VERSPRITE

ENVISIONS

CRITICAL THREAT REPORT

2021

VerSprite is an industry leader in risk-based security services and automation, and has pioneered the PASTA threat modeling methodoloy. VerSprite offers a strategic partnership to companies looking to evolve their security posture beyond compliance standards.

THE WORLD CHANGED IN 2020, THE THREATS DID NOT

In 2020, businesses witnessed the largest pandemic the world has seen in over 100 years. COVID-19 not only affected our personal lives, but it has ultimately changed the way we do business. With thousands of workers moving remote, organizations had to quickly implement new policies to secure thousands of endpoints outside the safety of a corporate-secured network, which led to new security gaps that left companies exposed.

As the pandemic took the spotlight in 2020, cybercrime trends from previous years increased in frequency and severity. Organizations continue to be breached by common threat vectors, including social engineering and unsecured networks. Thousands of businesses were forced to close their doors, leaving displaced individuals more desperate and motivated by financial gain. International tensions grew more strained as we witnessed one of the most successful nation-state attacks penetrate the US government and major corporations.

For our 2021 Envisions Threat Report, VerSprite's Geopolitical Risk and Threat Intelligence teams collaborated to create a list of six major cybersecurity predictions that will dominate the threat landscape for private and public sectors. Envisions 2021 will discuss the rise of insider threats, BYOD policies, the new era of the Internet of Things (IoT), blockchain technology in the financial industry, the risk associated with critical infrastructure, and rising international tensions. This year we included additional resources, including a list of the top industries that should include each threat in their security planning this year and a look back at how our 2020 predictions unfolded.

VERSPRITE

ENVISIONS

TABLE OF CONTENTS

HIT or MISS?

LOOKING BACK AT OUR 2020 THREAT PREDICTIONS

In last year's Envisions Threat Report, we made a series of 10 security predictions about what geo-political threats will proliferate in 2020. Like other cybersecurity organizations, nobody could have predicted the chaos caused by the pandemic. Companies were forced to move operations to work-from-home models overnight, leaving many IT leaders struggling to build up their data protection for employees that are now working outside the organization's corporate edge firewall. As security risks rapidly increased from a centralized to de-centralized network, some organizations successfully adopted and leveraged VPNs and multifactor authentication protocols, while others tried to get by with existing security configurations. In retrospect, we can all conclude that average defenses for evolving global threats, often ushered by various geo-political themes stand little chance of effectively reducing risk levels for organizations.

Although COVID-19 unveiled new risks and geo-political concerns at multiple levels, it clearly exposed DR and BCP plans everywhere and put the issue of business resiliency to the top of the excutive boardroom discussions. Before we examine our 2021 threat predictions, let us review how we scored on 2020 predictions.

Looking Back At Our 2020 Threat Predictions

B+

CORPORATE SOCIAL RESPONSIBILITY

Last year, we pressed upon the importance of developing contingency plans for operational disruptions attributed to climate change and environmental threats. At the time, we could not have predicted the severity of those warnings however, the devistating wildfires that spread throughout California, the Pantanal wetlands in Brazil and Australia, along witha great number of tropical phenomenons globally highlighted the importance of our first prediction around CSR. Despite our correct analysis in 2020 on the unprecedented rise of environmental threats, there hasn't been much in the way of CSR from global companies.

The year did introduce various conversations on the need for standards – from the World Economic Forum, followed by the Davos Manifesto. While we will not be delving into deeper predictions on this threat in 2021's report, organizations should continue focusing on social responsibility efforts to stay relevant in the fight againist climate change and protect their business operations in the rapidly escalating environmental threats that impact business continuity, particulary those that are MNCs .

C-

DEEPFAKES

In 2020, we disucssed the possibility of Deepfakes and online misinformation being used to amplify voter misconceptions, fears, suspicions, and undermining the creditability of political candidates among voters. The 2020 presidental election was polluted with large amounts of misinformation that caused people from around the world to question the integrity of the United States election process. We also saw an increase of deepfake technology used to advance social engineering techniques against corporations and government officials worldwide. To pair with the increase spread of misinformation, AI technology saw a large increase in 2020. This contributed heavily to the advancement of deepfakes.

A-

PANDEMIC

The 2020 COVID-19 pandemic flipped the entire world upside down by completely changing the way we perform day-to-day activites and business operations.

Beyond the chaos introduced by this devasting pandemic, cybercriminal

Looking Back At Our 2020 Threat Predictions

activitiy rose substantially in 2020, leveraging pandemic related news, alerts, philantropic causes as veiled attempts to trojan into a shifted attack surface – the distributed work-from-home network. Various illnesses beyond COVID-19 surfaced this year, but not to the pandemic status that has crippled the global economy.

