Cyber Security Predictions for 2021

FUJITSU

shaping tomorrow with you

Contents

Making predictions for 2020 seemed relatively straightforward 12 months ago. The number of cyber attacks was set to increase, and the ongoing digital transformation movement was still going to introduce new risks and vulnerabilities. But 2020 has been turbulent across the world, and the lasting effects of the last 12 months are challenging to predict.

Looking back at our cyber security predictions for 2020, we saw the acceleration of many of the highlighted trends. We predicted that "CISOs will need to play catch up to properly get to grips with changing risk profiles in areas such as the cloud," while in reality, the rapid growth in the use of cloud services – driven by an enormous shift in technology use due to the Coronavirus pandemic – left CISOs with a lot of work to do.

We also predicted that organizations would start to make better use of the security tools provided by their cloud service providers. In a year where many companies placed a freeze on IT budgets, many organizations chose to stick with tools available from existing partners rather than switch to cloud-agnostic tools. Furthermore, we predicted a rise in phishing extortion emails targeting people with claims that potentially embarrassing online behavior would be released to their contacts. This approach increased in a year where many phishing emails focused on the pandemic.

As we look forward to 2021, and what is likely to be a year of significant change, we are laying out our predictions. Unsurprisingly, we expect challenges to persist as organizations look to ensure their remote workforces' security and productivity. We also expect a reset in the attitudes towards risk as organizations grapple with the dilemma of tackling new challenges with lower security budgets. And we anticipate the increased use of new technologies to open new security vulnerabilities.

The next 12 months will undoubtedly have its challenges. Still, organizations that are aware of these risks and take steps to mitigate their impact will be well-positioned to secure future growth in what is likely to be another interesting year.

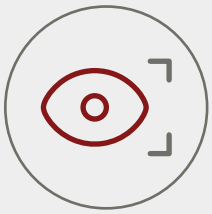
1 Working from home has increased the attack surface

The proliferation of working from home has forced many organizations to expedite their digital strategies.

Employees have been forced to change their working habits and patterns, as many people are now working from home. This increases the so-called attack surface for any company – mainly if employees use personal devices to connect to corporate resources, since these may not have an enterprise-class level of protection. Spear-phishing emails, in particular, increase the threat to organizations. These often follow traditional attack profiles in terms of initial reconnaissance via social media before any attempt is made to compromise a user's credentials. The end state is a crafted, targeted email. Increasingly, these emails appear to be more credible.

As home working looks set to continue, organizations should make sure employees are educated and alert for phishing emails.

2 Success requires finding the right balance between security and user experience



The global pandemic has changed user behavior in terms of how we are communicating, working, consuming, and spending our free time. This creates new requirements for the services we use. One common theme to all these changes and new demands is that all require our digital identities.

The sophistication of how organizations use, manage, and protect identities has not yet reached the so-called new normal. For many, this means that security controls surrounding identities still have a negative impact on user experience. Users find security to be complicated, cumbersome, and time-consuming. Consequently, frustration often results in users abandoning a service or bypassing security controls. The winners in the new normal will be those able to adapt to these new requirements and provide a strong user experience in a secure and trusted way.

3 Risk appetites must be re-evaluated

Many security teams will enter 2021 with reduced budgets due to the impact of COVID-19.

This will require careful evaluation of spending priorities and will necessitate hard choices about which investments to cut. This will mean firms cannot evolve their security posture in line with changing security threats. Consequently, they will have to **accept a higher risk** that complex attacks will be successful and go undetected for longer.

4 New life for ransomware attacks

Ransomware attacks are set to grow in scale and sophistication throughout the next year.

We are already seeing increasing numbers of attacks on previously untapped market sectors, such as healthcare. The nature of the damage of a ransomware attack is also changing. We see an increase in extortion in terms of the number of attackers threatening to release stolen data into the public domain (also known as Doxxing) rather than simply locking it away.

To compound these issues, we expect to see greater use of AI technology in ransomware attacks, as attackers seek to launch increasingly sophisticated, coordinated attacks to evade today's detection measures.

AI will be part of the problem. It also offers part of the solution, as it continues to develop greater capabilities to detect and flag suspicious behavior.

5 The age of disinformation attacks

The pandemic has had a significant impact on everyone and disrupted our social and work lives.

There has been one constant throughout: cybercriminals leveraging current topical themes, such as Brexit, elections, and COVID-19. At their core, criminals are launching social engineering attacks designed to take advantage – and even create – panic and fear. In 2021, we will see new themes used to target businesses and individuals, focusing on pandemic-related topics such as mandatory vaccines, health passports, mass testing, and lockdowns. We anticipate a lot of disinformation on these topics. With the desire of many to return to post-pandemic normality, we expect multi-vector attacks built on these themes from both criminal gangs and nation-states. Some countries are already testing the use of machine learning to defend against disinformation campaigns.

6 Security compromised while privacy preserved

DNS over HTTPS is set to become a common attack vector.

