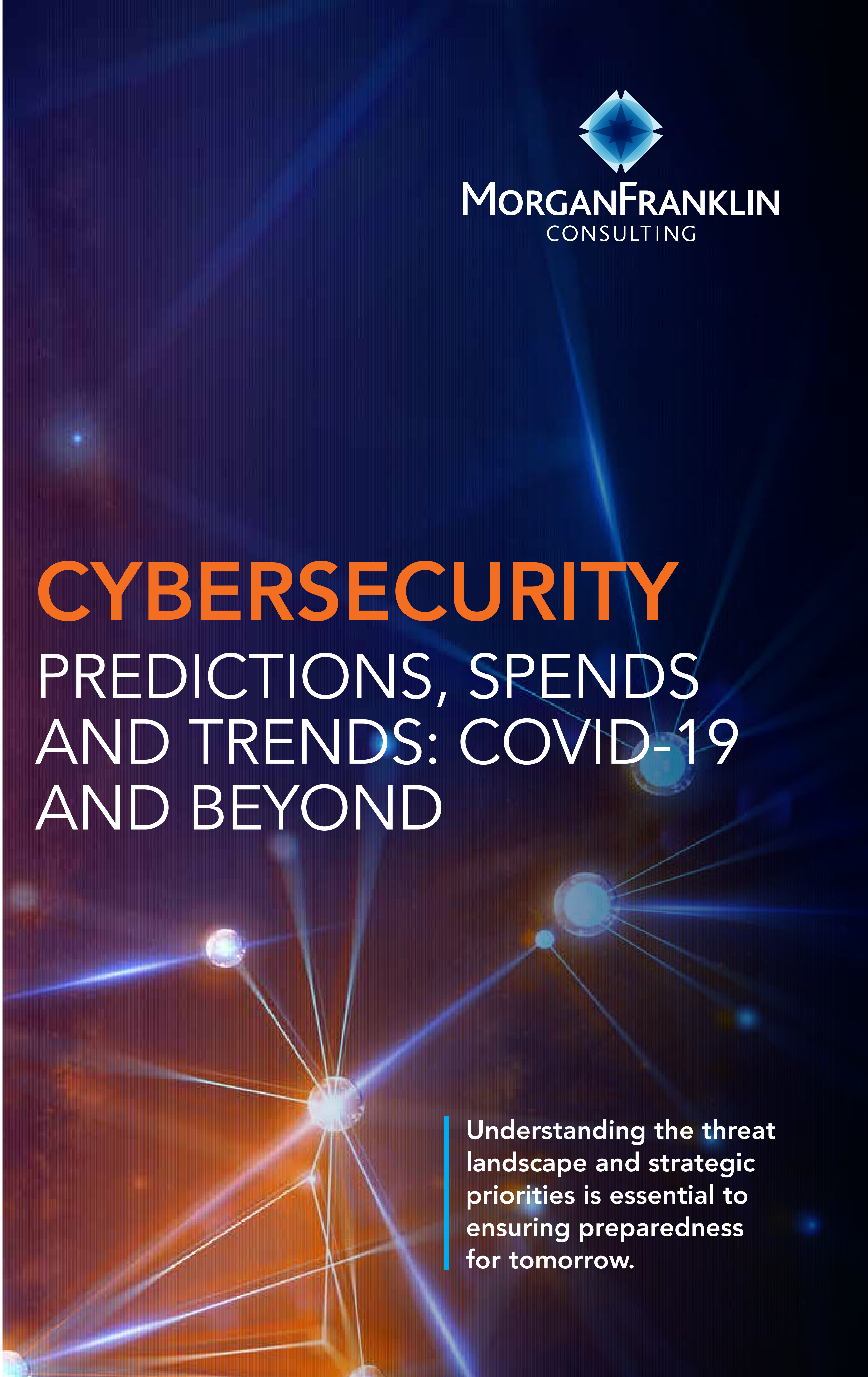


MorganFranklin
CONSULTING

2020

CYBERSECURITY

PREDICTIONS, SPENDS AND TRENDS: COVID-19 AND BEYOND

Understanding the threat landscape and strategic priorities is essential to ensuring preparedness for tomorrow.

Understanding the evolution of the cybersecurity threat landscape and strategic priorities for organizations throughout 2020 is essential to ensuring that an organization is prepared to meet the cybersecurity challenges of tomorrow.