The pandemic prognosis was accurate from our team and pandemics will unfortunately be leveraged by cybercriminmals to Trojan in veiled business or personal attempts to gain a target's attention. In our 2021 threat report, we are going to take a look at the implications of the new remote workplace and the Bring Your Own Device trend (BYOD) during this prolonged lockdown.

A+

HACKTIVISM

2020 saw an increase of social unrest across the globe, adding credence to our prognosis that hacktivism will have a rising effect on multiple fronts: politics, business, and societal affairs in general.

Activists are using new and innovative tactics that combine both digital and physical techniques to target governmnent agencies, officials, and corporations to make a statement. In Envisions 2021, we continue to explore the new tools that will allow for the growth of hacktivism and social unrest.

C+

5G WIRELESS TECHNOLOGY

The implementation of the 5G infrastucture took a big step forward during 2020. The full adoption of 5G networks have already started rolling out but process has slowed due to the significant costs to upgrade infrastructures and lockdown restrictions. Even with slowdowns, we saw new IoT devices in the work enviroment that are operating in 5G networks.

B+

DECOUPLING BETWEEN SHENZHEN AND SILICON VALLEY

2020 brought forth several offensive campaigns by Chinese hackers against foreign governments and corporate entities. From Malaysian government targets (related to government backed projects) in early January of 2020 to Chinese hackers attacking 75 companies in various industries (healthcare, manufacturing, media, and non-profit) in March, to

Looking Back At Our 2020 Threat Predictions

CISA revealing that Chinese hackers from their Ministry of State Security had been scanning U.S government and private networks for over a year in order to identify targets with vulnerabilities that could be attacked using current exploits.

The recent elaborated hacks targeting cybersecurity firms and government agencies only adds up to the tension the trade wars had introduced.

A+

MARITIME INDUSTRIES CYBER ATTACKS AGAINST

By mid-February, we saw a 400% increase in attempted cyberattacks against the maritime industry.

Although this threat continues to exist, the major attacks and infrastructure for state-sponsored hacking groups were targeting major US Government contractors in 2020. Cyber attacks against maritime industries will continue to exist, and increase as ships become more sophisticated and computerized.

C-

RUSSIA TARGETS COUNTRIES AFFILIATED WITH NATO

2020 proved just how concerned organizations and governments should be about Russia. Our 2020 prediction proved omonous and acquired more relevance as the world learned about Russia's alleged attack on SolarWinds' Orion, which resulted one of the most significant supply chain attacks to date. Major cybersecurity firms, corporations, and US government agencies were affected by this attack.

While the long-term effects of this attack have yet to be seen, we urge organizations to use this time to develop zero-trust policies for their vendors and do extensive vendor risk assessments. We will be covering this topic again in our 2021 report.

A+

RANSOMWARE

Last year, we saw large amounts of ransomware attacks specfically targeting the electronics and IT industries, healthcare, and education industries . This attack method has become a staple tool for small and medium cyber crime operations and will continue to be so in the future as

Looking Back At Our 2020 Threat Predictions

we watch its evolution.

EUROPEAN DISSONANCE FROM THE UNITED STATES

We initially predicted increased European dissonance from the US in our 2020 Envisions Report.

This proved accurate with the dissolution of the Privacy Shield Act, which was a privacy regulation recognized by the European Union and allowed US companies to operate in the EU. After this was revoked, we saw many companies searching for new ways to maintain operations in Europe, while struggling to implement controls that could comply with GDPR.

Insider threats make up 60% of cyber attacks and nearly a third of data breaches.

Threats from Within An Organization Itself Will Increase Security Blindspots

Why Insider & Involuntary Threats Need to Be on Your Radar in 2021

Many Cybersecurity programs are designed to protect an organization from outside threats, but 2020 proved that only focusing on outside risks leaves a large blind spot to threats that come from within the organization itself. Over the last year, we have seen an increase in incidents caused by individuals inside the organization, some voluntary and some not. Involuntary and insider threats have caused some of the largest losses in data breach history and we expect this trend will increase in 2021.

Why Insider Threats Are Overlooked

According to the US Homeland Security, "An insider threat is defined as the threat that an employee or a contractor will use his or her authorized access, wittingly or unwittingly, to do harm to the security of their organization." These can be the results of a malicious attack against a particular entity, or can be considered involuntary, meaning an employee accidentally violated policies that put the organization at risk.

There are major security gaps in how organizations defend against insider threats. This is often due to the unclear baseline for normal employee behavior and poor user access management control. This makes organizations a prime target for social engineering attacks and brute force attacks like phishing.

Types of Insider Threats

INVOLUNTARY NON-RESPONDERS

Involuntary non-responders is a type of insider threat that includes employees that choose to ignore and/or not participate in security awareness training. This group is likely to be successfully phished, or fall victim to a social engineering ploy, putting the organization at risk of a malicious malware, or ransomware attack.

