Whitepaper

icf.com

The Impact of COVID-19 on the Cybersecurity Sector

The COVID-19 pandemic has created an unprecedented push for businesses and employees to change the way we work and communicate. Companies are being forced to rapidly digitalize their business models, create flexible and remote working environments, reach clients, and manage employees predominately through digital channels. This creates opportunity for the cybersecurity sector to be responsive to the rapidly escalating increase in the quantity of cybersecurity attacks as well as an increasing number of businesses requiring cybersecurity services.

The demand for cybersecurity professionals already has outstripped the supply before the COVID-19 pandemic impacted our lives. In 2019, there was an estimated shortage of 500,000 cybersecurity professionals in the U.S. alone, with cybersecurity staffing shortages prevalent in nearly two-thirds of organizations.[1] Now, the gap is even wider, with an increasing demand for cybersecurity specifically in industries such as healthcare (including pharmaceuticals and biotech), banking, and insurance.[2] Also, the Cybersecurity and Infrastructure Agency (CISA) has named cybersecurity engineers, risk management analysts, and information technology specialists as essential staff to assess infrastructure viability and security needs due to COVID-19's onset.[3]

As a result of this crisis, there are new demands that will be required of cybersecurity professionals that will need to be addressed. However, based on our analysis, there are also opportunities and insights that will inform

[1] Lapena, R. (2020, February 10). *No relief for cybersecurity teams in sight, reveals Tripwire's latest skills gap report*. Tripwire. https://www.tripwire.com/state-of-security/featured/tripwires-skills-gap-report/

[2] Sweeny, C. (2020, March 27). *Cybersecurity skills in higher demand than usual due to COVID-19*. Wilson HCG. https://www.wilsonhcg.com/blog/cyber-security-skills-in-higher-demand

[3] T&D World (2020, March 21). CISA identifies critical workers amidst COVID-19 pandemic. https://www.tdworld.com/electric-utility-operations/article/21126748/cisa-identifies-critical-workers-amidst-covid19-pandemic

how the cybersecurity sector can adapt for the immediate future as well as for the long-term.

New Demands

A survey of existing cybersecurity professionals found that over 80% have witnessed a change in their day-to-day job responsibilities due to COVID-19. Nearly half have transitioned from traditional roles to assisting with other IT-related tasks, such as troubleshooting computer and networking problems, installing virtual private networks (VPNs), and manning helpdesks. This is likely to account for the increasing need for security services and networking for remote work environments. Additionally, nearly a quarter of cybersecurity professional surveyed reported that cybersecurity issues experienced by their organization have increased since transitioning to working remotely.[4] Our analysis finds that there are three major ways which COVID-19 is likely to impact the roles of cybersecurity professionals now and over the long-term.

Higher Frequency of Attacks	The type of security attacks has not changed. What has changed is their increased frequency, as well as has the number of businesses and employees who are susceptible. While employees who work remotely are safer from exposure to the coronavirus, they put themselves at higher risk of contracting virtual viruses, coming in csontact withmalware, phishing, and other security attacks by using personal internet networks and devices. As a result cybersecurity professionals are trying to put in place infrastructure so that organizations can adapt to the increasing security threats caused by remote working, including less secure networks, an increase in cyber criminals, and an increase in the number of ransomware attacks (e.g.,, attackers often claim to provide information or resources related to the coronavirus). Between January and March, 2020, spam has increased by over 25 percent, malware by 35 percent, and blocking of URL clicks by over 55 percent.[5] Additionally, impersonations are on the rise. Industries that have been hiring many employees due to COVID-19 – including retail and manufacturing – have recorded the highest increases in attacks. Also, the increasing use of video conference platforms to communicate between employees can also put companies at risk, since not all communication platforms are secure, and not all require that security functions (such as passwords and encryption) are enabled.

