Infosys®
Navigate your next

2021 CYBERSECURITY TRENDS REPORT

Infosys® | Knowledge Institute

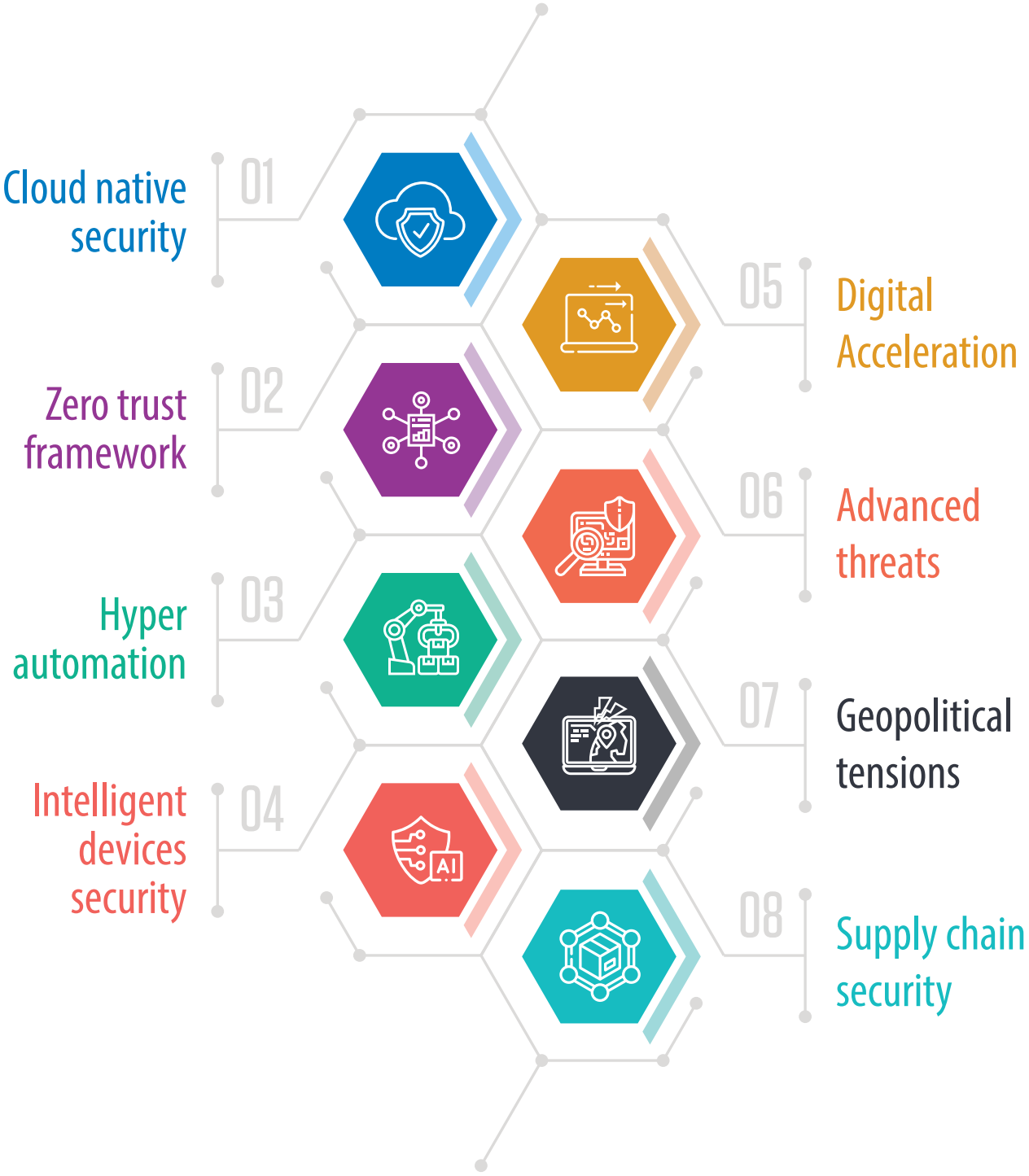
Contents

Foreword

The unprecedented events of 2020 disrupted businesses, damaged the global economy, and shook the cybersecurity industry. Companies across all sectors have experienced a spike in cyberattacks as COVID-19 reshaped the workplace. Throughout the year, hackers deployed various techniques to steal information and personal data from remote workers, hit hospitals with ransomware, and targeted the developers of COVID-19 vaccines. As organizations secured their remote workforces, most needed to rethink their existing policies, system controls, and risk management functions. The rapid shift to remote working increased most organizations' attack surface, exposing them to more vulnerabilities. This period also accelerated many trends, such as digitalization and migration to the cloud.

Looking ahead at the next 12 months, the world will still be in a transition period, trying to adapt to a changed economy. Organizations will be reevaluating their cybersecurity strategies and adopting more flexible operating models. The new cybersecurity environment will be shaped by the technology evolution. To help companies navigate this uncertain future, we defined eight key cybersecurity trends to watch in 2021.

Trends To Watch In 2021



Cloud native security

COVID-19 accelerated cloud adoption, as millions of employees were forced to abandon their offices overnight and work from home. Remote working relies on cloud computing applications that help employees efficiently accomplish their tasks from anywhere.

The cloud allows businesses and governments to adjust workloads as needed, and makes it easier to add new features such as analytics and artificial intelligence (AI). Combined, these features make organizations more resilient. Working in the cloud ensures that security patches are immediately installed, a common failing in traditional systems.

The risks for organizations using cloud services are generally associated with misconfigured storage, poor identity and access management controls, insecure application programming interfaces (APIs), data loss, breaches, and leaks. These risks will remain important throughout 2021 as more businesses adopt cloud computing models.

However, DevSecOps is changing the perception of cloud security. Now, security is baked into the code used to deploy cloud solutions. And the use of secure-by-design principles in software development means that security is considered throughout the engineering process, rather than just at the end of software development. This has meant that many of the old security concerns have disappeared.