In May 2020, Experian fell victim to a social engineering attack, leading to the release of private data for over 24 million South African consumers and over 800,000 businesses including ID numbers, telephone numbers, and physical email addresses. The attacker purported as a legitimate client representation to request services from the Experian employee.

INSIDER COLLABORATION

An insider collaboration stems from an outsider recruiting an organization's employee to work with them as they plan an attack against the organization. Cybercriminals will recruit employees via the dark web and other creative tactics.

In the summer of 2020, a Russian man named Egor Kriuchkov invited a Tesla employee to collaborate with a group that carries out insider threat attacks. The Tesla employee was offered $500,000 to install a malware in Tesla's network that would put the group in control of sensitive data, leading to a high paying ransom. Thankfully, the Tesla employee immediately informed the FBI, leading to Egor Kriuchkov's arrest.

UNSATISFIED FORMER OR CURRENT EMPLOYEE

A disgruntled employee could deliberately sabotage security tools inside the organization. For example, in September 2018, an ex-employee of Cisco accessed their AWS cloud infrastructure and was able to delete 456 virtual machines that support Cisco's WebEx Teams software, leading to the loss of over 16,000 WebEx accounts. The employee was recently sentenced to two years in prison.

VerSprite Cybersecurity
Experian Leaked 24 Million Customers' Data
THAT COULD HAVE BEEN PREVENTED WITH THIS TYPE OF TRAINING
Celebrate
Comment
Share
Send
VerSprite Cybersecurity
Click To Learn More About Defending Against Insider Threats

Social Media Will Be An Important Battleground for Insider Threats in 2021

Sophisticated social engineering attacks will spotlight 2021 on social media sites as attackers target authoritative figures inside organizations. Cybercriminals are improving their attack plans using deepfakes to lure users into clicking links and sharing these links to their contacts, making it more difficult to detect social engineering attacks for regular users.

We can expect to see these types of attacks and more targeted attacks that will compromise social media accounts from key individuals at government entities and corporations to either try to impersonate them better or directly coerce them into becoming insiders. We have seen these attacks in 2020, though not as sophisticated, and will see an increase in 2021 due to the ease of use of many of the tools used to carry on these attacks.

Compromising employees' personal devices and social media accounts to blackmail them into becoming insiders will start to be more widespread. As social media becomes even more pervasive and an individual user may have at least one account in each of the sites and applications, we will see more abuse cases that leverages social media and synthetic media on top of traditional attacks to profit from exploiting users.

230,000 new malware samples are produced every day – and this is predicted to only keep growing.

The Way To Defend Against Insider Threats is To Be Proactive

VerSprite's **Enterprise Risk Assessments** can aid your organization in understanding if the current controls your organization has implemented would impede and/or detect if a threat exists around your data or if permissions give individuals within your company access to sensitive data they are not supposed to access. VerSprite's unique **organizational threat models** can look outside your organization to identify groups and risks to your organization and its employees.

TOP INDUSTRIES TO WATCH IN 2021 FOR INSIDE THREATS

A study published by Bitglass reported 61% of respondents encountered an insider attack over the last 12 months. Similarly, Verizon published an insider threat report where they listed 5 industries with the highest percentages of insider threats. Among those industries listed was **Manufacturing**. Annually, manufacturing companies report $8.86 million in losses for a single organization. Considering this and the plague of vulnerabilities coming from manufacturing organizations in 2020, this industry is most likely to see the greatest impact by insider threats.

The bring your own device BYOD market is growing fast. As of 2019 the market was valued at $186.09 billion USD and is **predicted to reach $430.45 billion USD by the end of 2025**, according to Mordor Intelligence.

THE NEW REMOTE WORKPLACE BRINGS HIGHTENED CONCERNS FOR ENDPOINT SECURITY

When COVID-19 spread throughout the globe, organizations were forced to send employees home rapidly, leaving little to no time to secure the thousands of new networks and threat landscapes properly. Employees were forced to connect to their company's network from their own devices, potentially leaving sensitive data at risk. Before the pandemic, 17% of U.S employees worked from home 5 days or more per week, a number that increased to 44% during the Coronavirus pandemic. According to Statista, this number will keep increasing as companies realize many roles can be done from home. The Bring Your Own Device (BYOD) model gives employees the task of responsibly selecting, maintaining, supporting, and securing their personal devices. Although the BYOD model presents several benefits for organizations, endpoint security and BYOD policies must become a priority in 2021 as the pandemic continues to challenge the status quo of the workplace.

Most companies are not properly protecting their networks from open endpoint and BYOD security threats. In a recent survey by McAfee, researchers found that over 60% of organizations allow their employees to use their personal devices to access company networks. Still, less than 45% of these companies don't have an employee-owned device policy in their security programs. Bitglass reported that 72% of employee devices did not have any malware prevention software. With the massive rise in ransomware attacks in 2020, the chance for enterprise data to be lost has never been higher.

