a threat actor and malicious activity, though it also generates additional development and infrastructure overhead for attackers. The percentage of malware samples analyzed by FireEye from 2006 to 2016 that used legitimate services for C2 increased from approximately four percent in 2008 to nearly nine percent in 2016, and we believe this will continue to grow into 2019 and beyond.

# On Assignment with FireEye Mandiant



Expect to see a spike in financial threat actors targeting e-commerce websites and gift cards.

### **Russian Targeting Broadens, While Emerging Nations Scramble to Keep Up**

New attempts to conduct ICS attacks by Russian actors will emerge. These will likely be testing or prepositioning of tools rather than actual disruptive or destructive attacks, but geopolitical events could lead to actual attacks in some geographies, particularly Ukraine or other former Soviet republics.

Russia will continue to conduct influence operations, both via inauthentic media and through more covert operations such as hacking and tactically leaking data in ways that may sow discord. One focus of such operations will be the Middle East, where Russia has an interest in maintaining the split between Gulf Cooperation Council (GCC) countries (namely Saudi and UAE) and Qatar, all regional U.S. allies.

As we have seen with the rise of Iran, North Korea, and Vietnam over the past few years, we can expect many other emerging cyber nations to come to the fore in 2019. This will be driven by many factors, but the primary reason will be the pressure to keep up with other nations and to develop a cyber program similar to that of a traditional military capability.

Iranian attackers in particular will continue to improve capabilities, even as we see new, less capable groups emerge supporting Iranian government goals. This will continue the trend of growth in both sophistication and volume of attacks by Iran.

### **A Continued Shift from Point of Sale to E-commerce Environments**

We expect to see an increase in attacks on e-commerce websites, as well as gift card fraud. In the U.S. retail industry, the move to chip and signature and mobile payment (e.g. Apple Pay) has made it more difficult for hackers to profit from theft of credit card data. In several point of sale (POS) breaches we worked, the banks reported surprisingly low fraud rates because the attackers didn't have the full magnetic stripe (track 2 data).

Expect to see a spike in financial threat actors targeting e-commerce websites and gift cards. In our 2018 investigations, we've already seen attackers install e-commerce "skimmers" to steal personally identifiable information (PII), payment card numbers and CVVs. Once the criminals have this data, it's relatively easy for them to make purchases or sell the information on the dark web.

### Online Banking Portals in the Crosshairs of Attackers

Attacks against online banking portals and applications are becoming more sophisticated and will likely become more attractive to cyber criminals in 2019. Recent attacks against two North American banking portals showed attackers spending significant amounts of time on reverse engineering the account registration, and authentication workflows. The threat actors then designed a sophisticated attack that combines card enumeration, session corruption, brute forcing, and password spraying techniques to compromise banking credentials and bypass step-up authentication.

Once the attacker gained access to the account, they were able to initiate online fund transfers, order checkbooks and update the destination for the existing transactions. In most cases, the typical vulnerability assessment practices would not pick these vulnerabilities up since identifying them required a much more focused and customized approach than the automated means available through security tools.

We expect large-scale account takeover attacks against online portals will increase, and we could very well see a few cases of large fraud as a result of these attacks.

### Target: Supply Chain


In 2019, we expect to observe an increase in both state sponsored and financially motivated supply chain attacks. As organizations have improved their posture and built up their perimeter defenses, attackers will shift their focus to compromising third party vendors, customers or partners with the goal of gaining access to a target's network.

We recently saw APT10, a Chinese espionage group, compromise service providers in Canada and the U.S. to gain access to a target's network. We assess APT10 is particularly focused on compromising the supply chain of major U.S. companies in order to enable the theft of business-sensitive information and enhance targeted technology theft by non-cyber means, without violating the Xi-Obama Agreement by directly stealing intellectual property via cyber means. We have also seen software-based supply chain attacks being used by both state sponsored groups such as North Korea's Lazarus and China's APT31, as well as financial actors, to bypass detection controls by exploiting the intrinsic trust that many organizations and security vendors put on known software development companies (certificate theft).

