FIREEYE™ | MANDIANT®

A GLOBAL RESET

Cyber Security Predictions 2021

The most reliable way to **predict** the future is to **create it**.

—Abraham Lincoln

A CONFIDENT APPROACH TO UNEXPECTED CHANGES

Companies across all industries commonly release forward-looking reports about what's to come in the next year, but nobody in 2019 anticipated the global pandemic or the worldwide reaction to it. In one way or another, our personal lives were upended. Organizations were forced to make decisions that fundamentally, and perhaps permanently, changed the way they do business.

While 2020 was filled with great uncertainty, there are still guarantees in the cyber security realm. Threat actors will continue to attack without any regard for the challenges faced by their targets. These actors continue to be motivated by espionage and monetary gain, though their TTPs will always evolve. This means organizations will continue to be breached, resulting in business disruptions, data compromise, reputational harm, and almost always a financial loss.

Knowing what we know, and with a constant eye toward the future, we have compiled a list of cyber security expectations for the coming year. In this report, *A Global Reset: Cyber Security Predictions 2021*, we tackle the following topics: remote work and other impacts of the global pandemic, ransomware, nation-state activity, cloud security and security validation.

We extend a huge debt of gratitude to the many FireEye and Mandiant Solutions people and teams that helped make this report happen. In particular, this report would not be possible without the expert insights provided by our various leaders, including Sandra Joyce, EVP of Mandiant Threat Intelligence; Major General Earl Matthews, VP of Strategy; Dave Baumgartner, CIO; Martin Holste, CTO for Cloud; and John Hultquist, Senior Director of Intelligence Analysis.

Now let's take a look at the security forecast for 2021.

Despite the urgency of their work, threat actors will continue to **target healthcare** providers and **vaccine makers.**

REMOTE WORK AND OTHER IMPACTS OF THE GLOBAL PANDEMIC

In the near term, the coronavirus will likely continue to have a significant impact on normal business operations, with a focus on supporting remote work, virtual events and new productivity platforms. The pandemic forced almost every organization to become better at operating under significantly changed working conditions and in the wake of a changing environment, IT and IT security challenges will most likely persist throughout 2021.

In the longer term, technology solutions will step in to facilitate the return to work, school and other activities, potentially introducing new risks for privacy, personally identifiable information (PII) and protected health information (PHI). Similarly, the desire to reduce the risk of human exposure may further accelerate the shift to autonomous vehicle and robotic solutions in transportation, manufacturing and other fields.

Virtual private networks (VPN) will continue to have their place in 2021. Tunneling is the most-used method for accessing remote resources. Organizations should be ready to have this capability in place as remote work continues to expand and becomes a more common way of doing business.

The pandemic has highlighted the importance of face time with colleagues. Seeing one another when we speak, or simply hearing a voice, really goes further than an email. From a security perspective, one consideration is the security of the webcam on whatever device is connected to it. Based on increased use of such technologies, we expect to see chief security officers and cyber operations teams continue to mark a number of niche areas as high priorities for spending as we go into the next year.

When looking at other priorities for spending in 2021, we definitely expect to see a continued increase in perimeter security, mostly due to remote work. Increased spending on ecommerce security due to increased activity is also expected, resulting in higher spending on a pay-per-seat or pay-per-megabyte license, and ultimately causing companies to shift additional funds away from in-house systems to more outsourced services. Remote access will continue to be explored, especially around helpdesk and related employee interfaces.

Unfortunately, we're already seeing the targeting of hospitals, manufacturing groups and related critical infrastructures dedicated to development and distribution of a COVID-19 vaccine. That targeting likely won't abate in 2021, so organizations and defenders will need to remain vigilant. Telehealth should also remain alert, because many patients are getting their initial evaluations with doctors from a web interface. Similarly, many educational institutions are reliant on telecommunications and web interfaces to educate children and the emerging workforce.

We have seen increasing numbers of state-sponsored actors targeting coronavirus research, treatment and response efforts. This direct targeting of government, healthcare, pharmaceutical and non-governmental organizations will likely continue due to the high-value information involved. We are seeing both Iran and China starting to target not only research companies, but also other health and biotechnology companies, and they will likely continue to lead the way in terms of COVID-19 espionage. The U.S. government has already publicly accused China, Russia and Iran of trying to hack into one of the global research firms.

When it comes to cyber security, organizations dedicated to supporting COVID-19 recovery efforts are going to have to start thinking outside the box in 2021. For example, some bioresearch companies are having their workforce operate from air-gapped computers, meaning those systems don't have access to the internet. As a best practice to mitigate threats, we recommend that anyone doing research—whether for IP or for other sensitive work—restrict their pursuit of that research on specific computers that are not used for any other purpose.

Ransomware is now a **national security issue** for the United States and for countries around the world, and it will only **get worse**.

PERSISTENCE AND GROWTH OF RANSOMWARE USAGE

The use of ransomware accelerated and became more dangerous than we've ever seen in 2020. Targeted attacks against medical facilities during a pandemic crossed a new line. This followed another first earlier in the year, when the use of ransomware was linked to the death of a person. A hospital in Germany was experiencing a ransomware attack and they had to turn away a patient. The patient was diverted to another hospital and ended up passing away in the ambulance.

