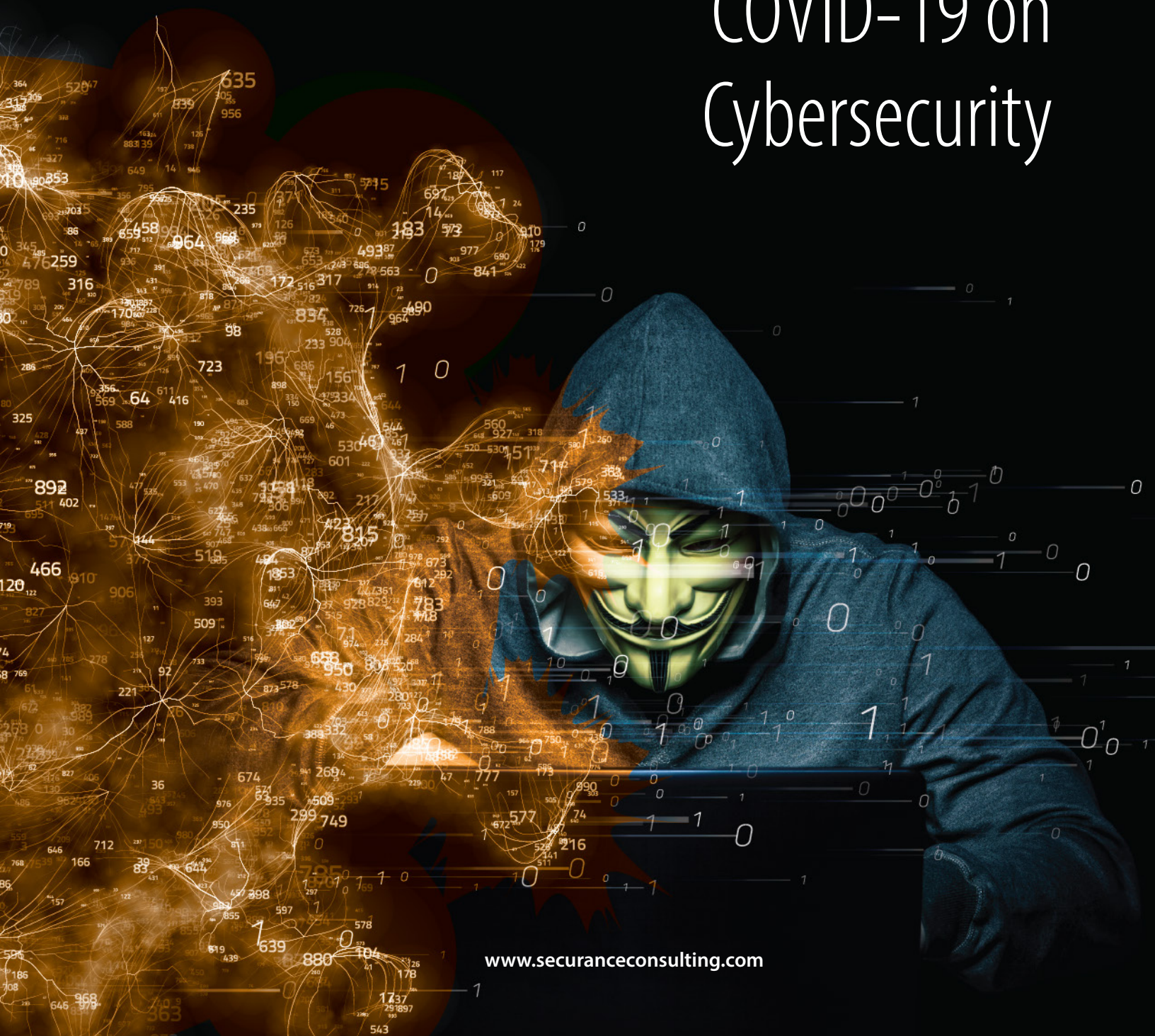
SECURANCE CONSULTING
Advantage of Insight AI

The Impact of COVID-19 on Cybersecurity



www.securanceconsulting.com

THE NEW NORMAL

COVID-19 has had far-reaching consequences, not only geographically, but also across industries. Over the past year, our personal lives have shifted (or been put on hold); careers have been altered or lost. The constant is ambiguity, and the questions that we ask include:

When will we get back to normal?
What changes will remain?
What is the "new normal"?