To avoid business disruptions, brand damage, and unauthorized access and/or data theft, companies must develop a strategy that encompasses policy, auditing functions, and progressive endpoint protection that are as robust as those provisions in Corporate Offices and Cloud Environments. As attackers learn of more companies switching to work from home (WFH) models, they will do more spear-phishing and other targeted attacks on top of random and easier to identify social engineering attacks, aided with technology such as Synthetic Media. If we sum the Unmanned Air and Ground Vehicles that are now super affordable, we will see more hacks and breaches happening at employees' homes.

ENDPOINT & BYOD RISK ASSESSMENTS

VerSprite can assist in addressing the risk associated with Endpoint and BYOD security with the help of a **vCISO**, the creation of policies and procedures to classify data, **risk assessments**, and by providing **the right controls** to secure sensitive corporate data. Developing BYOD security policies, procedures, and classifications tailored to your organization's business model and strategy is a critical step towards increasing your organization's security while employees are working from home. By performing an **Enterprise Risk Assessment**, VerSprite can help you understand what scenarios are more likely to happen within your company. For example, targeting specific personnel, technology, or information. By utilizing a third-party vCISO, you will have a custom managed CISO program that will define, manage, and optimize your security programs. VerSprite's security experts will be your trusted security partner to remediate endpoint and BYOD security with actionable plans for you to implement inside your organization.

TOP INDUSTRIES TO WATCH FOR BYOD THREATS IN 2021

Several industries have moved to a work-from-home atmosphere because of the pandemic. Of those industries, it should come as no surprise that the **healthcare industry** is of the most concern. Many positions in the healthcare industry have moved to remote positions to combat the curve of the pandemic. These positions deal with sensitive data from hospital revenue to patient sensitive data. Organizations are unable to control the working conditions, making for an environment of vulnerabilities. While the financial industry has seen an increase in WFH activities and makes for a good competitor for this top position, the type of data that the healthcare industry can expose is of greater concern.

THREE TOP SECURITY RISKS WITH OPEN ENDPOINTS AND BYOD MODELS

MALWARE

BYOD increases the size of an organization's threat landscape. Employees download several apps, documents, and more that could have a hidden virus or malware strand.

DEVICE THEFT OR LOSS

If an employee was not properly following their BYOD security measures and loses their electronic device, they could put their organization at high risk. Once a stolen device is in the hands of a cybercriminal, they can easily crack their password, giving them direct access to the network.

LACK OF SECURITY AWARENESS TRAINING

Regardless of the technology strides the industry makes to protect organizations from cybercriminals, the human element is the weakest access point. Inadequate security training can lead to employees not truly understand their company's requirements while securing their devices, leading to potential errors that could compromise their organization's security system.

IoT Devices in the Workplace Threaten Organizational Security

As Internet of Things (IoT) devices become more diverse, access policies that are tailored towards the function and roles of individual IoT devices will become crucial for organizations. The current lack of security controls for IoT devices and the little to no manufacturers, makes IoT devices a hot target for abuse cases and attacks in 2021.

The New Era of Workplaces

As trends continue to move operations to remove work in 2021, there will be an increase in demand for IoT devices including, smart offices, remote medical devices, and remote monitoring options. These devices generate new Wi-Fi and Bluetooth access points that can be easily exploited by cybercriminals.

Vulnerabilities found in IoT devices can be challenging to patch, allowing for more sophisticated and targeted attacks that use war flying, ransomware, Bluetooth, and other wireless technology. Attackers focus on obtaining the physical location of an individual through OSINT, leveraging social media to prepare and perpetuate a series of wireless attacks in vehicles, homes, or offices, through the use of Unmanned Air Vehicles (UAV) and Unmanned Ground Vehicles (UGV) training.

With the increased demand for IoT devices, manufacturers are working to build quicker and more improved versions, ultimately pushing the security safety elements to the side. Despite the major updates and enhancements to IoT devices, security risks are still in tack due to the lack of updates, malware and ransomware, and the use of default credentials.

According to ThreatPost, **more than half of IoT devices are vulnerable** to severe attacks, and 98% of all IoT device traffic is unencrypted, with the potential to expose personal and confidential data. In a recent study, researchers found a 15% – 16% increase in IoT breaches since 2017. Gartner forecasts that more than half a billion wearable devices will be sold worldwide in 2021, up from roughly 310 million in 2017. Wearables include smartwatches, head-mounted displays, body-worn cameras, Bluetooth headsets, and fitness monitors.

IoT Inside Cars

With the increase in smart connected devices, cybercriminals will find new, creative ways to infiltrate your devices, and most likely your car. ABI has forecasted that more than 20 million connected cars will ship with built-in software-based security technology by 2020 — and Spanish telecom provider Telefonica stated that by 2020, 90% of cars will be online, compared with just 2% in 2012. The cars that we drive will become more connected than ever, increasing the relationship between car technology and functionality. As cars become more software based, they put passenger's safety at risk.

