SecureSource©
INTERNATIONAL
Wednesday, 20 May 2020

TOP LINE

Working from home has become commonplace amid the ongoing pandemic, untethering many workers from corporate headquarters and office environments. Other members of the workforce are facing pay cuts, furloughs, and layoffs as industrial and manufacturing sectors continue to be hit hard by pandemic related shutdowns. These realities form a confluence of factors which heighten the risk of cybercrime and corporate espionage in unique ways. Security profiles typically exist in two realms: the physical and cyber. With so much of the global workforce at home, the lines between the realms are blurring and many companies are scrambling to catch up.

Technology acts as enabler for state or private actors interested determined to hack into corporate or home networks. Remote work has transformed many of these networks into one and the same. Additionally, the proliferation of hacking tools, mobile devices, and digital data has made it easier for clueless or disgruntled executives and employees to enable the exfiltration of sensitive data. Protections built into corporate computer networks are often lacking at home, making cyber security training and individual cyber-hygiene all the more important. For example, corporate in office computers may have USB entry or download sensors lacking in more portable laptops or tablets. At home internet connections often have limited security and fraud detection built into them compared to more robust corporate networks. Social engineering attacks may target other members of a worker's household to gain access to a corporate network.

Amidst the current economic downturn, cuts to corporate security measures may seem like a straightforward way to save money. Guards, access control systems and devices, cameras, sensors, and alarms are expensive. However, cutting security capabilities makes businesses more vulnerable to the exfiltration of proprietary data through remote attack or insider access. Meanwhile, rising numbers of furloughed and unemployed workers heighten their vulnerability to an approach by a state or private actor interested in intellectual property or proprietary information. Fraudulent remote work opportunities for financial remuneration may ensnare a financially overleveraged worker not otherwise disposed to sharing sensitive data without appropriate due diligence.

Business leaders must understand gaps in their physical and cyber infrastructure regardless of where it is deployed so as to bolster the security of connections, monitor for abnormalities, and deploy strong incident response programs to ensure business continuity. Workforces across industries should be trained in cyber security regardless of their level due to the crosscutting nature of network access. Cyber defenses should protect against remote attacks and insider threats alike and may need to be rebuilt to account for the prevalence of portable devices, which may not typically be allowed in certain security environments.

Questions to Consider:

What policies and procedures does your company have in place to protect against remote hacking or insider threat scenarios? What additional functions do you need to prevent the exfiltration of proprietary data? What physical security measures have you put in place to safeguard key personnel subject to possible surveillance and the threat of violent crime?

COVID-19: THE HIGHLIGHTS

Research suggests extended trajectories for COVID-19 outbreaks across the globe, with some recent modeling suggesting the virus could continue to spread through temperate regions through 2025. Amidst this backdrop, the race for a vaccine has escalated even as the U.S. has threatened to pull funding from the World Health Organization over its early handling of the outbreak in China. Federal warnings of coordinated unemployment fraud and Chinese targeting of research organizations focused on COVID-19 have escalated. These warnings highlight how the intense focus on COVID-19 has permeated our physical and cyber worlds alike, emphasizing the importance of protecting against vulnerabilities and bolstering the security of our interconnected lives.

BEYOND THE NOISE

Cyber risk: Remote work is creating unique cyber vulnerabilities in organizations' infrastructure and blurring the lines between physical and cyber infrastructure. Businesses must view their risk profiles through a lens which integrates physical and cyber security. Additionally, understanding the new cyber risks and establishing appropriate baseline defenses is essential to reducing the consequences of cyberattacks. The majority of breaches come through access to a privileged account. Many external breaches come through hacks or phishing scams while internal breaches are more likely to come from employees anticipating their exit. As such, protecting privileged access credentials is critical to the security of physical and cyber infrastructure.

- Secure infrastructure: Establish or bolster systems that protect against insider threats and remote attacks; monitor for abnormalities and protect against unauthorized exfiltration of data. Implement processes and procedures to destroy strong incident response programs to ensure business continuity. Protect against the compromise of privileged access credentials by controlling on site and remote access.

Cyber crime: Cyber crime has accelerated amidst the COVID-19 pandemic, with retail and manufacturing companies being particularly hard hit. The attacks seek to capitalize on insufficiently robust verification processes and remote workforces which have not been provided with consistent cyber security awareness training. Home networks hosting a multitude of devices that are not updated as consistently as corporate systems are particularly vulnerable to hacking or malware attacks.

- Secure access: Implement cyber security awareness training for every member of a workforce, regardless of their level. Encourage consistent security and software updates on personal and work devices. Establish procedures to limit data permitted outside of firewalled or password protected digital environments.

TRUSTED RESOURCES: for numbers & guidance

Johns Hopkins University – Coronavirus Resource Center

World Health Organization – COVID-19 Pandemic

Center for Disease Control – Coronavirus (COVID-19)

Please contact Secure Source International at info@securesource.com to schedule a leadership roundtable with our intelligence and security experts to dive into these topics and discuss security and safety related best-practices.