We expect ransomware to continue its rapid growth in 2021, with ransomware varieties increasing along with frequency of attacks. One troubling trend is that attackers are not only making adjustments to their ransomware TTPs, but also increasingly moving to ransomware-as-a-service, which includes offering malware and the skills to deploy it on a one-time or ongoing basis.

In 2021, threat actors will increasingly target the most critical assets held by organizations. Through post-intrusion reconnaissance and the deep enumeration of networks, we currently see threat actors locking up the most relied on and sensitive data and architectures, which leads to much higher ransom amounts. Ransoms have already reached the tens of millions of dollars, and we expect these demands to get worse.

While many organizations pay ransoms and do regain access to their data, they often forget that the attackers still have their data. Ransomware operators are becoming increasingly aggressive, and in 2021 we expect to see attackers use retained data in other ways as they digest the content. This could include returning with more demands or publicly embarrassing an organization.

In 2021, organizations need to be prepared for a ransomware attack. This means ensuring that networks are segmented, that an actual plan is in place and that tabletop exercises have been conducted with senior leaders and other key staff so everyone is ready to take an optimal action. Organizations should have an incident response service-level agreement (SLA) in place. They should also establish secured backups that teams can revert to when necessary. Organizations are going to be targeted and they are going to be compromised, so it is crucial to have prevention and recovery strategies in place.

Nation-state activity will continue to be **dominated by traditional espionage against** both **governments** and perceived threats to **regime stability**.

ESPIONAGE AS AN ONGOING DRIVER OF NATION-STATE ACTIVITY

Major nation-state threat actors continuing efforts in 2021 will include Russia, China, Iran and North Korea. These countries are significant sponsors of threat activity, both regionally and globally. Beyond that, we're seeing an uptick in activity from Vietnam and South Asia. Those nations are expected to increase operations next year.

We observed considerable espionage activity prior to the U.S. presidential election, and we will continue to see the targeting of U.S. political information in 2021 from actors such as APT28 from Russia and APT31 from China. Cyber threat actors would want to monitor and conduct reconnaissance and espionage on whomever is in charge after the election, so the U.S. government and presidential administration should expect to see a flurry of spear phishing emails from nation states that want to position themselves in target networks to perform espionage.

Spear phishing is one of the most popular infection vectors when it comes to nation-state threat activity, and it will continue to dominate in 2021. In addition, an increasing number of nation-state actors are focusing on intrusion techniques that don't require any victim interaction, such as exploiting web-facing applications and password spraying. We observed these tactics being used by a number of Iranian, Russian and Chinese groups in 2020, and we expect them to continue in 2021. Countries that are just getting into the business of cyber espionage will continue to turn to third-party intrusion vendors for tools and capability enhancement.

Based on developments observed in 2020, the Chinese cyber threat apparatus appears to present a more serious threat than previously assessed, with implications for 2021 and beyond. Despite strategic plans focused on international trade and remaining engaged with the international community, evidence suggests that norms and diplomatic agreements do not significantly limit China's use of its cyber threat capabilities—for example, in IP theft operations—particularly when serving high-priority missions.

Hong Kong's new national security law and human rights abuses in Xinjiang highlight China's willingness to leverage technology to solidify control domestically. The border dispute with India and military exercises in the South China Sea demonstrate China's desire to project regional hegemony, and the Belt and Road Initiative (BRI) extends China's ambitions for economic and political influence. As China continues its soft power projection across Europe, Africa and Asia through the BRI, we will continue to see cyber activity accompanying those efforts.

Expanding cloud usage will require organizations to **improve visibility into their cloud** footprint, assets and provider relationships **to manage risks**.

CLOUD SECURITY TAKING THE LIMELIGHT

Companies will need to spend time building up awareness of their cloud presence in 2021. About 95 percent of companies have some type of cloud presence, even if only for internal functions such as human resources or payroll. Organizations that don't think of or consider common solutions such as Microsoft Office 365 to be a cloud platform put themselves at greater risk.

Many companies deferred multi-factor authentication to legacy systems as they were accelerating their migration to cloud platforms in recent years. The urgency of business requirements often drives organizations to move technology adoption efforts forward faster without having the right security controls in place. As a result, many organizations will be playing catch-up on the security front as we move into 2021. Organizations need to secure the methods of access to data, and that means focusing on identity and access management and revisiting who qualifies for privileged access.

Many cloud threats are the same as those encountered on in-house networks. In 2021, cloud attacks are expected to continue to be executed through:

- Stolen credentials, typically via phishing
- Exploitation of cloud misconfigurations
- Vulnerable cloud application hacking

Prevention and detection strategies will be crucial for all organizations to guard against such threats.

Whether large or small, no organization is immune to cloud risk. Next year, we expect to see organizations newer to the cloud making plenty of rookie mistakes, and organizations increasing their attack surface to the point that getting compromised is inevitable. When it comes to a relatively newer technology such as cloud, there are ample opportunities for error, so organizations must focus on preparedness and asset management. Full and accurate tracking of cloud assets should be a priority in 2021.