2021 IoT Defenses

Organizations need a security strategy that commences with a threat library relevant to the organization, its technological footprint, and the current landscape that blurs the line between physical and virtual. VerSprite conducts **Enterprise Risk Assessments** to assess current controls' effectiveness and provides threat maps that will allow organizations to detect and understand any gaps in such controls and the overall security strategy.

TOP INDUSTRIES TO WATCH FOR IoT THREATS IN 2021

All industries will be impacted by IOAT, however the industry that is most likely to see the most harm done by this form of attack is the healthcare industry. With the 300% increase seen in data breaches in healthcare, as well as the fact that according to Black Book Market Research's study, 75% of healthcare organizations reported they are not prepared to handle an attack. Bring-your-own-device is common in the healthcare industry where proper policies and securities are not in place to respond to an attack.

Altcoins + Blockchain: The New Fintech Power Couple

For many years' altcoins based on blockchain technology have been used for speculation purposes and, in many cases, as a major scam. However, major banks and even countries have been investing in research and infrastructure to allow this technology to be used legitimately, making blockchain technology one of the hottest software of the 2020s. Blockchain technology will allow people to send money globally within seconds and at an affordable price.

With this advancement, we expect the financial industry will be adopting blockchain technology faster in the coming year. The benefits of using blockchain technology in fintech include reduced operational cost, eliminating third parties, and revamping the identify verification process. Some of the largest consumer finance companies and stock exchanges including New York Stock Exchange, Australian Stock Exchange, Mastercard, VISA, and American Express are adopting and investing in blockchain technology. For banks and financial institutions, the intention to adopt blockchain technology will be to facilitate payments primarily through the distributed network using certain cryptocurrencies, depending on the country, as part of a global plan to lead the digital transformation of DeFi (decentralized finance) in the world's economy.

Cryptocurrency's Underlining Cybersecurity Timebomb

With the growing popularity of cryptocurrency, the increased risk of cyberattacks includes extortion attempts, ransomware, and distributed denial of service (DDoS) attacks. These attacks happen on the trading platforms and websites of service providers intending to shut down the system completely. Blockchain technology in altcoins is used to decentralize control between a group or person and give all parties collective control. Due to the decentralize control of altcoin's blockchain, transactions are completely transparent allowing anyone access to live transactions. To successfully implement and adopt new technology inside your fintech organization, it is crucial to assess and manage the risk associated with the technology properly. A proper implementation process will be key because the majority of the vulnerabilities have been found in the implementation and vetting process of blockchain technologies, rather than in the technology itself, similar to what happens when implementing cryptography. Since many cryptocurrencies and blockchain technologies are still in their early development stages, unknown vulnerabilities can compromise crypto wallets and increase the chances of fraudulent Initial Coin Offerings (ICOS).

Although IT may vary from industry to industry, we will see more DaPPS (Decentralized Apps) going mainstream and be part of the digital landscape. Just like any new technology, understanding this technology might be the competitive edge for your organization. Blockchain technology has proven the right medium to build these apps and integrate somewhat easily with technology for user validation like digital signature amongst others.

According to BPM, the total value of cryptocurrencies committed to bets using Etherium smart contracts, as measured by DeFi Pulse, surpassed $1 billion in February 2020. The figure has since surpassed $10 billion. This number does not represent the amount people are making from their DeFi bets, but rather how much they have committed to those bets.

Security Solutions for Blockchain Technology & Cryptocurrency

Although blockchain technology is advertised as reliable and well protected, hackers continue to exploit vulnerabilities including low-security hot wallets, insider threats, poor input validation and the lack of multi-signature. VerSprite takes pride into having professionals that understand this technology and perform assessments to DAPPs.

Our clients push innovation in the cryptocurrency space and rely on us to help them secure this new frontier too.

If you are a startup that wants to validate its security controls or if you are a financial organization looking into this market, our GRC consultants can perform a **Vendor Risk Assessment** that is completely custom to your industry's specific needs and the technology behind it.

TOP INDUSTRIES TO WATCH FOR BLOCKCHAIN THREATS IN 2021

The **financial industry** has been moving towards cryptocurrency payments and some have even created their own blockchain-based systems. Therefore, this industry is most likely to be impacted by the rise in cryptocurrency use and blockchain environments. Italy's banking sector is using Spunta (blockchain network) to reconcile balances between banks, according to the founder of Spunta. He is hoping for growth across Europe followed by globally. ConsenSys, a blockchain software company, is working on central banking for digital currencies in Hong Kong, Australia, France, and Thailand.

Risks To Critical Infrastructure Can Cause a Domino Effect of Disruptions

Critical infrastructure and systems have been desirable targets for decades, but we have recently seen a diversification in how attackers are targeting government, healthcare, and other critical infrastructures.

