RISK INSIGHTS

LloydSadd INSURANCE BROKERS

NAVACORD®

www.lloydsadd.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 you millions.

Creating a culture of information and cyber security is now 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 his/her 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. 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.

  Watch for:
  - Spoofs of email addresses
  - Compressed attachments
  - Impersonalized messages
  - Spelling or grammar errors
  - Scare tactics and overly tight deadlines
  - Imitations of known brands

- 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.

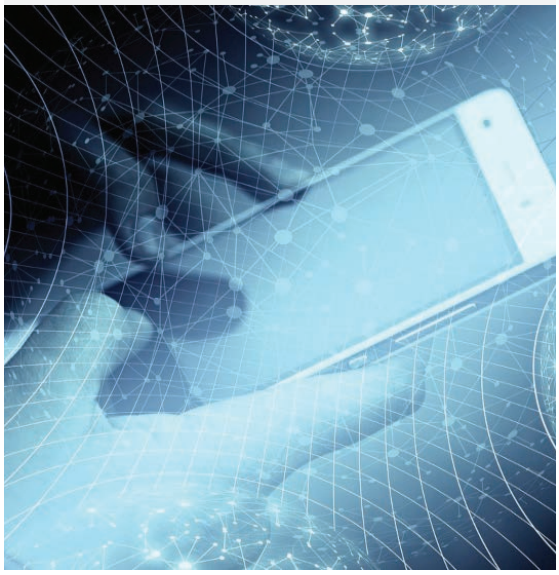
- Watering Holes:

  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.

3. PREPARE FOR DISRUPTION

Prepare for the worst. A remote workforce can make it more challenging for IT staff to monitor and contain 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 cyber criminal, notify the head of your IT department, Finance, and your Insurance Advisor as soon as possible.

It's a new reality for many and it is putting even the strongest IT and Business Continuity teams to the test.



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

LET US HELP YOU MANAGE YOUR RISK

Suite 700, 10240 – 124 Street,
Edmonton, Alberta T5N 3W6
1-800-665-5243

lloydsadd.com
navacord.com
info@lloydsadd.com

2020_03_COVID

Local Touch. National Strength.™