When it comes to cybersecurity, IT professionals, their employers, and other employees all felt the impact of COVID-19, though in different ways. As the pandemic set in, IT professionals scrambled to fortify defenses, instate new remote working processes, and connect an unexpected network of home offices. Employers made tough decisions about how to keep operations churning securely, despite budget and staff cuts. Employees struggled to perform well at their jobs while working from home with new technologies and processes in place.

The obvious cause of the new normal is COVID-19. But, the root cause of the changes in the cybersecurity landscape is a little more complicated— and it affects everyone, whether or not they work in cybersecurity.

THE CAUSE

As federal, state, and local governments mandated quarantines, many businesses shut down on-premise work. This caused an unprecedented number of traditional commuters to work from home (WFH), in many cases, using unsecured remote working devices. With little warning, IT departments had to create remote infrastructure where there had previously been little to none. This sudden shift, backed by scant budgets and foreknowledge, left many with ramshackle processes, vulnerable devices, and a growing cyber attack surface.

In unfamiliar territory, everyone and everything is vulnerable. Over the past year, untested remote infrastructure, untrained personnel, and a lack of formal cybersecurity processes created the opening malicious actors needed to launch a significant number of dangerous (and lucrative) attacks.

THE CHANGES

Securing remote infrastructure at a moment's notice

COVID-19 took the world by surprise. Virtually overnight, remote infrastructure became critical to sustain business operations. Organizations that didn't have the budget, time, or resources to mobilize quickly and securely opened attack avenues for malicious actors. For example, delayed updates to email and web filters allowed malicious emails to be delivered to employees— notoriously, the weakest link in cybersecurity.

Additionally, reduced budgets, caused by revenue losses, meant that businesses had to compromise to secure the WFH environment. For some businesses, this meant setting other, less critical security projects aside. A recent report by McKinsey cites the following examples:

A software company rerouted resources designated for a security automation project to cover gaps in multifactor authentication (MFA)

A consumer packaged goods company postponed cybersecurity war games to accelerate the rollout of a virtual private network (VPN)

A financial services company postponed security red team exercises to mitigate vulnerabilities in remote work applications[2]

For companies such as these, beefing up remote access security was a significant investment— and a setback in other areas of cybersecurity.

Human error

Employees have always been prone to social engineering attacks, but, according to surveys taken during the pandemic, they're more so when WFH. At the start of the pandemic in March 2020, 61 percent of IT and security leaders were concerned that cyber attacks targeting their employees would increase— and they were right. In March alone, organizations saw a 26-percent increase in the volume, severity, and and/or scope of cyber attacks.[3]

The Multi-State Information Sharing and Analysis Center (MS-ISAC) and Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) Security Operations Center (SOC) saw an in increase in these attack types in particular:

- Phishing and malspam
- Credential stuffing
- Ransomware
- Remote desktop protocol (RDP) targeting
- Distributed denial of service (DDoS) attacks[4]

> **91%** of global enterprises reported an increase in overall cyber attacks as a result of employees working from home.[5]

THE IMPACT

Cybersecurity providers and investments

Now more than ever, businesses look to cybersecurity providers for solutions. They expect providers to deliver not only new approaches and technologies to fight emerging threats, but also customized solutions that allay specific pain points. In this time of uncertainty— and evolving cyber threats— many organizations must rely on security providers to plan long-term protection strategies and implement the right technologies (e.g., cloud, remote access) to safeguard data.