Government Agencies at Risk of Cyberattacks in 2021

In September 2020, cybercriminals targeted the State of Washington and launched a multi-layered malware attack. The attackers were able to infiltrate multiple state agencies and spread sophisticated malware allowing them deeper access. Attackers deployed two dangerous malware strands, the Emotet banking Trojan and Trickbot. These specific strands are commonly used by the Russian cybergang, Ryuk, and target financial and banking institutions. This attack put several critical infrastructures at risk, including government facilities, communication, financial, and information technology.

Despite federal protection from the Health Insurance Portability and Accountability Act of 1996 (HIPAA), one in four Americans has fallen victim to a healthcare data breach. Healthcare breaches are among the most violating attacks due to the exposure of sensitive information, including an individual’s health history.

On January 2nd, 2020, Health Share of Oregon, the state's largest Medicaid coordinated care organization (CCO), said thier contracted non-emergent medical transportation (Ride to Care) vendor GridWorks suffered a break-in, resulting in stolen data from over 654,362 Medicaid members.

If cybercriminals can successfully infiltrate a hospital’s infrastructure, they will force healthcare workers to move offline with no access to patient records and various other systems being used. With healthcare-related cyberattacks increasing by 150% since COVID-19 hit the United States, we predict the security gaps that were exposed by the pandemic will allow for an exponential increase in healthcare related cyberattacks during 2021. The large amount of hospitals that have already been compromised in 2020, the growth of medical resources including Telehealth and IoT medical devices, and the health sector being at higher compacity than usual make healthcare and public health infrastructure a vulnerable target for cyberattacks.

Fusion Between IT and OT Creates Vulnerabilities

Cybercriminals’ increased interest to gain economic or political power paired with the development of new command systems and network devices, makes today’s industrial control systems more vulnerable than ever. Operational Technology is now controlling day-to-day operations inside organizations responsible for the utilities, healthcare delivery, and provision of essential government services.

> **Operational technology (OT) is** hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events.
>
> **- Gartner**

OT can be used to control public transportation, power supply stations, dam openings, pipeline operations, supply-chain operations, and other critical infrastructure processes.

Industrial OT

Before OT, industrial systems were manually monitored and managed by humans with little to no connection to outside networks, making them an undesirable target for cybercriminals. In today’s world, industrial systems have to move online to deliver analytics and data and increase their efficiency levels. The fusion between IT and OT has given organizations a panoramic view to deliver accurate information to their clients. Although OT has increased efficiency levels for many organizations, new security risks need to be discussed.

Since the 2015 cyberattack that infiltrated Ukraine's entire power grid, cybercriminals have continued to exploit network-connected operation technologies to gain access inside critical infrastructures. If attackers can gain admin control to OT controls, they can corrupt the OT and IT systems, disrupt operations, wipe out servers, and ultimately put people's welfare at risk.

OT and Supply Chains

CISA interviewed 450 executives across multiple industries including, aerospace and defense, financial services, manufacturing and production, technology, energy and utilities, and other commercial sectors and asked them what they believe the biggest risk to their supply chains are. 76% identified COVID-19 as the biggest ongoing risk, followed by cyber threats at 44%. When asked the same questions about future risk, 66% identifying COVID-19 as the future risk companies are preparing for, followed by cyber risks at 48%. Operational and Information Technology (IT/OT) offers organizations low-cost and innovative features to increase their supply chain effectiveness. With the benefits comes the risk of a potential compromise of their supply-chain that could result in a risk to the end-user.

