BKS
PARTNERS
INSIGHT BEYOND INSURANCE

CYBER READINESS GUIDE:
COVID-19

Employers across the country are moving employees to a virtual work environment in response to the COVID-19 pandemic. This massive and sudden shift opens many doors for cyber-criminals and exacerbates certain cyber risks that need to be swiftly addressed to protect organizations' balance sheets. It's crucial to consider the following telecommuting-related cyber threats and best practices to reduce the risk of cyber breaches amid the coronavirus pandemic.

Telecommuting Cyber Risks:

Access Points

- Similar to a burglar gaining a better probability of entering a building if it has more doors and windows, a cyber-criminal is more likely to gain entry to a company's system when employees and vendors are using many different personal wireless networks and/or devices at their homes. Multiple points of entry expose Personally Identifiable Information (PII) and Protected Health Information (PHI) of employees.

Social Engineering/Phishing

- Malicious actors are capitalizing on increased distraction and leveraging a sense of urgency to carry out coronavirus-themed cyber attacks. Tactics include charitable donations to affected individuals, links to conduct surveys, and requests to update passwords from sketchy sites.
- Frequently, a cyber-criminal will gain access to a company network and lie dormant while learning the intricacies of communication specific to that organization and their employees. When the time is right, they will strike by impersonating an executive or manager and convince the employee to wire company funds to a phony bank account.

Unsecured Networks

- Employees may decide to work at a local coffee shop or other public venues to take advantage of the free WIFI. However, due to financial constraints, most local coffee shops and public places do not have the same level of network security as more substantial businesses, making it easier for that network to be compromised and breached.

Capacity Challenges and Issues

- Due to an influx of IT help requests related to telecommuting, IT departments may have less availability to monitor the company network. For many employees, this is the first time working from home for an extended period of time. Also, with a sudden surge of work from home employees, systems and applications may face outages, slowdowns, and capacity issues.

Organizational Best Practices:

- Test remote access systems regularly. Ideally, host a trial day where everyone works from home to identify potential issues and fix them before the mandatory telecommuting period begins.
- Route access to company or client networks, shared drives, and sensitive corporate information through a Virtual Private Network (VPN). A VPN encrypts the internet traffic between a remote device and company or client networks, allowing for a more secure connection.
- Patch, update, and monitor the VPN regularly.
- Configure the VPN with multi-factor authentication as an added security layer to ensure that only authorized individuals can access the company network.
- Update company policies and communication to address working on a private network (not on public WIFI) and keeping work-related phone calls private.

- Address storage and destruction of confidential information in company policies.
- Educate employees on general and COVID-19 specific phishing scams. Then train employees on how to spot phishing attacks and test their ability to do so. Running simulated campaigns throughout the year will help keep employees engaged in their ability to detect a phishing attack and how to avoid them.
- Consider employing an electronic password management/vault service.
- Review incident response plans to ensure they contemplate a remote working environment and an IT staff that will likely be stretched thin.
- Ensure executives know their roles when an incident occurs, including the specific events or circumstances that require escalation.
- Utilize sophisticated endpoint detection and response (EDR) software to quarantine any compromised remote workstations and limit a cyber criminal's ability to navigate the network.
- Review your current cyber insurance policy to assess limit and coverage adequacy related to the increased cyber risks borne by a remote working environment.

Best Practices for Employees:

- Only correspond through company email or other company-approved communication apps while working remotely. Likewise, avoid personal computers for work-related duties.
- Don't rely on personal cloud storage apps or personal email accounts for saving, accessing, or distributing company documents and information.
- Understand what constitutes sensitive data within the organization. Sensitive data may include intellectual property, customer lists, confidential customer information, as well as sensitive employee information, etc.
- Scrutinize emails and text messages containing links. One strategy to accomplish this is to hover over the link to view the IP address before clicking.
- Use longer, more complex passwords, and avoid passwords that include known facts, such as a birthday or address.
- Immediately alert management or IT of a suspected breach or successful cyber-attack.

By now, it's widely known that the COVID-19 pandemic continues to affect working environments and essential business operations. The new reality for many organizations involves a remote workforce that brings new and increased cyber risks. Staying up to date on the relevant cyber threats and adhering to best practices to reduce risk will lead to peace of mind during uncertain times.

BKS-PARTNERS | INSIGHT BEYOND INSURANCE

BKS-Partners is an award-winning entrepreneur-led and inspired insurance brokerage firm delivering expertly crafted Commercial Insurance and Risk Management, Private Insurance and Risk Management, Employee Benefits and Benefit Administration, Asset and Income Protection, and Risk Mitigation strategies to clients wherever their passions and businesses take them throughout the U.S. and abroad. BKS-Partners has award-winning industry expertise, colleagues, competencies, insurers, and most importantly, a highly differentiated culture that our clients consider an invaluable expansion of their business. Learn more about BKS-Partners at ***www.bks-partners.com***.