Digital acceleration

Enterprises are adopting work from home models, which make collaboration security a growing concern. Organizations are racing to keep up with the security fears that accompany their digital acceleration. To increase productivity, remote employees are using more collaboration tools, such as Slack, Microsoft Teams, and Zoom. These apps create greater data security and compliance issues, and increase the risk of insider threats. The sharing functions can lead to confidential data leakage. Some platforms allow guest access, which creates another set of risks. And Microsoft Teams has an app store full of third-party plugins.

Despite vendors' attempts, these collaboration tools cannot patch vulnerabilities fast enough. In 2020, we have seen zero-day attacks against Slack and Zoom. And as companies spend more money on collaboration applications, we expect threat actors to launch further zero-day attacks against these tools throughout 2021.

Zero trust framework

IT departments in 2020 had to provide millions of employees with remote access to corporate networks. Firms relied on virtual private networks (VPNs), which increased the attack surface, hampered productivity, and broke native application experiences. Through VPN, an authorized user can get access to the entire network and to its sensitive resources. In 2020, hackers specifically targeted VPN connections to get access to networks.

In 2021, as more applications move to the cloud, the number of remote users will only increase. Companies are expected to opt for a more reliable solution called zero trust network access (ZTNA), also known as software defined perimeter (SDP). By 2023, 60% of companies will replace VPNs with ZTNA, according to Gartner.[1] ZTNA is a more agile approach that improves user experience, security, and visibility. Instead of placing authorized users on a network, ZTNA grants them access to specific applications. It reduces attack surface, improves connectivity, and doesn't directly expose applications to the internet.

Advanced threats

COVID-19 scams

In 2021, we will still see the impacts of the new coronavirus on businesses and society. However, these impacts will change as the year progresses. As businesses continue adapting to the new reality, criminals will use these vulnerable times to launch their attacks. In 2020, we saw how cybercriminals took advantage of the fear and uncertainty surrounding COVID-19 and sent themed phishing campaigns, breached systems, and delivered malware.