That said, most organizations (67 percent) have been confident in their IT infrastructure and providers, with only 22 percent shopping for new security solutions and services to address post-pandemic needs.[3]

Only 7 percent of small and medium-sized businesses (SMBs) made security purchases in response to the pandemic. This small percentage this might indicate one or more persistent problems: that SMBs lack visibility into their risk environments, the budget to support new investments, or both.[3]

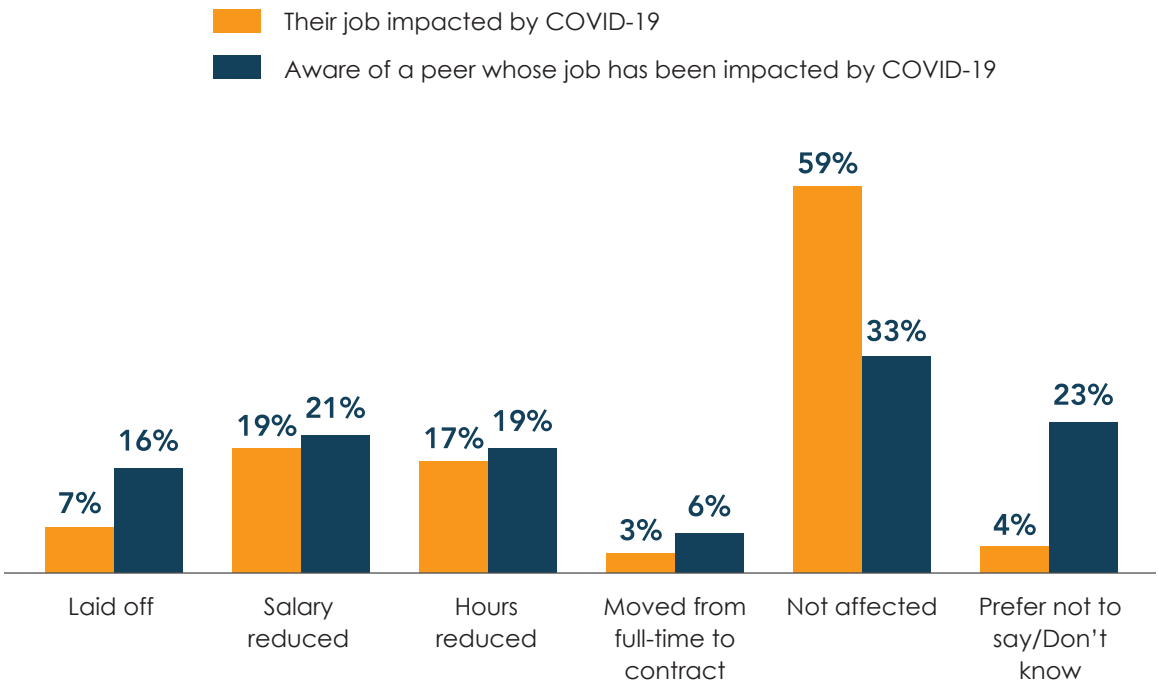
> Financial services and healthcare have been the least likely industries to invest in new technologies and services during COVID-19, because of their rigorous pre-pandemiccompliance and security requirements.[3]

Cybersecurity experts

Since the onset of COVID-19, the demand for cybersecurity experts has reached an all-time high. However, in a recent international survey by Robert Half, 32 percent of executives said locating cybersecurity experts with specialized knowledge and skills has still been incredibly challenging.[6]

Surprisingly, 700,000 new cybersecurity professionals joined the industry in 2020, a 25-percent increase from 2019. At first glance, one might think the cybersecurity skills gap is closing. After all, the skills shortage did drop from 4.07 million to 3.12 million. Unfortunately, the numbers are misleading. Revenue losses in 2020 led to layoffs, reduced hours, salary reductions, and full-time jobs demoted to contract-based roles. While fresh blood might have been pumped into the industry, COVID-19 forced many organizations to forfeit cybersecurity staff and stop recruiting altogether.[1]

COVID-19's Impact on Cybersecurity Jobs



(ISC)2 CYBERSECURITY WORKFORCE STUDY, 2020

44% of chief information and technology officers consider safeguarding company data and maintaining IT security their top priorities in 2021— over cutting costs, innovation, and process automation.[6]