Evolution of the Cybersecurity Landscape

Every year, the cyber threat landscape is different from the previous one, and 2020 is no exception. Expanding digital attack surfaces, increased regulatory complexity, and concerns about software supply chain security all create challenges for enterprise cybersecurity.

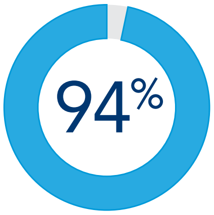
Growth of Digital Attack Surfaces

Organizations' attack surfaces are rapidly expanding. Adoption of cloud computing, the Internet of Things (IoT), and enterprise use of mobile devices, whether company-owned or bring your own device (BYOD), creates new security challenges for organizations.

CLOUD COMPUTING

In 2019, over 94% of companies used cloud computing, and 84% of them adopted a multi-cloud strategy[1], spreading their cloud footprint over multiple cloud service providers. This complex cloud architecture is difficult to secure, and the majority of security professionals struggle with the cloud shared responsibility model, which is a fundamental concept of cloud security.[2]

COVID-19 has demonstrated the value of cloud computing as "shelter in place" orders have limited organizations' ability to maintain on-site infrastructure.



of companies used cloud computing in 2019

While the use of cloud computing is growing, security teams' understanding of the environment and the cloud shared responsibility model has not kept up. As a result, the number of cloud-related data breaches is likely to continue to increase in 2020 and beyond.

THE INTERNET OF THINGS

While the number of consumer Internet of Things (IoT) devices is growing rapidly, the use of the IoT is not limited to the home. In 2020, enterprise and automotive use of IoT devices is expected to grow to 85.8 billion connected endpoints, a 21% increase from the previous year[3]. These devices are used for a variety of sensitive and critical operations, including devices intended to monitor critical infrastructure and Internet of Medical Things (IoMT) devices that collect and process sensitive medical data.

This growth in the use of IoT in business contexts is concerning since IoT devices are notorious for their poor security. The famous Mirai botnet was built simply by logging into devices using

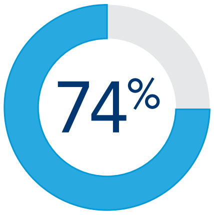
[1] https://info.flexera.com/SLO-CM-WP-State-of-the-Cloud-2019

[2] https://www.tripwire.com/state-of-security/security-data-protection/cloud/survey-84-of-security-pros-said-their-organizations-struggled-to-maintain-security-configurations-in-the-cloud/

[3] https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io

default usernames and passwords,[4] and this attack vector is still a threat, as demonstrated by a recent leak of over 500,000 active devices' IP addresses and login credentials.[5]

Beyond poor credential security, IoT devices are prone to vulnerabilities and built-in backdoors. Since these devices often receive limited oversight and infrequent patching but are connected to the Internet, they are a potential vector for an attacker to gain a foothold on enterprise networks. This is especially a concern in the healthcare sector, where organizations are overwhelmed with the response to COVID-19 and networks contain a wealth of sensitive patient data.



of companies had bring your own device policies in 2019

MOBILE DEVICES

The use of mobile devices for business purposes is growing rapidly. In 2019, over 74% of businesses had BYOD policies allowing employees to use their personal devices for business purposes.[6] With COVID-19, this number is likely closer to 100%. However, nearly half of organizations lack a clear BYOD security policy.

Mobile devices represent a serious potential security risk for organizations. These devices move from untrusted external networks to the internal wireless network, potentially unintentionally carrying malware behind the network firewall or allowing internal sensitive data to be stolen on insecure WiFi. Additionally, many mobile device manufacturers are slow to provide patches, if they provide them at all, leaving mobile devices open to the latest attacks.

WORK FROM HOME AND PERSONALLY OWNED DEVICES

The growth of work from home in the wake of COVID-19 created new potential attack vectors for cybercriminals. The Remote Desktop Protocol (RDP) is a commonly-used solution to enable employees to access their corporate machines - which have all the necessary software installed for them to do their jobs - from their houses. However, RDP is a top infection vector for ransomware, and the increase in organizations exposing it to the public Internet has created a target-rich environment for cybercriminals performing credential stuffing attacks.

Employee-owned devices used for business also present cyber threats to the enterprise. These devices likely do not comply with corporate policies or have the organization's antivirus and other security solutions installed on them. Despite this, they are granted access to the corporate network and sensitive data, especially during the COVID-19 pandemic.