As COVID-19 continues to rule the headlines, attackers will use this topic in phishing campaigns. Pharmaceutical companies developing vaccines will continue to be targeted by malicious attackers — including nation-states — seeking opportunities to exploit the situation.

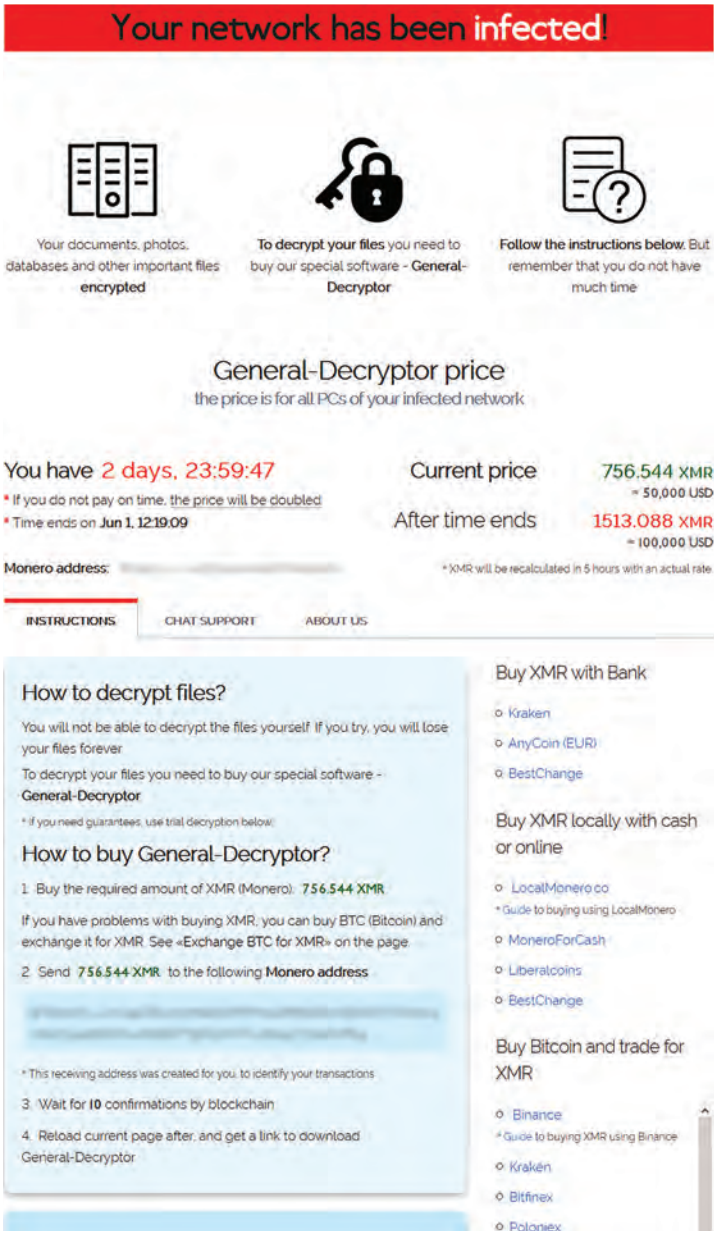
Threats-as-a-service

Today, both malware and ransomware are accessible to anyone who is willing and able to pay for it. Cybercriminals are renting their malware to customers on a subscription basis. With threats available as a service, criminals can target businesses and governments easier. This also opens up malware to people who don't necessarily have the technical knowledge to design the tools themselves.

Malware-as-a-service (MaaS) frameworks offer ready-made botnets that can launch

distributed denial of service (DDoS) attacks. In 2020, we have also seen more MaaS offerings, joined with malware loaders, to deliver ransomware: GuLoader, Emotet, Trickbot, Z-Loader, and Ryuk. Increasingly, threat actors are collaborating on malware operations. This collaborative work makes it challenging to narrow an attack strategy to specific tactics and techniques. As different variants of malware loaders are detected, malware authors are modifying the original variants with newer intrusive techniques that make them more difficult to detect. Such chatter in underground forums is increasing daily.