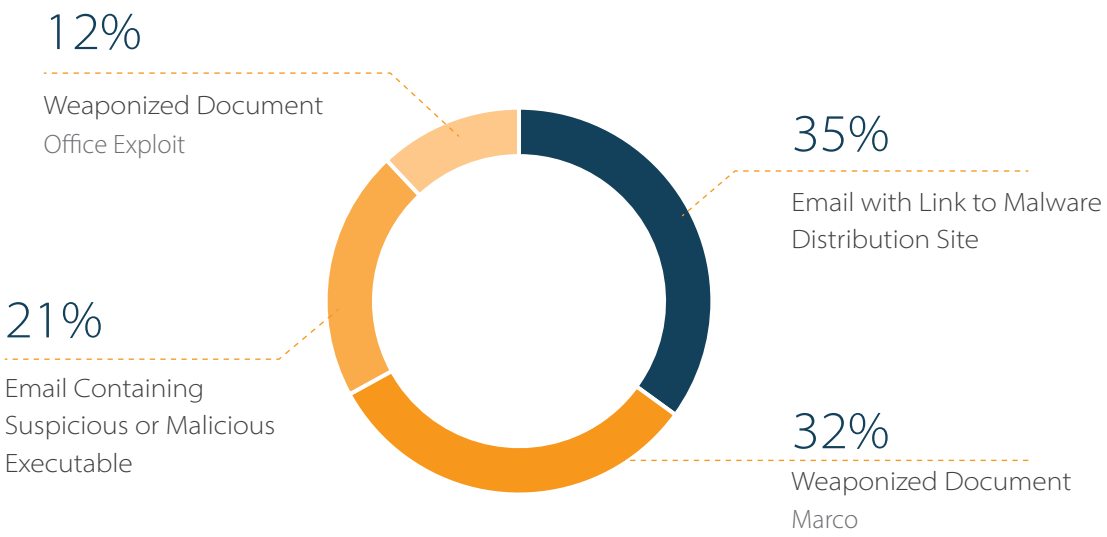
Malicious attacks

Cyber attacks skyrocketed during the first few months of the pandemic, with phishing and spear phishing as the most common attack methods. Interestingly, rather than rely on the tried and true, attackers introduced new attack methods during the pandemic. The overall result is a 75-percent increase in new attacks, which cannot be detected and mitigated by antivirus software alone.[8]

56% of survey respondents said cybersecurity staff shortages increase their organizations' security risk.[7]

Over the past year, Cynet detected an influx of spear phishing emails used to achieve initial system access. The breakdown is depicted in the graphic below.