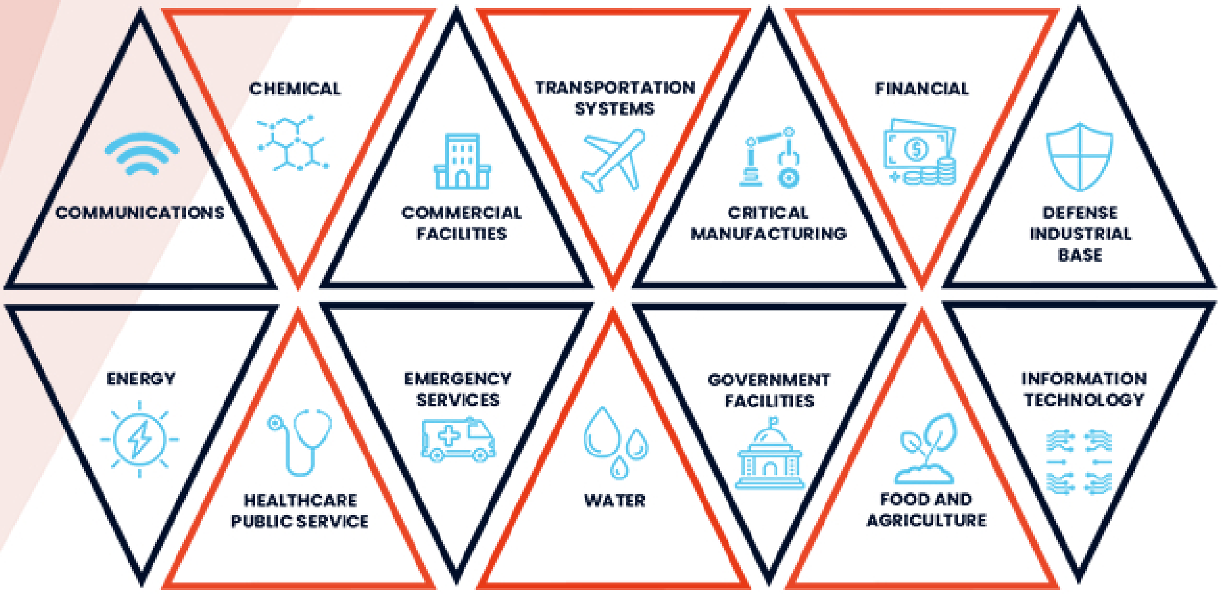
In early December 2020, IBM security researchers discovered a worldwide phishing campaign specifically targeting companies involved with the overseas supply chain for COVID-19 vaccine distribution. The COVID-19 vaccine distribution could last for several months, putting supply-chain operations at risk for several organization's involved with the safe delivery of vaccines.

Protect Disruptions To Your Operation By Looking To Supply Chains and Organizational Threats

As infrastructure risks continue to rise, organizations must take a proactive approach to security and risk analysis. VerSprite can assist you in detecting and prioritizing threats to your organization through several services, including

Enterprise Risk Assessments that allow you to prioritize remediation and focus your efforts and budget to respond to the most critical vulnerabilieis first. For organizations with physical supply chains, we recommend getting an **organizational threat model** and **vendor supply chain vignette** to properly assess and prepare for risks that may cause operational disruption.

TOP INDUSTRIES TO WATCH FOR CRITICAL INFRASTRUCTURE THREATS IN 2021



Organizations & Government Agencies Will See An Increase of Nation-State Backed Cyberattacks

As geopolitical issues and tension continue to develop, we can expect to see an increase in disruptive attacks backed by nation-states. In 2020, we saw several attacks against the US government, like the recent SolarWinds supply chain attack and the multiple attempts by Iranian state groups targeting United States election websites to gather voter data and conduct voter intimidation campaigns. Nation-State sponsored attacks have one motive: to position their nation in a competitive position against their economic and political enemies.

2021 will see more nation-state attacks targeting government agencies and officials as cybercriminals try to collect data on the United States' new administration. Organizations and government agencies should expect to see an increase in spear-phishing campaigns and supply chain attack attempts and take proactive security measures to defend sensitive data and networks. With the change in the presidential administration in late January, expect to see new policies and sanctions drafted against North Korea, Russia, or China. The creation of these new policies alone will lead to an uptick in targeted attacks backed by nation-states. President-elect Joe Biden has already announced he will work with allies to create international rules that will hold nation-states accountable for cyberattacks. These statements will also trigger a higher frequency of attack attempts on the US government.

Private and Public Sectors Should Prepare for Increased Cyberattacks

Other industries that will be targeted in 2021 are healthcare, information technology, and media channels. The COVID-19 vaccine has begun its early distribution process. The US, United Kingdom, and Canada have all reported Russian and Chinese state actors trying to infiltrate and manipulate the vaccine's development. In September 2020, we saw the first cybersecurity attack that led to death. A Russian group successfully carried out a ransomware attack on a German hospital, causing the clinic's network to crash, forcing them to move critical patients to other locations, ultimately leading to one of their patients' death. The same group was also able to infiltrate and take down 250 UHS healthcare facilities.

The recent SolarWinds supply chain attack involved several organizations, including FireEye. We expect to see more attacks on information security companies because they house and protect several healthcare and government clients. Social channels and the media have always been a hot target for cybercriminals. Social channels like Facebook will continue to see nation-state sponsored misinformation campaigns as our world continues to rely on reliable, trustworthy news.

Zero-Trust Policies & Active Threat Monitoring Is The Best Gameplan Against Nation-State Threats

Organizations must adopt a zero-trust policy, incorporate stricter accont access privileges, and require all employees to use multi-factor authentication. Vulnerability and patching checks should be implemented into DevOps processes as new applications are developed. With spear phishing being the number one vector for nation-state attacks, companies will want to invest more in their security awareness training efforts.

Versprite can help private organizations and government agencies create proactive security policies and attack vector analysis that hardens them from malicious attackers. Our consultants can help by offering **Threat Vulnerability Management** services, expanding your security teams' viewpoint with additional **Virtual SOC**, 24/7 monitoring services; and providing your team the blueprint to guide your security efforts by performing an **organizational threat model** that maps out your attack surfaces based on your business objectives. Our **Virtual CISO** services can also assist your team to write security-focused policies unique to your operation.