Figure 1. The ransom note seen by victims in Sodinokibi campaign



Source: Symantec[2]

> Ransomware will be the biggest threat to businesses in 2021

In 2020, one in three ransomware attacks involved Sodinokibi, a ransomware-as-a-service (RaaS).[3] RaaS operations are used exclusively for tailored targeted attacks. At first, they threaten to expose compromised data in the open or on the dark web, and then demand a ransom. When an organization refuses to pay, they conduct a DDoS attack making the victim's services unavailable. This harms the brand reputation of the victimized organization, forcing it to pay. The RaaS model also helps ransomware developers monetize their creations by working with other threat actors. For example, Sodinokibi has engaged with more than 39 such partners.[4] With ransomware becoming more innovative and targeted, it is likely to be the biggest threat to businesses in 2021.

Hyperautomation

AI integration

The use of AI and machine learning (ML) is gaining popularity in cybersecurity circles. The innovative technologies offer a number of benefits that can help minimize cyberthreats, protect vital infrastructure, and stop unwanted intrusions. AI can analyze large quantities of risk data from a variety of sources, providing valuable threat intelligence. By identifying completely new dangers, threat identification systems can reduce

the time that cybersecurity teams spend on detection, response, and remediation. In 2021, we predict that AI and ML technology will gain greater maturity and offer more high-impact uses. Firms will also adopt and implement these solutions to enhance their cybersecurity risk management systems.

AI is also attractive to criminals as they can use it to improve their attacks — making them less costly, more automated, and easier to execute at scale. Threat actors use AI and ML to create new variants of older malware, find vulnerabilities, guess passwords, break CAPTCHA, and clone voices. Automated systems controlled by AI can test systems and networks, scanning for unfamiliar vulnerabilities that could be exploited. This technology can also power social engineering attacks, thus significantly increasing their success rate. In 2021, we can expect attackers to manipulate AI to design new smart malicious innovations.

Automated, data-rich phishing

Phishing is highly reliant on end-user judgment. But data availability, automation, and increased targeting of higher value users make it harder to spot a phishing attack. Today, attackers use more advanced methods to create well-executed business email compromise attacks. Phishing threats are highly localized, personalized, and geotargeted.

While email remains the No. 1 attack vector, cybercriminals are also using other ways to trick their victims into giving up personal information or login credentials, or even sending money. Increasingly, phishing involves SMS texting attacks against mobile devices, or use of messaging on social media and gaming platforms.

In 2021, we predict that automated spear-phishing attacks will prey on fears around the pandemic, politics, and the economy. Historically, malicious actors spent a lot of time crafting spear-phishing emails with malicious attachments or hyperlinks. But this trend is expected to change as cybercriminals now use AI and ML to automate those manual processes. For example, state-sponsored attackers with advanced phishing toolkits can obtain huge amounts of data by scanning social media networks and company websites. With this data, they can initiate large numbers of spear-phishing attacks, with believable content customized to each victim. This automated process will increase the number of spear-phishing emails that an attacker can send

at a time, thus improving the chances of success.

Here are recent examples:

- Instagram-based phishing scams — One phishing campaign targeted thousands of popular Instagram accounts, from celebrities to small-business owners. The scammers sent users a direct message, claiming to be the Instagram help center. The messages said that a copyright violation complaint had been filed against them and that their account was at risk of being deleted.
- WordPress customized phishing page — A phishing campaign targeted WordPress's website owners and administrators. The fraudulent message claimed that a domain name server (DNS) security feature had to be added to the recipient's website. The message urged intended victims to click on a link and enter their credentials to upgrade their website.