INCREASED REGULATORY COMPLEXITY

The passage of the EU's General Data

[4] https://www.csoonline.com/article/3126924/here-are-the-61-passwords-that-powered-the-mirai-iot-botnet.html
[5] https://www.zdnet.com/article/hacker-leaks-passwords-for-more-than-500000-servers-routers-and-iot-devices/
[6] https://continuitycentral.com/index.php/news/technology/3973-many-companies-are-putting-their-data-at-risk-by-failing-to-secure-byod

Protection Regulation (GDPR) and its enactment in May 2018 kicked off a rush of new data protection laws. In January 2020, the California Consumer Privacy Act, the most famous of the new US state-level data protection laws went into effect as well. Additionally, new laws are going into effect in Brazil and Thailand, and India and South Korea are looking to increase their data privacy protections.[7]

Each additional data protection law that is passed and goes into effect increases the cost and complexity of maintaining compliance with applicable laws. Over one-third of enterprises spent more than one million dollars on achieving GDPR compliance alone.[8] As new data protection laws are passed and go into effect in 2020, companies require security architectures that comply with a patchwork of data protection laws and provide security against real attacks.

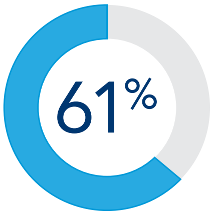
These challenges were exacerbated by the forced transition to telework inspired by COVID-19. During the pandemic, reporting requirements were relaxed for some regulations, but regulatory compliance was still mandatory. Organizations needed to rapidly discover how to maintain compliance with environments and workflows not covered by their existing compliance strategies.

THIRD-PARTY RISK MANAGEMENT

Organizations can inherit third-party risk from a number of different sources. Two common sources of external risk are the software supply chain and relationships with third-party vendors and suppliers.

The security of the software supply chain is a growing concern for many enterprises. Software developed in-house can include vulnerabilities, but it can also inherit vulnerabilities or embedded malicious code from third-party code that it imports or is dependent upon. The average web application has 1,000 dependencies, each of which have an average of 80 dependencies of their own.[9] Each of these dependencies represents a potential security leak, and cybercriminals are actively working to exploit the software supply chain in certain industries.

Third-party risk can also originate from relationships with vendors, suppliers, and partners. 94% of organizations give external organizations access to their networks, and 72% of these partners have elevated or administrator-level permissions.[10] Additionally, 61% of organizations lack the visibility necessary to determine if third parties are accessing unauthorized data. Unsecured third-party accounts on an organization's network enable a cybercriminal to use a partner's network to access an organization and exfiltrate sensitive data.



of companies lack the visibility to determine if third parties are accessing their data

[7] https://www.endpointprotector.com/blog/data-protection-legislation-around-the-world-in-2020/
[8] https://datagrail.io/gdpr-ccpa-cost-report
[10] https://www.cbsnews.com/news/ransomware-attack-621-hospitals-cities-and-schools-hit-so-far-in-2019/
[11] https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate
[12] https://www.coveware.com/blog/marriage-ransomware-data-breach
[13] https://arstechnica.com/information-technology/2020/02/new-ransomware-intentionally-meddles-with-critical-infrastructure/
[14] https://www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704
[15] https://enterprise.verizon.com/resources/reports/dbir/

Ongoing Trends in 2020

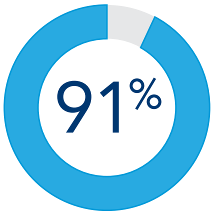
The cyber threat landscape can change rapidly. However, some trends tend to continue from year to year. Many of the major threats faced by organizations in 2019 are expected to be a significant security concern through 2020 as well.

RANSOMWARE

Ransomware has existed for over a decade but became famous in 2017 with the outbreaks of the WannaCry ransomware worm and the NotPetya wiper. Since then, ransomware has consistently held its position as one of the greatest cybersecurity threats facing businesses.