Last year, there were seven significant software supply chain events that were made public. These attacks may involve embedding backdoors in legitimate software, using stolen certificates to sign malicious files in order to bypass detection or subverting the update process for a software to download and execute malicious code during an update process.

Most organizations are not great at managing supply chain attacks as they are difficult to detect, and require much more effective vendor risk management practices than are currently being enforced.

# Under the Lens of FireEye Labs



**Social engineering is the most commonly used attacker technique** because it works, and end of the year predictions is the perfect time to remind users that they should always be on the lookout for this tactic.

### **As the Threat Landscape Evolves, So Does Security**

With technology constantly evolving and the IoT growing by the minute, the threat landscape is expanding exponentially. As a result, new strategic defenses will arise as part of technology architectures to combat these threats.

Availability of features and transfer of code that could be used to exploit and/or run active codes will be minimized. We are already seeing this in progress with the reduced usage of features such as Flash and Java. Macros, and even sharing of documents, may very well disappear. This will be enabled by cloud and secured by walls around concepts such as “apps” and “containers” as services. Essentially, business productivity and collaboration will happen in isolated and/or virtual environments, while appearing more open than ever, increasing the flow of information and content.

Moving forward, we also expect the IoT will have less information, and fewer resources and actual features to exploit. The attacks that can and do leverage the future IoT will be very complex and hard to detect and defend against. There will, of course, always be emerging next-generation endpoint, network, cloud and other security technologies to help, but it will be an uphill battle.

### **Business Email Compromise Leveraged in Targeted Attacks**

Social engineering is the most commonly used attacker technique because it works, and end of the year predictions is the perfect time to remind users that they should always be on the lookout for this tactic. We will see all sorts of phishing and spear phishing tactics being leveraged in targeted attacks, but specifically, we expect to see more cases of CEO fraud, or business email compromise (BEC). With today's solutions becoming increasingly successful at detecting phishing attacks and other email scams, BEC is expected to spike significantly, so employees should be extra vigilant when it comes to emails from key individuals in their organizations — especially when the email requests some type of action to be taken.

### Use of Emerging Technologies to Evade Detection

As discussed in last year's FireEye security predictions report, we have been seeing a steady increase in cyber criminals adopting cloud-based infrastructure to carry out sophisticated attacks. That was true throughout 2018, and in 2019 and beyond, we expect to see the use of emerging technologies such as blockchain and AI to obfuscate attacks.

Also, with the increase in the number of AI-based cyber security products deployed in organizations, and security vendors innovating to bring new AI-based security products to the market, attackers will begin adapting their behavior accordingly. Next year we are expecting to see use of new techniques to evade AI-based solutions, including threats that blend in with normal traffic and threats that provide misleading data to challenge and disrupt machine learning models.

### Other Evasive Maneuvers

Attackers leveraged a number of unique and original evasion techniques in their attacks throughout 2018, and we expect to see those techniques returning in 2019, along with some new innovative evasion methods. One such technique that will likely increase due to the success it has is password protected attacks. In 2018, we saw password protected malicious attachments in emails, with the password being sent as an image attachment. An unsuspecting user who followed the instructions and opened the attachment would become compromised.

While those password protected attacks are a little more spray-and-pray, we expect similar trends to dominate the targeted attack space. Attackers will continue to introduce new ways to evade detection by security vendors. Use of WMI-based queries to profile the execution environment was prominent in targeted attacks this year, and due to that success there is no doubt it will return next year. Attackers will also continue using GeoIP and user agent-based evasions in their attacks, as well as new file types to dodge protections. Finally, expect attackers to find new and innovative ways to defeat sandbox environments.



# Global Insights: **APAC**

The impact of skilled individual attackers and nation-state actors with skills but insufficient resources **will be felt more strongly by organizations that have failed to keep up with security developments.**



### Sights on the 2020 Olympics in Tokyo

If history is any indication, we should expect to see an increase in threat activity targeting companies and organizations in Japan throughout 2019 and leading up to the 2020 Olympics being held in Tokyo. The industries we expect to see being targeted include critical infrastructure, media and broadcasting, government, tourism and hospitality, and local and international Olympics organizing committees. The threat activity we are most on the lookout for ranges from phishing and fake ticket websites, to distributed denial of service (DDoS) attacks, to ransomware distribution, to intellectual property theft.

