TELEWORK AND INCREASED CYBERSECURITY RISKS

Tony Wang, CISA, CIA, CISSP, PMP
Partner

Cybersecurity is now a critical business focus and having cybersecurity experts to detect weak controls and avoid a security incident is a necessity. This has never been more evident since the beginning of 2020. Since the beginning of 2020, the deadly COVID-19 virus has affected the world and has claimed millions of lives. COVID-19 has changed the way people live and operate their businesses, as many organizations have transitioned to full-time remote work. As of March 2020, an estimated 16 million U.S. knowledge workers have started working from home [1]. Due to the change in their work environment, a recent study shows that 80% of companies experienced an increase in cybersecurity risk [2]. This has posed a challenge during the COVID-19 pandemic, particularly in times of heightened stress. Cybercrime has also increased by 63%, typically caused by human errors from phishing attacks, social engineering, and failure to follow system security protocols and policies since the start of the pandemic [2]. The increased risk and crime rates are because cybersecurity was considered an afterthought within many industrial environments. More importantly, the basics of cybersecurity are still not being practiced regularly, leading to employees not practicing their security awareness protocol when performing their job duties at home.

The transition to remote work and lack of security awareness has further resulted in multiple security incidents. Statistics show that 80% of data breaches have occurred either because of brute-force attacks or stolen credentials, including a notable surge in business email compromise [3]. The level of security from the home environment is not as effective as in an office environment due to the lack of additional layers of securities that each organization offers. Also, security measures such as the limitation of personal device use, security patches, timely encryption of passwords, firewalls, and regular software upgrades are not as readily available in a remote work environment. Coalition, Inc, a cyber risk and security management company, stated that they observed a 67% increase in email attacks during the pandemic [4]. Nearly 16 billion records have been exposed to hackers, which is a 273% increase in comparison to 2019 [3].

One of the most significant cybersecurity incidents in 2020 was the security breach of Garmin, a GPS and fitness wearables company. Hackers deployed WastedLocker, a ransomware tool used to deactivate every operating program through encryption of internal systems to prevent customers from accessing online services. The hackers then demanded a fee for the decryption key, and Garmin was believed to pay the $10 million ransom.

[1] https://slackhq.com/report-remote-work-during-coronavirus
[2] https://www.securitymagazine.com/articles/93885-human-error-poses-cybersecurity-challenges-for-80-of-businesses-during-the-covid-19-pandemic
[3] https://www.gmi-insurance.com/post/the-biggest-data-breaches-of-2020
[4] https://www.securitymagazine.com/articles/93322-cybersecurity-claims-trends-amid-covid-19

Although not confirmed, it was believed that EvilCorp, a Russian hacking group, carried out the ransomware attack by breaking into the server through a phishing email sent to one of Garmin's employees [5]. WastedLocker contains a silent bypass feature for security measures such as User Account Control (UAC) on Windows machines, which is used to prevent malicious privilege escalation. The ransomware is able to silently elevate its privileges without displaying the UAC prompt [6]. Without the added security measures that are available in an office environment, it becomes easier for hackers to carry out such phishing attacks. Another significant cybersecurity incident in 2020 was the security breach of the Department of Defense (DoD). The DoD Chief Information Officer stated that 37 network attack cases had been reported as more employees started teleworking. The organization's network experienced a surge of cyberattacks during a virtual town hall meeting [7].

There are many uncertainties regarding the return to normalcy in 2021. However, cybersecurity will still be a concern for all organizations. The work from home trend will continue to define the threat landscape, and endpoints will become the attack vector of choice. The cybersecurity budget in 2021 will climb higher than pre-pandemic limits. Authentication, cloud data protection, and application monitoring will top the list of Chief Information Security Officer budget and cybersecurity priorities [8]. Due to the importance of organizations' security training programs, Williams Adley can provide assessments of organizations' overall security awareness and role-based training programs to ensure that agencies assess the skills, knowledge, and abilities of their workforce to identify any knowledge and/or skill gaps. In addition to training program assessments, Williams Adley can provide cybersecurity risk assessment and management services to help improve organizations' overall information security posture.

[5] https://terranovasecurity.com/garmin-security-breach/
[6] https://threatpost.com/garmin-pays-evil-corp-ransomware-attack-reports/157971/
[7] https://defensesystems.com/articles/2020/03/18/dod-telework-cyber-attacks.aspx
[8] https://threatpost.com/2021-cybersecurity-trends/162629/