With WannaCry, ransomware attacks were designed to cause wide-scale damage, spreading themselves through networks by exploiting unpatched vulnerabilities. In 2019, the main focus of ransomware attacks shifted to exploiting large organizations with extremely focused attacks. The first three quarters of 2019 alone included over 600 attacks against schools, hospitals, and similar institutions.[11] In 2020, ransomware attacks will continue to be a threat to large organizations. Ransomware variants like Ryuk and Sodinokibi specifically target large enterprises and commonly demand ransoms of more than $1 million. Paying the ransom does not guarantee data recovery as only 98% of organizations receive a decryptor after paying, and these decryptors recover approximately 97% of an organization's data.[12]

Ransomware attacks have also evolved in 2019 to include new functionality. Ransomware authors have added data stealing functionality to their malware, enabling them to threaten a data breach if ransomware are not paid.[13] Ransomware variants have also been detected to specifically target critical infrastructure, killing crucial processes on industrial control systems.[14] In 2020, it is likely that additional innovations will expand the impacts of a ransomware attack.



of cyberattacks start with a phishing email

PHISHING

Phishing attacks have been a leading enterprise security threat for a long time. In 2016, 91% of successful cyberattacks started with a phishing email,[15] and not much has changed in recent years. In 2019, almost a third of data breaches involved a phishing email.[16]

Phishing attacks are a common technique because they consistently work. However, this does not stop phishers from innovating. In recent years, phishing

[11] https://www.cbsnews.com/news/ransomware-attack-621-hospitals-cities-and-schools-hit-so-far-in-2019/
[12] https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate
[13] https://www.coveware.com/blog/marriage-ransomware-data-breach
[14] https://arstechnica.com/information-technology/2020/02/new-ransomware-intentionally-meddles-with-critical-infrastructure/
[15] https://www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704

[12] https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate
[13] https://www.coveware.com/blog/marriage-ransomware-data-breach
[14] https://arstechnica.com/information-technology/2020/02/new-ransomware-intentionally-meddles-with-critical-infrastructure/
[15] https://www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704

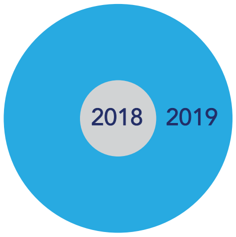
[16] https://enterprise.verizon.com/resources/reports/dbir/

attacks targeting mobile devices have increased dramatically, taking advantage of an "always connected" culture. In early 2020, phishers have taken advantage of the climate of uncertainty and fear associated with the COVID-19 pandemic to increase the effectiveness of their attacks.

In 2020, phishers are also anticipated to start making use of artificial intelligence (AI) and machine learning (ML) to increase the effectiveness of their attacks.[17] The effectiveness of phishing emails and landing pages will be automatically tested to improve conversion rates, and common maintenance activities, like registration of new phishing domains, may become increasingly automated.

CREDENTIAL STUFFING

Credential stuffing attacks take advantage of the massive amounts of personal data leaked during data breaches. Since 62% of people reuse passwords across personal and business accounts,[18] breached passwords present a significant threat to enterprise security. In 2020, the number and volume of credential stuffing attacks will only increase. Malicious bots already comprise one-fifth of Internet traffic,[19] and, as data breaches accelerate and the value of breached data rises, cybercriminals will only have more credentials to test with stuffing attacks.



Cyberattacks grew by 300% by the middle of 2019

Additionally, the growth of telework in the wake of COVID-19 means that companies are exposing more systems to the public Internet to enable employees to work effectively from home.

CLOUD BREACHES

While 94% of businesses use cloud computing,[20] many of these organizations are not securing their data properly in the cloud. Over half of businesses using cloud services have had customer data leaked in a data breach.[21]
In 2020, as more sensitive data is added to cloud deployments, the rate and volume of cloud data breaches is only expected to increase. With over half of organizations storing data unencrypted in the cloud,[22] any security misconfiguration that allows unauthorized access to an organization's cloud resources can result in a data breach.

IOT/IOMT-FOCUSED ATTACKS

In the first half of 2019, cyberattacks targeting IoT devices grew by 300%.[23] Additionally, cyberattacks targeting IoMT devices have resulted in 82% of healthcare organizations with deployed IoT devices experiencing cyberattacks against these devices.[24] During COVID-19, During COVID-19, healthcare has been especially targeted by cybercriminals, so this number is likely to be much higher in 2020 and beyond.

