AIRD BERLIS

SPOTLIGHT
MEDIA, SPORTS AND COMMUNICATIONS LAW BLOG

Mar 27, 2020

Cyberattacks and Cybersecurity Measures Amid the COVID-19 Pandemic

By Paige Backman and David Mba

As the COVID-19 pandemic continues, cyber criminals are finding ways to capitalize on the growing levels of concern and fear accompanying the pandemic.

We refer to our **blog posted March 26, 2020,**for additional practical ways to watch for and respond to potential cyberattacks and social engineering efforts. Below we continue to provide information we feel will be helpful in navigating the cyber threats in these unusual times.

In recent weeks, the Canadian Anti-Fraud Centre (CAFC) has issued a bulletin alert regarding the increase in COVID-19 related fraudulent scams, and cybersecurity researchers have found that the use of "coronavirus" and "COVID-19" in domain names, potentially unwanted email messages, and phishing and malware delivery schemes has skyrocketed. The Canadian Centre for Cyber Security (the "Cyber Centre") also recently issued an alert to Canadian health organizations warning of an elevated risk of cyberattacks to health organizations working in response to the pandemic. However, while the alert highlights risks to the medical and health communities in Canada, the advice and guidance issued was also directed to other Canadian businesses, particularly those with employees teleworking through VPNs.

Unfortunately, with numerous businesses transitioning to working remotely during the pandemic, and amid this increase in cybercriminal activities, the likelihood of cyberattacks and losses for businesses is high.

Given these heightened risks, it is more important now for companies to inform themselves of the cyber threats their organizations face, and to take adequate steps to protect themselves and their employees.

Scope of the COVID-19 cyber threats

According to the cybersecurity firm, Sophos, the raw number of domain names being registered that are related to the COVID-19 pandemic has grown rapidly over the past few weeks. On March 20, in the four largest top-level domains monitored (.com, .us. .org, and .info), ,people registered 3,011 new domains that contained the text "covid" or "corona." Since February 8, they observed 42,578 (as of midnight, March 24) newly-registered covid or corona domain names. While some of these domains may have been registered for benign or even beneficial purposes, many are being registered as part of spamming and phishing schemes.

Correlating with the increase in COVID-19 related domain name registrations is the number of phishing attempts referencing the virus. These attacks typically occur through spoofs of government, healthcare or research information, emails or websites that disseminate malicious links containing malware or ransomware.

The CAFC recently updated its list of known COVID-19 related scams to capture some of these spoofs, which now include the following:

- Cleaning or heating companies offering duct cleaning services or filters to protect from COVID-19
- Center for Disease Control and Prevention (CDC) or the World Health Organization (WHO) offering fake lists for sale of COVID-19 infected people in your neighborhood
- Public Health Agency of Canada providing false results claiming you have tested positive for COVID-19, tricking you into confirming your health card and credit card numbers for a prescription

- Red Cross and other known charities offering free medical products (e.g. masks) for a donation
- Government departments sending out coronavirus-themed phishing emails tricking you into opening malicious attachments and revealing sensitive personal and financial details
- Private companies offering fake COVID-19 tests for sale

In addition, the Cyber Centre has also provided the following examples of COVID-19 phishing email subjects:

- *Cancel shipment due to corona virus _ New shipping schedule details*
- *Corona is spinning out of control*
- *Feeling helpless against Corona?*
- *Military source exposes shocking TRUTH about Coronavirus*
- *Corona virus is here, are you ready? (Learn how to survive)*
- *Get your coronavirus supplies while they last*

What measures should employees and employers use to prevent cyberattacks during the pandemic?

Employers and employees both must take active steps in protecting the company and themselves from cyberattacks, especially while working remotely. Some of these steps should include:

- Ensuring appropriate security policies have been put in place
- Monitoring logs for malicious or unusual activity
- Encouraging employees to ensure they get the latest health information from these legitimate sources:
  - Coronavirus disease (COVID-19) (Public Health Agency of Canada)
  - Coronavirus disease (COVID-19) outbreak (World Health Organization)
- Ensuring that employees are aware of phishing email tactics and are well informed on how to tell the difference between fake and legitimate email sources
- If employees are working remotely, encouraging employees to ensure all devices, operating systems and software applications are up-to-date with the latest patches and versions
- Devices used for work-related functions should be encrypted wherever possible
- As employees work from home, the company should ensure that they have access to a quick and easy way of reporting security issues to the IT team

For more tips and advice on how to best avert cyberattacks, visit the Cyber Centre's website, which contains numerous helpful resources and provides continuous updates such as alerts and advisories highlighting new vulnerabilities that emerge in the cyber space.

Cyber insurance

Questions relating to cyber insurance will likely arise. Certain cyber insurance can assist with backstopping the business's risk arising from cyberattacks. The intent of cyber insurance or cyber risk insurance is to provide insurance coverage for internet-based risks or risks relating to information technology infrastructure and activities. As we mentioned in a previous blog, cyber risk policies can provide certain coverage for various liabilities:

- Data breaches that expose the personal information of an organization's customers
- Business interruption caused by a cyberattack

- Loss or destruction of data
- Computer fraud
- Ransomware attacks and other forms of cyber extortion

Cyber insurance is still a relatively immature area of insurance. This results in inconsistent coverage and language among policies and few relevant cases before the courts to interpret the policies in real life scenarios. It is important that a knowledgeable and experienced cyber insurance broker is retained to provide guidance, but it is equally important that the IT team in your business be involved in scoping the needs and reviewing policies in detail. It is important for the IT team and management to understand not only the possible coverage, but the conditions of coverage and the exceptions to coverage. Conditions can include installation of upgrades and patches in a timeframe that is not workable in the business. Exceptions can include certain cybercrimes resulting from social engineering that forms the basis of many of the attacks. The conditions and exceptions to coverage can, in many instances, render the insurance unusable in a practical setting.

Aird & Berlis LLP's privacy and data security experts can provide support and legal guidance to help your organization implement a comprehensive cyber risk management strategy and determine if cyber risk insurance is appropriate for your organization.

Authors

Paige Backman
Partner
T 416.865.7700
pbackman@airdberlis.com

David Mba
Student-at-Law
T 416.863.1500 x3320
dmba@airdberlis.com