[4] Cision (2020, April 28). *ISC² survey finds cybersecurity professionals being repurposed during COVID-19 pandemic*. https://www.prnewswire.com/news-releases/isc-survey-finds-cybersecurity-professionals-being-repurposed-during-covid-19-pandemic-301048308.html

[5] Woollacott, E. (2020, May 5). *Cybersecurity and COVID-19: The first 100 days*. Forbes. https://www.forbes.com/sites/emmawoollacott/2020/05/05/exclusive-cybersecurity-and-covid-19the-first-100-days/#1f00f23839d5

Increased Number of Businesses Requiring Cybersecurity	According to Talent Trends, only two in five companies report they were mostly or fully digital prior to the COVID-19 outbreak. We have seen the impact of this rapid change with VPN use expanding by 66% at the end of March.[6] Cybersecurity professionals are and will continue needed to help businesses rapidly transition to remote working environments by establishing remote security tools, root access to machines, and networking capabilities. While some businesses may have already had these systems in place, many businesses – and especially small businesses – have yet to digitalize their business models. Where many businesses had previously leaned on physical and in-office security for protection of their data and information, the transition to remote work means that these companies can no longer rely on secure office computers, networks, internet, and security procedures. Instead, they must pivot to ensure that every employee working from home is doing so safely and data is being transferred securely whenever they logon. This could mean ensuring that employees are using safe networks and using VPNs, and that they are appropriately following security protocols. If employees are using personal computers or phones, businesses must also establish "bring-your-own-device" security procedures that are followed by staff. Companies need to ensure both that employees' data aren't being exposed to threats and that employees themselves aren't engaging in unsafe or malicious activities. This all may be challenging to companies who were not prepared to transition to digital business practices.
Increased Security Needs for Certain Industries	The healthcare sector are expected to see an increased demand for remote security. Due to COVID-19, individuals are looking to online platforms for medical information and services. While many healthcare organizations already have advanced internet-driven services, they are still more risk-prone, as attackers have been matching scams to the news and COVID-19-related misinformation, which especially targets these industries. These organizations are also dealing with much higher online traffic. Additionally, banks and insurance companies will be particularly impacted, as companies in these sectors tend to rely on older technology infrastructure that cannot physically be relocated or transferred online quickly. For instance, many insurance companies continue to run on mainframes, which require employees work in a physical office space.

[6] Mercer (2020). Win with empathy: Global talent trends 2020. Retrieved from: https://workingnation.com/covid-19-cybersecurity-and-it-workers-are-essential-in-demand-employees/

Essentially, companies and employees are facing steep learning curves and not much room to make mistakes, as these mistakes can result in serious security breaches. As an increasing number of businesses are looking to deploy remote technology use as fast as possible, cybersecurity professionals can facilitate these transitions while protecting systems and educating users on the importance of appropriately following security policies. We expect to see many of these demands and resulting changes continuing into the long-term. Businesses that establish remote working environments may end up discovering they benefit from shifting to a fully or partially remote workforce. It may also encourage a push for the consolidation and integration of security management and software defined networks, impacting the way companies function, connect to networks, and utilize technology in the long-term.[7]

In-Demand Skills for the Future

Despite these uncertain times, COVID-19 represents an ideal time for the cybersecurity sector to capitalize on the change to remote work and increased demand for cybersecurity services.

First, the push to remote work has shown that **networking is critical** for businesses who wish to work remotely. Software defined networking is cost effective and reliable, as people increasingly move their network away from physical infrastructure.[8] Those looking to enter the cybersecurity sector as a profession should be trained in network configuration, as it will increasingly be needed by a wider range of companies in the future.

Second, cybersecurity professionals will need to **learn to work remotely in team environments**. Security operations teams typically incorporate in-person meetings for teams to collaborate, problem solve, and perform remediation, such as by testing, conducting threat analyses, and deployment ofinnovative design thinking.[9] These processes are typically very collaborative because they require professionals to be innovative, brainstorm, troubleshoot, and problem-solve in a team setting. The switch to remote work requires that the cybersecurity sector itself adapt to provide better remote support tools and protections for its own professionals so that they can continue to innovate and work in realtime to find solutions to the current cybersecurity threats and deamands.