This has become a standard feature of mainstream web browsers such as Google Chrome, Mozilla Firefox, and Microsoft Edge. Effectively, this means security controls cannot analyze website requests. On the surface, this is a viable development in terms of user privacy. However, many cyber security attacks rely on access to an external website to retrieve malicious files as part of a multi-stage attack. DNS over HTTPS encrypts these requests, meaning that these requests are masked from security controls, and giving an attacker the upper hand before cyber defenders can react and respond.

Organizations should carefully evaluate whether to enable this feature on corporate devices and consider the new office dynamic, with an increasing number of workers connecting from home on personal devices to corporate infrastructure and services, increasing the opportunity for this attack type.

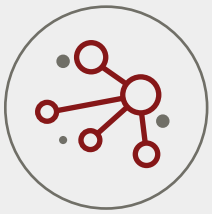
7 5G will rapidly open more potential vulnerabilities

As 5G technology matures and telcos continue to roll out 5G networks, security concerns will also increase.

Among others, these will stem from an endless stream of insecure IoT devices that manufacturers are rushing to market, as well as the security requirements of critical national infrastructures. 5G security is and will remain a national security concern. It will increase enterprises' need to revisit their security strategy for using public and untrusted mobile networks.

Organizations cannot ignore the opportunities that 5G provides. Nevertheless, to ensure their safety, they should adopt a secure-by-design mindset when exploring how to use 5G networks best.

8 Security concerns for the Internet of Behaviors

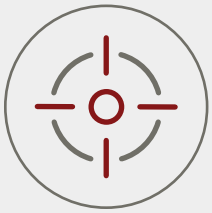


As we develop new remote ways of going about our everyday business during the pandemic, the world is now connected more than ever.

The Internet of Things (IoT) has driven innovation in every area of life, including connected homes, internet-enabled and autonomous cars, health monitoring via smartwatches, and even the testing of drones to deliver our online shopping. However, the IoT exploded without a robust security framework. The proliferation of attacks meant that the privacy of CCTV cameras and some other IoT devices was compromised in huge DDoS attacks. 5G will accelerate the potential for the use of connected devices to track individuals' everyday behavior, observe where we go, who we see, where we shop, what we buy – and even to use facial recognition to work out our identity.

This innovation must be coupled with robust data privacy controls, which should be evaluated up front rather than as an afterthought, so we can trust that the same data is not used nefariously and targeted by threat actors.

9 Hitting where it hurts



Attacks that target characteristics specific to certain industries will continue to present more significant opportunities.

The number of attacks on connected cars has **risen sharply** in the last year, while in the manufacturing and utility sector, **Operational Technology (OT) systems have seen a quadruple figure percentage increase in attacks**. The targeting of these technologies is growing because they have less mature security controls. Many can directly impact an organization's operations. We expect this trend to continue in 2021.

On the positive side, we expect more organizations to **recognize the value of cloud computing as a reliable means to deliver OT security** to locations where it is not practical or feasible for a physical deployment.

10 Cloud-centric does not equal threat free

Multi-layered cloud protection will take on new importance in 2021.

As organizations move toward a cloud-centric future, there will be continued disruption attempts for monetary, intellectual property, or political gain. In the first half of 2019, Netscout reported 4.8 million DDOS attacks. Ransomware attacks were also up 50% in Q3, according to data from Check Point. Such attacks can cripple businesses in very short timeframes, and the financial impact has seen companies willing to pay a ransom for their data or bring their services back online.

This trend is a cause for concern, and multi-layered cloud protection should be a focus area for many businesses in 2021 as they balance digitalization and security.

Conclusion

Our predictions for 2021 underline that cyber threats pose a greater risk than ever for organizations looking to embrace digitalization.

With the increased volume, complexity and business impact of attacks, organizations must rethink how they approach these risks if they are to stay secure. Organizations that integrate security-by-design as a fundamental part of their transformation are best positioned to flourish as the world moves through the recovery stage and returns to growth.

Fujitsu has extensive experience in providing Managed Security Services and Security Consulting Services to organizations around the world. Naturally to the most stringent security standards. We at Fujitsu help our customers to build trust with their customers and embrace the future with confidence.

Why Fujitsu Security?

When working with you to safeguard your business, we look at all of the elements needed to achieve a successful cyber security program:

- Our all-inclusive approach to security works to combine our highly skilled threat intelligence analysts using advanced analytics tools and best-of-breed security technologies to deliver 24/7 support
- The strength of our proven experience, vendor relationships, and global scale means that we are well placed to optimize your approach to security and protect your reputation, operations and bottom-line.

Taking an intelligence-led approach enables us to deliver immediate value and, by providing impartial and industry-specific guidance, we can advise you on how to mitigate risks, helping your business focus on opportunities to create value – securely.

> Find out more or contact your Fujitsu Account Manager to see how we can help you manage the ever-changing landscape of cyber security threats – now.

FUJITSU

Tel: +44 (0) 1235 79 7711
Email: askfujitsu@fujitsu.com
Web: www.fujitsu.com/emeia/themes/security/