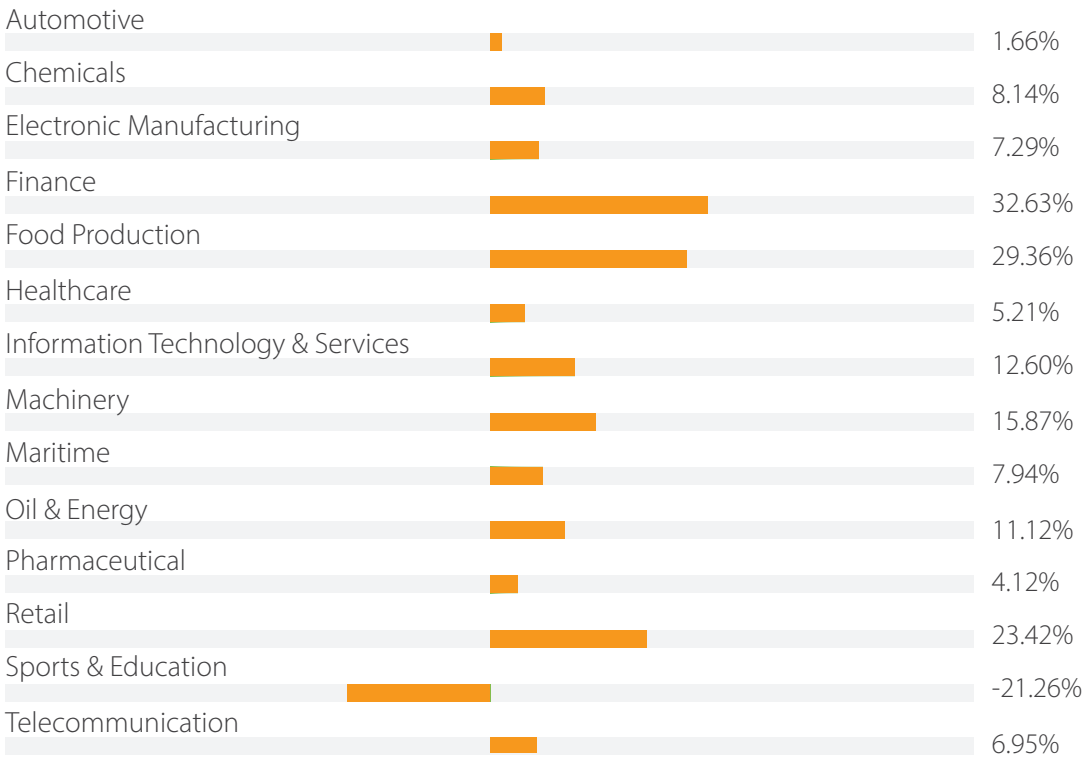
Email-Delivered Malware Distribution



Cynet COVID-19 Cyberattack Analysis, 2020

Enterprising attackers have taken advantage of confusion, stress, and vulnerable techologies and processes to target nearly every industry, with several experiencing an increase in attacks of over 20 percent.

Trends in Cyber Attack During COVID-19 (Industry)



Cynet COVID-19 Cyberattack Analysis, 2020

EMPLOYEES WORKING FROM HOME

PricewaterhouseCoopers' December 2020 remote work survey indicated remote work post-COVID has been an "overwhelming success for both employees and employers." 83 percent of employers stated that the shift to WFH has been successful, up from 73 percent in a similar survey conducted in June 2020.[9]

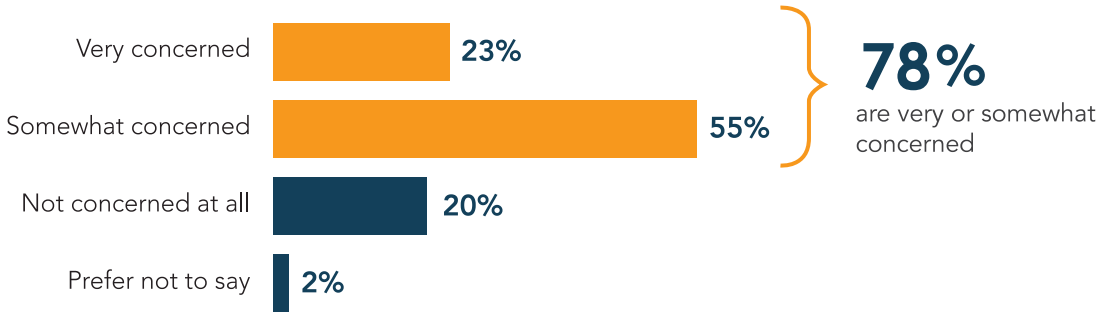
Given these positive results, it's hard to imagine remote work ending cold turkey. If productivity is up, and everyone is happier, we can expect this side effect to linger. In fact, fewer than one in five executives said they wanted to return to the office as if COVID-19 had never happened.[9] The trick for organizations and executives will be to strike the right balance between office work and WFH to preserve employee happiness and productivity while still fostering team collaboration and teamwork.

Cybersecrity experts have had to go into the office at times during the pandemic, though most (78 percent) are concerned for their safety. Most of those surveyed could not carry out the full scope of their duties remotely, either due to the nature of the organization itself or the remote working technologies available to them.[1]

Reasons Cybersecurity Experts Go to the Office

(ISC)2 CYBERSECURITY WORKFORCE STUDY, 2020

Cybersecurity Experts Worried About Their Safety in the Office



(ISC)2 CYBERSECURITY WORKFORCE STUDY, 2020

> High-tech firms had the highest proportion of remote employees prior to the pandemic's impact, at **31.9%**, and continue to have the highest today, at **90.2%**.[3]

THE SOLUTION

Cybersecurity measures

Given the large remote workforce (and the uncertain timeline for returning to the office), organizations should take a hard look at their remote and overall IT infrastructure to determine security gaps and vulnerabilities. Budget permitting, it would be prudent to enlist the help of cybersecurity professionals to perform vulnerability and penetration testing, an IT risk assessment, and/or a security controls review. Ensuring the correct technologies and processes are in place is crucial to maintaining a secure operating environment. Especially with growing remote infrastructure, policies around access management, for example, are key to deflecting malicious attacks.