Additionally, there is great interest in Japan from nation states such as North Korea and China, so we can expect threat actors from these countries to be performing reconnaissance and testing defenses prior to the main event. The 2012 Summer Olympics in London were targeted, as were the 2016 Olympics in Rio, so it's likely the pattern will continue.

### Threat Evolution

In 2019, we expect to see less-skilled actors gain access to better social engineering, better tools and broader targets. The continuing moves to cashless societies will see low value theft become more difficult to detect, and the large banking organizations will see that it is cheaper to manage the issue by paying back the low value theft rather than putting much effort into stopping it. The low-end criminals will continue to see value in targeting individuals rather than better secured organizations.

The impact of skilled individual attackers and nation-state actors with skills but insufficient resources will be felt more strongly by organizations that have failed to keep up with security developments. We will see more instances of large volumes of data extracted from such organizations.

Highly skilled and experienced actors will move into a mature espionage/criminal layer. They will better blend into the background and be even more difficult to detect and deter. Chinese and Russian actors will expand their operations significantly; however, the use of commercial software and the drive to maintain access to a system will mean they will place a greater emphasis on hiding who they are and what they want.

# Global Insights: **EMEA**

With attribution, cyber criminal activities will hopefully become harder to execute in the long run, **and this could bring deterrence.**

### **The Dark Side of Social Media**

In 2017 and 2018, we saw social media serve as a platform for information operations and disinformation driven by individuals, political parties and foreign nations. While there have been many ongoing discussions and hearings in United States Congress, in the EU and the UK, not much has been accomplished.

In the last half of 2018, FireEye announced an extensive network of information operations — presumed to be driven by the political interest of Iran — that involved social media. With the upcoming elections across EMEA in 2019, we predict that social media will continue to be the leading platform to produce information operations driven by foreign countries with a strategic interest in a particular state or a region. The mission could either be to promote a particular political party that might be friendlier towards specific foreign policies, or to drive a political narrative, causing conflict within the country.

In 2019, we expect influence operations on a large scale with major nations, but also use of influence in media and on social networks with regard to local conflicts in Eastern Europe, as well as in APAC and in other parts of the world. These types of campaigns will be more difficult to detect due to their nature, and it will be challenging for cyber security companies and governments to detect and deter the authors. Attribution will be key.

### **Lack of Resources Introduces Risk**

In our previous yearly predictions for EMEA, we talked about the increasing lack of security resources. Companies continue to struggle to hire qualified security professionals, and therefore we continue to see organizations either outsource or hire external companies to help drive security.

Outsourcing and partnering with third-party managed service providers can help companies mature their cyber defense capabilities, but if vendor or provider security capabilities are not assessed, there may be a heightened risk of compromises. In recent years, we have seen increased interest from cyber espionage threat groups, as well as less organized cyber criminals, in targeting (managed) service and security providers, contractors and outsourcing companies to carry out their mission.

We expect this trend of targeting the supply chain — both vendors and software — to continue, and recommend that companies conduct security assessments of products, providers and potential software to assess and understand the cyber security maturity within the provider, vendor or supplier.

### The Fight Begins with Attribution

In August 2018, the United States Department of Justice announced that three members of FIN7 were in custody. The arrest of **FIN7 members was significant** because it highlighted the importance of how the right collection of intrusion data, threat research, incident response and sharing between security companies can improve attribution, which can lead to actual arrests of cyber criminals.

Europe, and in particular Eastern Europe, has a long history of having a strong cyber criminal element, and while cybercrime is indeed borderless, many activities can be traced to countries where there is either less interest in conducting arrests or where there are no global agreements for potential extradition to other countries.

With attribution, cyber criminal activities will hopefully become harder to execute in the long run, and this could bring deterrence. In 2019, we expect to see more arrests made in the cyber criminal ecosystem based on reliable and accurate attribution. It is vital that cyber security — and in particular cyber threat intelligence — provides attribution, thus supporting enterprises, governments and law enforcement in an ongoing effort to combat cyber criminals.

