Cyber Risk Implications of the Coronavirus Outbreak

Concern about the spread of the coronavirus has triggered the largest "work-from-home" mobilization in history. In this risk alert, Aon outlines the practical steps organizations can take to remain cyber resilient amid the crisis.

The outbreak of COVID-19 has caused significant disruption to businesses and a degree of panic within the employee community. Companies across Canada have activated contingency and business continuity plans and have allowed or instructed employees to work from home to limit the spread of the virus. In a new reality where millions of people are working remotely, secure networks are now more critical than ever. To remain operational and secure, Aon recommends that companies take the following steps:

- **Defend against the phishing wave**
  Malicious actors will leverage the intense focus placed on the virus and the fear and panic it creates. Security researchers have already observed phishing emails posing as alerts regarding COVID-19. These emails will typically contain attachments which purport to offer information about the outbreak or updates on how recipients may stay safe. In an environment where people are stressed and hungry for more information, there is a lack of commitment to security best practices.

  This is the time for organizations to remind employees of the need for vigilance and the dangers of opening attachments and links from untrusted sources. Running a simulated spear phishing campaign can also demonstrate the level of resilience to these attacks. At a more technical level, up-to-date antivirus and monitoring tools can limit the effectiveness of successful spear phishing attacks.

- **Test system preparedness**
  Organizations will be experiencing an unprecedent amount of traffic accessing the network remotely. Companies with an agile workforce have been preparing for this contingency for some time and will be well-equipped to maintain network integrity through the use of sophisticated virtual private networks (VPNs) and multi-factor authentication. Enterprise security teams are recommended to increase monitoring for attacker activities deriving from work-from-home users, as employees' personal computers are a weak point that attackers will leverage in order to gain access to corporate resources.

  For those less prepared, COVID-19 presents a challenge. There is a risk that the increased volume of network traffic will place a strain on IT systems and personnel and that employees will be accessing sensitive data and systems via unsecure networks or devices. We recommend that these organizations migrate as quickly as possible to remote working and bring-your-own-device (BYOD) standards. VPNs should be patched regularly (for example, a vulnerability in the Pulse Secure VPN was patched in April 2019 but companies which failed to update were falling victim to ransomware in December) and networks should be load-tested to ensure that the increased traffic can be handled.

- **Brace for disruption**
  A remote workforce can make it more difficult for IT staff to monitor and contain threats to network security. In an office environment, when a threat is detected, IT can immediately quarantine the device, disconnecting the endpoint (i.e. the compromised computer) from the corporate network while conducting investigations. Where users are working remotely, organizations should ensure that, to the extent possible, IT and security colleagues are readily contactable and ideally able to physically address a compromise at its source. Sophisticated endpoint detection and response (EDR) software can also be used to quarantine workstations remotely, limiting the potential for malicious actors to move through the network.

  As this risk moves beyond the technical, companies should adopt an enterprise risk approach. This can include rehearsing business continuity plans (BCP) and senior management response through tabletop crisis simulations that focus on cyber scenarios as well as how pandemics and other similarly disruptive events are likely to impact upon automation, connectivity and cyber resilience.

  Companies can also safeguard against the increased risk of disruption through a robust cyber insurance policy which, in the event of a digital disruption to systems, can provide cover for business interruption losses, as well as the costs of engaging forensic experts to investigate and remediate a breach.

COVID-19 presents a range of challenges to businesses across Canada but developments in technology since the SARS outbreak means companies can remain operational and nimble in the face of uncertainty. Keeping one eye on the pervasive cyber threat in the midst of this crisis is critical to ensuring ongoing success.

Empower Results®