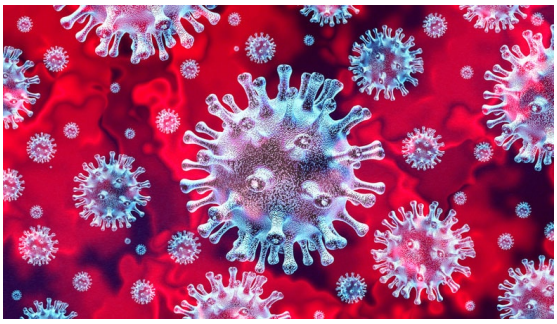
BLOG

Securing the Remote Workforce in the Wake of the COVID-19 Global Health Crisis

Apr 22, 2020



As anticipated at the onset of the COVID-19 pandemic the industry has seen a significant uptick in cyber fraud in the last month and a half. The FBI recently cited an average number of 3,000 to 4,000 daily complaints about online scams compared to approximately 1,000 prior to COVID-19.

Cyber criminals are opportunistic and taking advantage of companies at their most vulnerable. This is a result of the following unique risk factors that have been heightened with the rapid shift to remote working arrangements:

- Resources from Operations & Information Security diverted elsewhere.
- Employees are using technology that they are less familiar with and there is a greater potential for unintentional errors.
- Employees are using personal devices that are less secure and potentially already compromised to connect with company systems and applications.
- Increased reliance on technology and outsourced IT vendors in particular.
- Less of a focus on everyday corporate initiatives including Cyber Security due to a shift in organizational priorities.
- Disconnected workforce makes it challenging to follow established risk management protocols.
- Employees have distractions in their home environment that they do not have on premises.

The threat actors are primarily exploiting these vulnerabilities using phishing emails preying on the fears and curiosity around COVID-19. Examples of these emails include messages doctored to look like a company's purchase order for supplies like face masks, Clorox wipes, and hand sanitizer messages manipulated to look like updates from governmental organizations like the World Health Organization.

In order to mitigate these threats we are recommending the following steps to protect your organization.

- Update information security policies and acceptable use policies to address telecommuting arrangements.
- Conduct due diligence on COVID-19 implications and the business continuity plan of key vendors providing IT services.
- Ensure that the incident response plan and reporting procedures are updated to address remote working realities.
- While employees are being inundated with communication it is more important now than ever to

reinforce security awareness training by deploying training modules, sending bulletins about COVID-19 phishing campaigns, and conducting phishing simulations.
- Enable mutli-factor authentication for all employees.
- Ensure all employees are using secure Wi-Fi networks and accessing company servers via a Virtual Private Network.
- Reinforce company policy that corporate files should only be saved on the company network and not locally on company issued devices or personal devices.
- Encourage all employees to mute or shut down in home smart devices.

There are also a number of potential insurance coverage implications and long term market ramifications that we are closely monitoring.

- Does your insurance policy have any exclusionary language that would preclude coverage for claims arising out of unencrypted devices or from employees using their own personal devices? This language should be avoided and negotiated out of Cyber policies.
- Does your policy include Contingent Network Interruption Coverage and System Failure Network Interruption coverage? These are important coverage elements given the increased reliance on outsourced IT service providers and the strain on key systems and infrastructure.
- Are current limits adequate given this dramatic shift to remote working?
- Given the potential for increased claims activity and overall hardening of the insurance marketplace it is likely that there will be increased scrutiny on renewal on the following issues:
    - Information Security budgets maintained in spite of any financial hardship.
    - Use of multi-factor authentication widely deployed.
    - Increased employee training and phishing simulations.
    - Updates to information security policies to address telecommuting and use of personal devices.

Below you will find a webinar we recently hosted on Securing the Remote Workforce. To see full slides click here.

TAGS:
Cyber Liability