Geopolitical tensions

Geopolitics is an important driver of aggressive cybersecurity activity. As these tensions rise in 2021, we can expect destructive cyberattacks against Internet of Things (IoT) devices and industrial control systems (ICS). Health care, energy, oil, gas, and manufacturing sectors will remain the top targets for advanced persistent threat groups and espionage agents. On the dark web, we can also expect a spike in the sale of destructive malware specifically crafted for attacking ICS infrastructure.

Attackers will improve their tactics by placing false flags in the attack life cycle to cover their tracks and reasons behind the attack. For instance, use of Russian language by North Korea's Lazarus Group as well as unusual tool sets can divert an analyst's focus toward the wrong organization. Security professionals might face challenges in mapping evidence during investigations. This can lead to false allegations.

> Health care, energy, oil, gas, and manufacturing sectors will continue to face highest number of cyberattacks

Russia

In 2020, the Russian cyber espionage group Strontium, also known as APT29 and Fancy Bear, targeted more than 200 organizations, including political parties and campaigns, advocacy groups, and consultants serving U.S. Republicans and Democrats. The attacker group known as APT29, working for Russia's Foreign Intelligence Services, breached a top cybersecurity firm

and multiple U.S. government agencies including the Treasury, Commerce, and Energy departments, and the National Nuclear Security Administration. In 2021, we predict that Russian hackers will continue targeting government agencies to understand the plans and motives of politicians and policymakers.

Iran

We predict that Iranian sponsored criminal groups will target U.S. infrastructure in reprisal for the assassination of Iranian Major General Qassem Soleimani. We can also expect that Iranian hackers will continue to target Israel's government, which has been a frequent barrier to Iran's nuclear research projects.

United States

Another significant event of 2020 was Joe Biden's victory in the U.S. presidential election. Biden characterized Russia as an "opponent" and the nation that poses the biggest threat to U.S. security. Similarly, Biden perceives China as a threat to the U.S. economy and also national security. In 2021, we can expect more cyberattacks targeting both nations and their critical infrastructure.

China

In 2020, we saw Chinese national hacking groups targeting countries that falsely accused China of creating the new coronavirus as a weapon. In 2021, we can expect Chinese-backed hackers to launch mass surveillance and espionage campaigns against U.S. citizens by targeting mobile networks.

North Korea

In 2021, we can expect that North Korea will launch attacks on financial institutions, but they will be less geo-linked. It will target countries that are less likely to impose sanctions or have no political leverage over its regime. But to achieve national security goals, companies in the United States and South Korea or other regional adversaries might be targeted.

Intelligent device security

Proliferation of more endpoints

5G will create better connectivity by delivering greater speed and capacity and providing low latency. That will lead to the proliferation of endpoints, as individuals and companies become more connected. By 2025, 2.7 billion devices will be connected to 5G.[5] As a result, attackers will target that growing number of endpoints and connectivity vulnerabilities.

Figure 2. Top 10 countries that intend to pursue multiple national objectives using cyber means

China , United States , United Kingdom , Russia , Netherlands , Israel , Spain, Australia, Canada, Iran

Source: Harvard's Belfer Center National Cyber Power Index (NCPI)

In recent years, IoT devices have become common targets for cybercriminals. Security incidents on IoT devices are an ongoing trend that is only expected to worsen. In 2021, we will see more attacks directed against connected health care devices, smart workplaces, and remote asset monitoring. Digital eavesdropping by hackers using compromised connected speakers, cameras, and screens could also become a more prevalent type of attack.

In time, more IoT gadgets will connect directly to 5G networks, rather than to Wi-Fi routers. This pattern will make those devices increasingly defenseless against direct attack. For home clients, it will likewise make it progressively harder to screen all IoT devices, since they sidestep a central router. The ability to back up or transmit massive volumes of data effectively to cloud-based storage will give attackers rich new targets to breach.

> 2.7 billion devices will be connected to 5G by 2025

In 2021, the emergence of 5G-enabled laptops and hotspots will increase security risks for corporate traffic. Since most connected devices will not implement security by design, threat actors will target unprotected IoT devices with specifically designed malware. We will also see more IoT botnets, many of them based on Mirai and other well-known malware. This will increase remote infrastructure instability and create higher risks of DDoS attacks.