TOP INDUSTRIES TO WATCH FOR NATION-STATE CYBERATTACKS IN 2021

Several industries have moved to a work-from-home atmosphere because of the pandemic. Of those industries, it should come as no surprise that the **healthcare industry** is of the most concern. Many positions in the healthcare industry have moved to remote positions to combat the curve of the pandemic. These positions deal with sensitive data from hospital revenue to patient sensitive data. Organizations are unable to control the working conditions, making for an environment of vulnerabilities. While the **financial industry** has seen an increase in WFH activities and makes for a good competitor for this top position, the type of data the healthcare industry can expose is of greater concern.

CHALLENGING THE INDUSTRY STANDARD

VERSPRITE

CYBERSECURITY

2021 will see cybercriminal activity adapting as technology advances and as each successful attack is studied by those with malicious intent. Organizations can use the intel we provided in this report as a security blueprint to help challenge your defenses before attackers do. However, each organization has unique attack surfaces that change yearly, and we recommend you do a thorough organizational threat model annually to get the best understanding of your threat landscape.

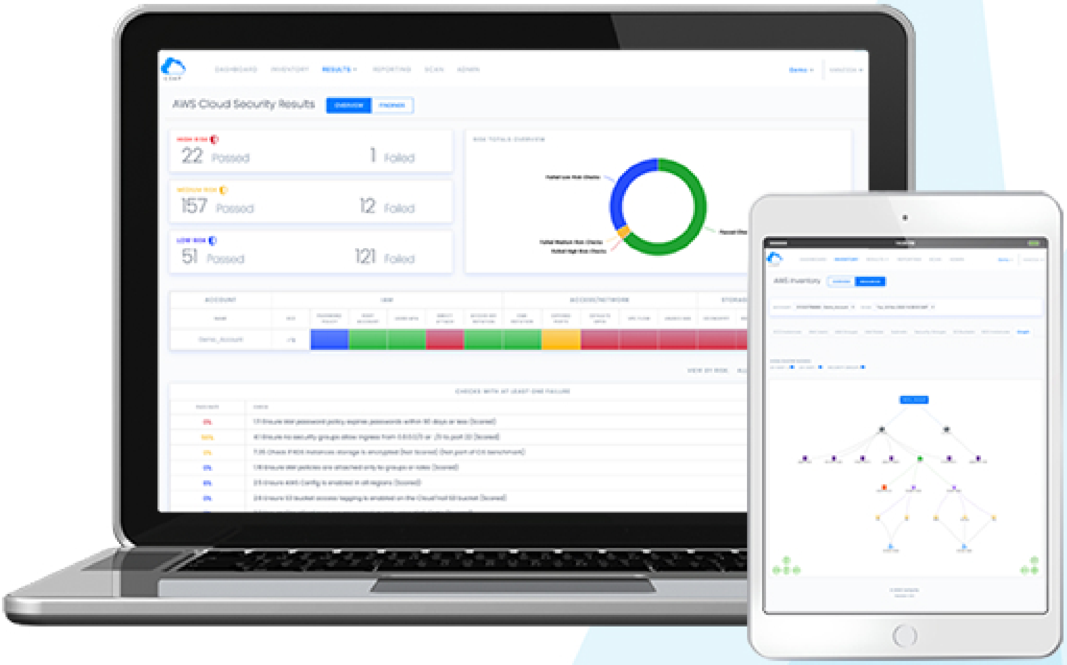
In 2020, VerSprite was named an **Inc. 5000 fastest growing company** for being an industry leader in PASTA-driven organizational threat modeling and evolved cybersecurity solutions.

Founded in 2007, we are a private cybersecurity consulting firm that **partners with organizations' security teams to expand the visibility** into their networks, identify security gaps and best remediation steps, and give them advanced threat intel tools.

VerSprite has a **97% client retention rate**. We can work with your team to perform penetration tests, evolved red teaming engagements, vCISO services, vSOC 24/7 monitoring services, and VerSprite's advanced security tools - Cloud Security Assessment Platform and Cyber Threat Intelligence Portal. We currently partner with over 200 companies worldwide and look forward to helping your team combat the threats we outlined in this report.

VERSPRITE
CSAP

CLOUD VISIBILITY + SECURITY



AWS + AZURE + GCP

VerSprite's Cloud Security Assessment Platform expands your team's visibility into resources across all your cloud accounts and regions. Integrate your current security tools into CSAP to monitor from one dashboard. Scan your environment, create reports, and get remediation tips based on the latest updates from VerSprite's Threat Intel group.

BOOK YOUR LIVE DEMO

VERSPRITE

ENVISIONS

CRITICAL THREAT REPORT

2021