Organizations also need to be more aware of their relationship with cloud providers. One of the things many organizations misunderstand is that they cannot hand off risk when outsourcing or moving to the cloud because while the cloud provider is responsible for securing the cloud, the customer is still responsible for determining who has access to the cloud, how they have access to the cloud, and the protection of their data in the cloud. The organization must determine what to protect and how to protect it, and ensure those protections are implemented correctly.

We are in a period of economic uncertainty, and **validation** will help **ensure** organizations are maximizing their **return on their cyber security investment**.

SECURITY VALIDATION TO KEEP DEFENSES AND BUDGETS IN CHECK

As the economy continues to be strained moving into 2021, cyber security spend will be increasingly scrutinized. We expect many organizations to invest in security validation to understand if their technology is deployed optimally, if threats are being detected and blocked, if security settings are configured correctly, and if they are getting a good return on investment.

Security validation provides quantifiable data to the business on the effectiveness of their cyber security controls. Since increased remote work will persist into 2021, validation will help organizations answer questions such as:

- Is my VPN working like it should?
- What vulnerabilities or gaps do I have in my remote infratructure?
- Do people who have higher level privileges still need them now that they're working from home rather than on premises where their access could more easily be monitored?

Prior to the pandemic, many organizations preferred to operate their validation platforms onsite and with their own teams. Now, with the shift to remote work, in-house security validation efforts are expected to transition to fully managed or co-managed security validation in 2021.

Security effectiveness as a business metric will grow in 2021. This is the measure of whether an organization's security is getting better or worse over time, and how to optimize tools and rationalize spend. CISOs will need better ways of obtaining this information for their CIOs and CFOs, and they will turn to security validation to justify how much money they are spending towards effective cyber security.

Security automation and training are also expected to be areas of significant growth in 2021. Companies will continue to automate routine tasks so they can free up expertise for more high-value activities. Security validation will help identify areas ripe for automation as well as those that should be prioritized for more expert attention. The increased risk from remote work, especially for those organizations without established processes and policies for data access, will warrant significant additional security awareness training. Again, security validation can help by identifying some of the focus areas for that training.

POSITIVE SECURITY RESULTS WITH EFFECTIVE PLANNING AND IMPLEMENTATION

Organizations had much to overcome in 2020 and a rapidly changing security environment was just one challenge. We know the chance of these challenges continuing into 2021 are high, and the adversity will be from more than just cyber threat actors.

Fortunately, many companies—particularly those that had never planned to fully support a remote workforce—have taken steps to enable their workers while ensuring that access to basic functions and sensitive corporate data is secure. But the job of cyber security is never done.

The global pandemic has brought on more than just remote work. On the preventative end, we've seen the targeting of research and manufacturing facilities tasked with development and distribution of a COVID-19 vaccine. On the response side, we are seeing the targeting of hospitals where people are receiving treatments from healthcare providers who are putting their lives on the line. Some of these attacks fall under the category of espionage, but others have simply been for financial gain, showing that some attackers truly have no regard for human life.

When it comes to financial gain, industries that were heavily targeted were able to make great strides towards securing their weak points. For example, cyber criminals have moved past targeting point-of-sale (POS) devices for credit card information because the defensive measures were able to raise the cost of an attack beyond what was profitable for bad actors.

Today, it's all about ransomware. This once opportunistic threat that used to cost organizations thousands of dollars is now being deployed in sophisticated operations with ransom demands upwards of a million dollars. Ransomware is only going to get worse in 2021, and organizations are going to need to be prepared with incident response plans and data backups. We can look to our past success with securing POS systems and know these are solvable problems.

With another U.S. presidential election in the books, the U.S. government should expect to see an uptick in spear phishing and other attacks from nation states that want to conduct espionage to gain a decision advantage. Russia, China, North Korea and Iran are significant sponsors of this activity, but we also expect to see an uptick in activity from Vietnam and South Asia.

Over the past few years we have seen organizations make massive migrations to the cloud at breakneck speed, and many haven't been vigilant about security along the way. These organizations must catch up on cloud security in 2021, and one way to help identify gaps and overlaps is through security validation. We expect to see more people turning to validation—particularly managed validation—to not only understand if their security is optimized, but also to help reduce their spend.

This past year was one of the most challenging in recent history and forced many organizations to stop what they were doing and reprioritize. FireEye and Mandiant Solutions continue to make great strides and help lead the charge wherever and whenever possible.

To learn more about FireEye, visit: **www.FireEye.com**
To learn more about Mandiant Solutions, visit: **www.FireEye.com/mandiant**

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

About FireEye
At FireEye, our mission is to relentlessly protect organizations with innovative technology, intelligence and expertise gained on the frontlines of cyber attacks. Learn how at www.FireEye.com.

About Mandiant Solutions
Mandiant Solutions brings together the world's leading threat intelligence and frontline expertise with continuous security validation to arm organizations with the tools needed to increase security effectiveness and reduce business risk.