[17] https://threatpost.com/2020-cybersecurity-trends-to-watch/151459/
[18] https://www.darkreading.com/informationweek-home/password-reuse-abounds-new-survey-shows/d/d-id/1331689
[19] https://www.zdnet.com/article/bad-bots-focus-on-financial-targets-make-up-20-percent-of-web-traffic/
[20] https://info.flexera.com/SLO-CM-WP-State-of-the-Cloud-2019
[21] https://www.helpnetsecurity.com/2020/01/28/accessing-cloud-services/
[22] https://www.thalesecurity.com/2019/cloud-security-research
[23] https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/#4b98f4b58926

IoT devices, like voice assistants and Internet-connected cameras, are "always on", meaning that they have constant access to a great deal of sensitive security data. During COVID-19, insecure personal IoT devices may be capable of viewing computer screens containing sensitive company data or recording business voice and video calls.

This, combined with the generally poor state of IoT security, means that they will continue to be a major target of attack in 2020 by cybercriminals targeting this sensitive data or wishing to add them to Distributed Denial of Service (DDoS) botnets.

CYBERSECURITY SKILLS GAP

One of the greatest challenges for enterprise cybersecurity is finding sufficient cybersecurity talent to staff their in-house SOCs and security teams. The cybersecurity industry is currently facing a skills shortage with an estimated 4.07 million positions currently unfilled. [25]

4.07 MILLION **cybersecurity positions are currently underfilled**

As the need for cybersecurity talent outpaces the supply, the cybersecurity skills gap will only grow larger in 2020. Globally, the cybersecurity workforce must grow 147% to meet demand, indicating a shortfall that is unlikely to be made up any time soon.

Next-Generation Cybersecurity

One of the primary drivers of the evolution of the cybersecurity threat landscape is the introduction of new technology and workflows. In 2020, the growing use of 5G, deepfake technology, and enterprise collaboration tools all impact the face of cyber threats.

5G NETWORKS

5G mobile networks are rapidly reaching maturity and widespread adoption. With 5G, mobile users will experience much higher data speeds, and the network infrastructure will also be capable of supporting a much denser set of mobile endpoint devices.

This evolution of mobile network technology sets the stage for an increase in use of enterprise IoT and mobile devices. Mobile networks offer more flexibility for device deployment; however, they also decrease the visibility of enterprises into business traffic.

5G networking also creates significant supply chain security concerns. A limited number of vendors are capable of providing 5G technology, making them more vulnerable to targeted cyberattacks. Additionally, 5G technology is more heavily dependent upon software, amplifying the potential impact of coding errors and software vulnerabilities.

COVID-19 has increased the pace of the digital revolution.

[24] https://www.hipaajournal.com/82-of-healthcare-organizations-have-experienced-a-cyberattack-on-their-iot-devices/
[25] https://www.isc2.org/News-and-Events/Press-Room/Posts/2019/11/06/ISC2-Finds-the-Cybersecurity-Workforce-Needs-to-Grow--145

DEEPFAKES

Deepfake technology enables the creation of extremely realistic fake audio or video recordings of an individual. The potential impacts of deepfake technology on election security and similar events are significant.

However, targeted deepfake attacks can also have a significant impact on an organization's cybersecurity. Impersonation of executives in social engineering attacks is already a well-established attack vector, and deepfake technology only makes these attacks more realistic. One attack, using AI to mimic the voice of the CEO on a phone call, enabled cybercriminals to steal $243,000 from a company,[26] and these types of attacks will only grow more common in 2020.

ENTERPRISE COLLABORATION TOOLS

Traditionally, most phishing attacks have targeted email since it is the primary medium for business communications. However, this is changing as organizations move to enterprise collaboration platforms, like Slack, and cloud-based storage, like Google Drive or OneDrive.

Since most enterprise cybersecurity awareness training focuses on the email threat, many employees trust these other platforms implicitly. Phishing campaigns using weaponized cloud-based documents or targeting employees through messaging applications will become even more popular in 2020.

COVID-19 has forced organizations to become increasingly reliant on online collaboration platforms and these platforms are receiving more attention from security researchers and cybercriminals, as demonstrated by the large number of security vulnerabilities discovered in the Zoom platform.

Enterprise Security Priorities for 2020

Expanding attack surfaces, ongoing cyber trends, and emerging new technology all create changes in the cyber threat landscape. Addressing the evolution of cyber threats and positioning themselves to face future ones drive certain enterprise cybersecurity initiatives in 2020.

ADDRESSING THE INSIDER THREAT

Over one-third of data breaches involve insiders.[27] Whether an employee leaks sensitive data with intention or through negligence, trusted employees pose a serious threat to enterprise data security. COVID-19 has only exacerbated this issue, as telework creates new opportunities for sensitive data to be leaked from insecure personal networks and devices.

