RISK INSIGHTS

IRIDIUM RISK SERVICES EVOLVED

NAVACORD®

www.irsnavacord.com | March 2020

Cyber Risk Implications of the Coronavirus Outbreak

The outbreak of COVID-19 has caused significant disruption to business and triggered the largest 'work-from-home' mobilization in recent decades. It's a new reality for many and it is putting even the strongest IT and Business Continuity teams to the test.

Of course, while everyone works to ensure key business functions remain operational and employees and families everywhere are safe, there is another set of individuals working just as hard to disrupt our efforts: *cyber criminals*.

The COVID-19 pandemic has provided the perfect cover and distraction for cyber criminals to attack your business and potentially force grave errors—which could cost your business millions.

Creating a culture of information and preparedness around cyber security is critical to protecting your business. We recommend that companies take the following precautions to help ensure their networks, data, and finances are protected:

1. TEST LOG IN AND ENDPOINT CAPABILITIES

All personal and business devices should be configured for secure remote working. This includes implementing a multi-factor authentication (MFA). MFA is an authentication process that requires more than just a password to protect an email account or digital identity, and is used to ensure that a person is who they say they are by requiring a minimum of two pieces of unique data to corroborate their identity. MFA significantly reduces the chances of a successful cyber attack.

A remote workforce makes it more difficult for IT staff to monitor and contain threats to network security. To further protect networks, businesses can implement endpoint detection and response (EDR) software that can be used to quarantine workstations remotely and limit the potential for malicious actors to move through their network.

2. PREPARE FOR DISRUPTION

Prepare for the worst. A remote workforce can make it more challenging for IT staff to monitor and contains threats to network security. In the event that a cyber attack occurs in your company, it is important to have an incident response plan in place. If you believe an employee has fallen victim to a cyber event or a cyber criminal, notify the head of your IT department, Finance, and your Insurance Advisor as soon as possible.

3. EDUCATE YOUR EMPLOYEES ON THE RISKS OF CYBER SOCIAL ENGINEERING

The biggest information security risk within a business is human error, and with so many employees working outside of their normal environments (at home, offsite, using Remote Desktop Applications, away from their regular teams or departments, etc.), they are notably distracted—and cyber criminals are taking advantage. **Education surrounding the risks of cyber social engineering is key.**

Ensure your employees understand and are on the look-out for:

Phishing/Vishing/Smishing

These attacks are attempts made through email (phishing), voice calls (vishing) or SMS (smishing) by a cyber criminal to obtain sensitive information. The fraudster sends phony emails or messages that appear to come from valid sources in an attempt to trick users into revealing personal or business financial information, or into installing malware or malicious macros.

For instance, the Sophos Security Team has spotted emails impersonating the World Health Organization (WHO). These emails ask victims to download a document called "Safety Measures", and then users are asked to verify their email by entering their credentials, redirecting those who fall for the scam to the legitimate WHO page, and delivering their credentials straight to the phisher.

Fraudulent Online Websites

Interpol has warned of a large increase in fraudulent websites claiming to sell masks, medical supplies and other high demand items that simply take money from victims and never deliver the promised goods. It is advisable that Internet users purchase items only from established and reputable sources.

Impersonation and Malware

There have been reports of airlines and travel companies being impersonated by fraudsters in a bid to either obtain sensitive information, like passport numbers, or install malware on victims' computers. They may say they want to advise you of COVID-19 infected passengers on past flights you've taken or offer discounts on future flights. When in doubt, we advise users to be vigilant when clicking on any links, delete any suspicious emails, and not disclose sensitive information if you are approached unexpectedly.

Fake Charities

Fraudsters are also developing fake charitable donation campaigns which claim to help individuals and communities impacted by the Coronavirus. Any money donated is sent to fraudulent accounts. Therefore, if you are wanting to support relief efforts, make sure to research the organizations you are looking to donate to.

Malware Downloads

A Twitter user has identified another malware campaign purporting to be a "Coronavirus Update: China Operations". The emails have attachments linking to malicious software.

Spear Phishing

Similar to phishing, this is a targeted and customized attack on a specific company or employee—usually directed to an individual who would have specific access to confidential information or controls, potentially within Finance or IT.

Watering Holes

This occurs when the attacker studies a specific group of users from a company and infects websites that members of the group are commonly known to visit. By infecting one user's computer, the cyber criminal can gain access to the network.

4. EXTERNAL RESOURCES

For further reading, please click on the links below:

- ***"Hackers target companies with Coronavirus Scams"*** *(Wall Street Journal)*
- ***"Coronavirus Used in Malicious Campaigns"*** *(TrendMicro)*
- ***"Cyber Experts step in as criminals seek to exploit Coronavirus fears"*** *(National Cyber Security Centre)*
- ***"Will Coronavirus Lead to more cyber attacks?"*** *(Harvard Business Review)*
- ***"Now meet the cyber threat in the name of Coronavirus"*** *(Cyber Security Insiders)*
- ***"Poll on Attacks once working from Home"*** *(Threat Post)*
- ***"Prepare now for the second wave of Coronavirus hacking"*** *(The Hill)*
- ***"Client advisory: Cybercriminals exploiting Coronavirus"*** *(CFC Underwriting)*

If you have questions specific to your business, or would like additional information, please reach out to your Iridium Advisor.

LET US HELP YOU MANAGE YOUR RISK

1100, Bow Valley Square 3
255 - Fifth Avenue SW
Calgary, AB T2P 3G6
855.585.9654

www.irsnavacord.com
www.navacord.com
info@irsnavacord.com

2020_03_COVID