Organizations should also consider moving to cloud environments, if they haven't already. Public cloud environments eliminate the need for staff to be on site to respond to an emergency or to roll out important security patches and updates. Cloud providers will be responsible for meeting customers' security requirements, such as those of financial institutions. As with any digital environment, businesses should engage professional consultants to assess the security of the cloud and its connected networks.

> **68%** of companies have between 5 and 10 technologies deployed to manage their security program. **20%** have 11 to 25 technologies.[5]

Talent

Skilled cybersecurity experts have been in short supply over the past decade. While there is no quick fix, organizations should prioritize the skills they truly need to obtain the most valuable, efficacious talent.

Top 5 cybersecurity skills your organization needs in 2021

Robert Half, How will COVID-19 shape demand for cyber-security skills in 2021?, 2020

01 **Information security**— Protecting data through authentication | authorization, malware analysis, incident response, risk management, and data recovery.

02 **Network security**— Securing wired and wireless networks and devices (e.g., firewalls, routers, switches), intrusion detection and prevention systems (IDPS), VPN and other remote access technologies, and endpoints.

03 **Cloud security**— Implementing security policies, procedures, controls, and technology specific to cloud-based systems, devices, and infrastructure.

04 **Web security**— Protecting websites and web applications, including operating systems and supporting infrastructure, from threats, such as viruses, ransomware, and DDoS attacks.

05 **Security architecture**— Includes knowledge of security hardware and software, cybersecurity risk management at the organization level, and analysis of business | IT needs.

> Employment in the U.S. must grow **41%** to meet cybersecurity staffing demand.[1]

Awareness

The human element in cybersecurity must be secured. No matter the technologies in place, if people aren't knowledgeable about cyber threats and their responsibility to defend against them, the risk of a security breach will remain high. Organizations should continuously train staff in cybersecurity hygiene and best practices, including how to deflect phishing and other common social attacks.

THE FUTURE

The effects of COVID-19 will endure long after the virus has been contained. On the bright side, the trial by fire made many organizations realize their IT security weaknesses and take the time to address them. On the other hand, budgets, staff, and morale have all suffered over the past year. Some hurdles, like the cybersecurity skills gap, will undoubtedly continue. To overcome this challenge, organizations must continue to prioritize security over other business needs, for the time being.

It may also be difficult for workers to transition back to the office after such a long stint away. Making IT security a top priority from the outset is critical, so staff do not forget important policies, procedures, and practices that keep company data safe.

More than anything, we must all focus on the lessons learned from this experience. Understanding cyber risks, their reach, and effects is critical to planning successful future initiatives. We may not be able to control the impact of COVID-19, but we can choose how we respond. Protecting people, technologies, and data from new and advanced threats is always the right investment.

> Across all vertical industries and company sizes, **73%** of organizations said they believe the impact of COVID-19 will alter how their business evaluates risk for at least the next five years. This figure was even higher— **83%**— in the retail sector.[3]

ABOUT SECURANCE

Securance has two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

SOURCES

1. https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B
2. https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets
3. https://www.csoonline.com/article/3535195/pandemic-impact-report-security-leaders-weigh-in.html
4. https://www.cisecurity.org/blog/resource-guide-for-cybersecurity-during-the-covid-19-pandemic/
5. https://www.carbonblack.com/wp-content/uploads/VMWCB-Report-GTR-Extended-Enterprise-Under-Threat-Global.pdf
6. https://www.roberthalf.co.uk/blog/hiring-and-management-advice/how-will-covid-19-shape-demand-cyber-security-skills-2021
7. https://www.infosecurity-magazine.com/news/fifth-uk-firms-planning-downsize/
8. https://go.cynet.com/covid-19-cyberattack-analysis
9. https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html

The Impact of COVID-19 on Cybersecurity

SECURANCE CONSULTING
Advantage of Insight AI

13916 Monroes Business Park, Suite 102, Tampa, FL 33635 • 877.578.0215
www.securanceconsulting.com