Insider threat and BYOD

Forrester predicted that insider data breaches would increase by 8% and account for one-third of all cybersecurity incidents in 2021.[6] As employees switched to remote working, many companies were unprepared to monitor unauthorized remote access and deal with weak passwords.

> In 2021, data breaches will increase by 8% and account for one-third of all cybersecurity incidents

COVID-19 forced businesses to allow employees to use their personal devices for work. The concept of bring your own device (BYOD) is a way to minimize costs and increase productivity through flexibility. It can also be used to incorporate gig workers into the traditional workforce. In 2021, remote employees and their devices will pose threats to corporate information security; home routers often don't have sufficient security controls. Hackers will target network vulnerabilities to enter the corporate systems through less secure home networks.

Supply chain security

Supply chains are a crucial element of every company's global business operations. Four in 10 cyberattacks occur not in an organization but in one of the links of its supply chain.[7] Thus, the strength of supply chain security depends on its weakest link. Many organizations experience breaches through their vendor ecosystem, when a third-party provider allows the company's data to be compromised. Organizations must constantly share valuable information with their suppliers. Once information is shared, a company loses direct control over it. This puts information at risk, threatening its confidentiality, availability, and integrity.

Accelerated digitization due to COVID-19 creates more vulnerabilities, as companies will have more third-party relationships and those third parties have more digital connections. As supply chains become more connected and complex, in 2021 we will see third-party risk management moving to the top of board priorities.

Mitigating threats

With the increase in targeted cyberattacks across platforms, sectors, and environments, it is increasingly important to understand the threats we face and the severity of their impact.

The trends we see could grow more sophisticated and intensify as technology advances. To stay secure in 2021, companies need to take a proactive cybersecurity approach that is aligned with their business's big picture strategy. To reduce risk and assure quality, they need to constantly measure and recalibrate their security controls. Lastly, organizations need to build cyber resilience capabilities to defend and recover rapidly from disruptions. Below are seven key recommendations that businesses can take to ensure they are always well prepared.

Implement security into design

The proliferation of more endpoints has increased the threat surface. A recent hack of FireEye demonstrated that even if an organization has the best tools, a motivated hacker can find a way into its network via external or internal vectors.

Companies need to ensure they adopt security measures early in the life cycle of any technology or digital change, and ensure the legacy stack is ring-fenced with security cover. It is also important for organizations to develop a mindset that incorporates security in systems, platforms, cloud, applications, and solutions.

Firms also need to continuously monitor and manage compliance in cloud and on-premise environments. They can do so by identifying and reducing vulnerabilities using real-time patching.

To create a culture of security, organizations need to launch awareness campaigns that teach employees about social engineering threats and how to avoid them. These recommendations will maximize visibility of threats and minimize security risks.

Invest in cloud security

As more businesses migrate to the cloud, it is critical that companies ensure their information is secure from cybercrime. Most incidents in the cloud happen because a company lacks a robust cybersecurity strategy. It is

crucial that organizations build a persistent model for remediation of security threats that can secure cloud design, allow for effective risk management, and secure cloud governance.

Cloud services providers offer a wide range of advanced security solutions. Picking the right one for the security problem at hand is difficult. However, with so much choice and inflated security expectations, firms should make sure they have a solid cloud security road map in place before launching the initiative. And cloud security solutions should not compromise the implementation of holistic security controls but go hand in hand with them. A Cloud Center of Excellence construct can work here, governing cloud usage and bringing together a team of "rightly" skilled experts that can evangelize security changes across technology, strategy, and operations.

Embrace the zero trust model

To reduce risks and enhance collaboration, companies need to reassess their existing access policies and parameters. A zero trust model can help create strong security controls that grant the minimal amount of access needed to get the job done. While VPNs connect users to corporate networks, ZTNA provides secure web gateways for remote access. To reduce the chances of an attacker getting into a company's network, organizations should use network segmentation to separate mission critical systems from other areas. A zero trust model will help reduce unauthorized access by verifying everything.