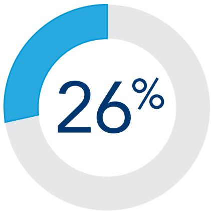
Insider threats can be difficult to detect and remediate since the employee already has legitimate access to an organization's systems and data. Protecting against insider threats requires implementation of a zero-trust security architecture, limiting access to data and systems on a need-to-

[26] https://threatpost.com/deep-fake-of-ceos-voice-swindles-company-out-of-243k/147982/
[27] https://enterprise.verizon.com/resources/reports/dbir/

know basis, and performing behavioral analysis to enable detection and response to anomalous behaviors that could indicate a potential threat.

CORRECTING MISALIGNED PRIORITIES

An accurate understanding of the organization's current cyber risk is essential to proper allocation of funding. However, many C-suites include executives with very different views of their company's current security posture. For example, a survey of Australian executives found that only 6% of CEOs were aware that they had experienced a data breach, compared to 63% of CISOs.[28] Similarly. 44% of CEOs believed that their company could rapidly recover from a cyberattack, but only 26% of CISOs agreed.



of CISOs believe their company would survive a cyber attack

Correcting these, and other cybersecurity misconceptions, requires clear communication between executives. The fact that, in 2019, one-fifth of CISOs now report directly to the CEO,[29] as opposed to the CIO, demonstrates that organizations are increasingly making cybersecurity a priority.

DEPLOYING MULTI-FACTOR AUTHENTICATION

Poor password security is a significant threat to enterprise security. An estimated 62% of employees reuse passwords between personal and business accounts, and the growth of credential stuffing attacks, especially against application programming interfaces (APIs) and the financial sector,[30] indicates that cybercriminals are taking advantage of this.

Implementing multi-factor authentication is a growing priority for executives. As employee and user account passwords are compromised, multi-factor authentication makes it more difficult for cybercriminals to gain access to these accounts. In 2020, adoption of multi-factor authentication is expected to grow, especially methods using biometric data.[31] One driver for this shift is the need to maintain regulatory compliance during the COVID-19 pandemic as regulations such as PCI DSS require MFA for teleworkers.[32]

CREATING A DEVSECOPS CULTURE

The number of vulnerabilities discovered in production code is significant. In 2019, over 22,000 new vulnerabilities were discovered and disclosed.[33] A patch-based vulnerability management process creates significant burdens for both the creator and users of the software and increases organizations' vulnerability to attack.

Reducing the number of vulnerabilities that reach production code requires integration of security into all phases of the development lifecycle. DevSecOps, which takes advantage of continuous

[28] https://www.helpnetsecurity.com/2020/01/06/cyber-risks-2020/
[29] https://www.itproportal.com/news/more-cisos-are-reporting-directly-to-the-ceo/
[30] https://www.csoonline.com/article/3527858/apis-are-becoming-a-major-target-for-credential-stuffing-attacks.html
[31] https://blog.lookout.com/five-ways-security-landscape-will-shift-2020
[32] https://blog.pcisecuritystandards.org/how-the-pci-dss-can-help-remote-workers
[33] https://pages.riskbasedsecurity.com/2019-year-end-vulnerability-quickview-report

integration and testing, helps to facilitate this by ensuring that vulnerability scans are run continuously and automatically, decreasing the effort and technical debt associated with remediating them.

INVESTING IN CYBER INSURANCE

The risk and impacts of cyberattacks are growing. Organizations are increasingly falling prey to expensive attacks, like ransomware or business email compromise (BEC) scams, and the average cost of an attack is growing.

As a result, organizations are anticipated to invest more in cybersecurity insurance in 2020.[34] While the expenses that insurance providers are willing to cover is limited, they can help to defray the costs associated with a cybersecurity incident.

Meeting Your Security Goals with MorganFranklin

MorganFranklin Consulting offers enterprise cybersecurity professional services and Managed Security Services (MSS) designed to meet an organization's unique cybersecurity needs. Partnering with MorganFranklin gives an enterprise access to deep cybersecurity expertise, full-service or a la carte SOC as a Service offerings, and the ability to fill vacant cybersecurity roles with trained consultants. Reach out for a consultation to find out how MorganFranklin can help you to address the 2020 cybersecurity threat landscape. ■

[34] https://www.helpnetsecurity.com/2019/12/30/2020-cybersecurity-trends/