### Critical Infrastructure Attacks Looming

In late 2017, we announced the findings of a new ICS attack framework that we named “**TRITON**.” TRITON is a significant discovery and worth mentioning in this report because it highlights the continued threat to critical infrastructure.

Critical Infrastructure covers many things, and for EMEA it is also sometimes cross-border infrastructure, providing either energy, power or resource extraction. In 2019, we expect to see an uptick in threats towards critical infrastructure. Because many of these environments do not have a unified security strategy between information technology and operational technology, we could potentially see a cyber attack causing disruption or destruction within critical infrastructure elements.

We will probably also continue to see attackers trying to interfere directly with operational technology networks to disturb business, ask for ransom, or for geopolitical reasons, as well as to demonstrate their capabilities. Due to its diversity and the number of plants deployed over the continent, Europe will be a target of these attacks in 2019. We could see threat actors on very old platforms where security and forensics are difficult to manage.

It is vital for countries and companies that rely heavily on ICS to address gaps between discovery and recovery of threats, as well as ensure they have capable security controls in place to identify risks as early as possible.



# Global Insights: **LATAM**



**Regions such as Latin America and Africa will become targets of more impactful attacks,** which will be relevant enough to gain coverage in media outlets around the world.

## **LATAM Threat Landscape, At a Glance**

Cybercrime, cyber espionage and hacktivism are some of the primary threats impacting the region, and we expect that to continue into 2019. Next year, we expect to see regional groups improving their TTPs to execute various campaigns. Spear phishing will continue to be the primary attack vector; however, we expect to see an uptick in supply chain attacks and end user attacks focused on telecommunications devices and IoT devices.

These improved TTPs will most likely be used in attacks against the financial and manufacturing industries; however, government, technology and services will also be within scope, with the latter two having a high chance at being targeted in supply chain attacks.

China will be seen as an imposing threat in the region, especially considering incidents associated with tampered hardware that is manufactured in the country. North Korea, Russia, and Iran will continue their standard activities, while cyber criminal groups from Africa and Latin America will improve and become more relevant.

Regions such as Latin America and Africa will become targets of more impactful attacks, which will be relevant enough to gain coverage in media outlets around the world. This will force companies with a presence in those regions to increase investments in security, and local government to enforce more laws and regulations. This will likely lead to newer attack groups being profiled and campaigns being attributed to them, which will hopefully lessen the threat.





# 2019 AND BEYOND

**While we have a lot to look forward to in 2019, we also have a lot we need to address and - as Kevin Mandia says - a lot we need to get right.**

Attribution and accountability are two of the biggest sticking points when it comes to winning the war in cyberspace. Without risks and repercussions for malicious activity carried out on the internet, attackers will keep attacking and organizations will keep getting breached. Recent indictments for hacking have offered a little hope for what could be, but more progress has to be made on this front to reduce the number of breaches we're seeing every year.

The cloud offers great opportunities for organizations and we will continue to see more migrations to the cloud as we move into 2019. We also expect to see more attacks targeting the cloud. It's not about whether the cloud is less secure, it's that attackers will simply go wherever there is data. As Martin Holste says, cloud security is about asking the right questions. Following up on even remotely questionable actions and activities taking place in the cloud goes a long way.

It's tough enough to imagine that hacking an airplane is considered feasible, but the aviation industry has a lot of other cyber issues to consider as well, including cyber espionage, customer information theft, illicit ticket sales, and extortion via ransomware and denial of service. Possibly the biggest outcome of all this is erosion of trust and fear of flying, which could have a more severe impact on the aviation industry than a breach.

Unfortunately, there is 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. We need to take it one step at a time — develop the right technology to automate easy tasks, build up trained security personnel to follow-up on critical alerts, and have published doctrine on rules of engagement in cyberspace.

We fully embrace that vision and look forward to leading the charge in 2019 and beyond.

To learn more about FireEye, visit: [www.FireEye.com](http://www.FireEye.com)

---

**FireEye, Inc.**

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

© 2018 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. SP-EXT-RPT-US-EN-000088-01

**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.