Assess and address supply chain risks

Enterprises need a robust risk management program in place that will provide visibility across the entire supply chain, identify threats and weaknesses, and monitor emerging risks. To effectively manage third-party risks, companies need to create an integrated governance and escalation framework, with clear division of responsibilities, ownership, and integrated workflows.

To address vulnerabilities, it is necessary to create security controls and evaluate partner access using zero trust principles. Companies need to implement risk-based partner segmentation for appropriate system access authentication. Businesses also need to evaluate partner risk through vendor-supplier security posture assessments as well as a questionnaire-based approach.

Secure home office

Home networks are 3 ½ times more likely than corporate

networks to have at least one malware family and 7 ½ times more likely to have five or more distinct types of malware, according to BitSight.[8] The cybersecurity ratings company found that in 45% of businesses, corporate networks were accessed from a device via a home network that was infected with at least one piece of malware. PCs, network-attached printers, and smart home products pose additional risks and can expose companies' services on the internet.

> Home networks are 3.5x more likely to have at least one malware family and 7.5x more likely to be infected by at least five different types of malware

To secure home offices, companies need to require universal multifactor authentication. Organizations need to keep systems updated with security patches and antivirus updates. To prevent data leakage, firms also need to disable insecure devices and protocols, enforce endpoint controls, and keep work and personal use devices separate. To keep BYOD and mobile devices secure, it is crucial to teach employees about risky online behavior — users need to secure passwords or PINs, regularly install new updates, install apps only from trusted developers, and keep personal information out of text messages.

Understand geopolitical threats

Our analysis of activities over the past decade demonstrates a clear link between geopolitical motivations and state-sponsored cyber campaigns. Organizations need to understand geopolitical influences as they can help them predict and prepare for serious cyberthreats before they happen. To determine how, when, and where they are likely to be targeted, organizations need to combine geopolitical intelligence with traditional threat intelligence gathering techniques.

> The global gap between filling vacant positions with qualified cybersecurity personnel will widen to around 2 million by 2022

Use innovative technology

Today, cybersecurity teams are inundated with alerts 24/7 but face shortages of skills and staff. By 2022, the worldwide gap between open positions and qualified cybersecurity personnel will widen to almost 2 million jobs.[9] By automating certain processes, companies can significantly free up staff time, thus enabling them to focus on other tasks. It is also important to remember that adversaries use AI to improve their attack strategies. We believe that it is crucial for companies to adopt innovative technology solutions. Platforms with AI and ML can be used to perform behavior-based analytics at a large scale. These approaches can also be used to hunt, detect, and remediate sophisticated cyberthreats earlier in the process. To learn more about AI and ML use cases, read the recent Infosys article "AI and ML in Cybersecurity Risk Management."

References

1. Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate, Coveware, 2020
2. Sodinokibi: Ransomware Attackers also Scanning for PoS Software, Leveraging Cobalt Strike, Symantec, 2020
3. In-Depth Analysis of the Top Cyber Threat Trends Over the Past Year, CrowdStrike, 2020
4. Insider data breaches set to increase due to remote work shift, ITPro., 2020
5. Market Forecast 5G Connections, Worldwide 2018-2025, CCS Insight, 2018
6. Market Guide for Zero Trust Network Access, Gartner, 2020
7. Securing the supply chain, Accenture, 2020
8. Identifying Unique Risks of Work from Home Remote Office Networks, BitSight, 2020
9. Urgent Need for Cybersecurity Professionals Grows, The Cyber Edge, 2020

Contributors

Anitha Palanisamy

Devakumar Periasamy

Venkatesh Sampath

Producer

Yulia De Bari

Infosys Knowledge Institute
yulia.debari@infosys.com

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.

To view our research, visit Infosys Knowledge Institute at infosys.com/IKI

For more information, contact askus@infosys.com