Third, COVID-19's impact requires that, more than ever, cybersecurity professionals have broader skills, and competencies including efficient and effective communication, patience, time management, agility, organization,

[7] Raywood, D. (2020, March 30). *The long-term impact of #COVID19 on the cybersecurity industry*. Infosecurity. https://www.infosecurity-magazine.com/news-features/long-impact-covid19-industry/
[8] E. Baer (personal communication, May 14, 2020).
[9] Homer, A. (2020, April 6). *5 critical issues cybersecurity teams face with COVID-19*. Security Infowatch. https://www.securityinfowatch.com/covid-19/article/21132855/5-critical-issues-cybersecurity-teams-face-with-covid19

and problem-solving. Existing cybersecurity professionals are being asked to pivot within their jobs to handle more IT-related issues, work one-on-one when p problems for employees, and adapt quickly as new threats arise. Both those who already work in cybersecurity and those who are considering entering the field must have the initiative, creativity, problem-solving know-how, and flexibility to adapt within their roles. They need to have patience and excellent communication skills when working with employees who will be experiencing challenges and frustrations in adapting to new work environments. They will need to have the skillset to clearly capture and document security processes so they are appropriately followed by all employees. More so, any individuals who are entering the cybersecurity field or are considering entering the field will need to acquire these skills while working and learning remotely.

Fourth, given the shortage of cybersecurity staff before COVID-19's onset, and the increasing demand for cybersecurity services because of it, it is important to get as many trained cybersecurity professionals into the field as possible.[10] This should include working with and conducting outreach with partners like educational institutions, registered apprenticeship programs, graduate talent programs, and high school pipeline programs to increase this critical labor pool and to efficiently develop, train, and help place entry-level professionals into cybersecurity positions. It may also include providing cross-training and up-skilling to existing IT professionals, so they have the skills and knowledge to pivot to cybersecurity roles.

Although COVID-19 has resulted in much uncertainty and changing work environments, the pandemic has provided an opportunity for the cybersecurity sector to adapt and innovate to meet the rapidly increasing demand for digital services. It also presents an ideal time to attract new talent to the sector. Now and in the future, well trained cybersecurity professionals are needed to assist a growing number of businesses who depend on these individuals to protect their data, information, and employees during these uncertain times.

[10] Sweeny, C. (2020, March 27). *Cybersecurity skills in higher demand than usual due to COVID-19*. Wilson HCG. https://www.wilsonhcg.com/blog/cyber-security-skills-in-higher-demand

About CYAI

CYAI is funded by the U.S. Department of Labor's (DOL) Employment and Training Administration (ETA) Office of Apprenticeship (OA). CYAI promotes sustainable development of cybersecurity apprenticeship programs for youth aged 16–21 and is administered by ICF. The goal of the initiative is to create at least 900 new cybersecurity apprenticeships for youth by 2024.

About ICF

ICF (NASDAQ:ICFI) is a global consulting services company with over 7,000 full- and part-time employees, but we are not your typical consultants. At ICF, business analysts and policy specialists work together with digital strategists, data scientists, workforce professionals, cybersecurity experts and creatives. We combine unmatched industry expertise with cutting-edge engagement capabilities to help organizations solve their most complex challenges. Since 1969, public and private sector clients have worked with ICF to navigate change and shape the future. Learn more at www.icf.com.

Author

Ms. Deppa has five years of experience integrating evidence-based evaluations within the social services field. At ICF, Ms. Deppa frequently uses her skills in qualitative and quantitative evaluation and writing to inform projects related to workforce development, career pathways, and social protection. She was previously a Fulbright Scholar in Turkey and holds a Master of Science from the London School of Economics.

Mark Ouellette is the Director for Workforce Innovations and Commercial Markets at ICF and has more than 20 years of experience designing, improving, and evaluating the effectiveness of workforce training programs. For the past 11 years, Mr. Ouellette has designed and implemented the California Advanced Lighting Controls Training Program (CALCTP), which has trained more than 8,500 electricians and 950 electrical contractors in advanced lighting. Mr. Ouellette developed a Southern California Regional Apprenticeship Strategy and supporting the expansion of registered apprenticeship programs for youth. Mr. Ouellette is leading up an initiative to expand the number of young people enrolled in a cybersecurity registered apprenticeship program.