Cyber Risks and the COVID-19 Pandemic

The spread of the new coronavirus and the resulting disease, COVID-19, has created immense challenges and hardships for individuals and companies. Unfortunately, some of those challenges are in the cyber arena.

The Cyber Risk Environment

Never being ones to miss an opportunity, cyber criminals and state actors are taking advantage of the disruption and uncertainty and are launching cyber attacks on remote workers at home and on supply chains.

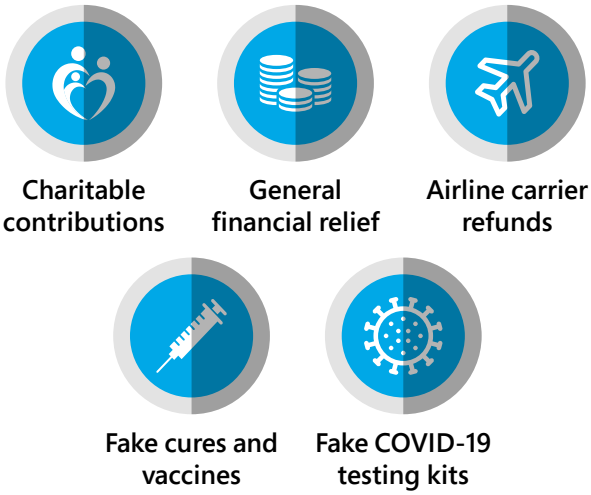
Phishing with COVID-19 as bait

Cyber criminals are focusing their efforts on phishing attacks. For example, in Italy emails have been sent stating that advice from the World Health Organization to avoid infection is contained in an attachment that purports to be a Word document. In fact, the attachment is a Visual Basic script that launches malware into the victim's computer. Similar attacks are taking place in other countries affected by the pandemic.

Other phishing attacks involve emails to employees that appear to come from senior executives, emails that purport to attach remote work policies, emails that purport to be from the US Centers for Disease Control and Prevention, and many more that encourage recipients to click on a link that installs malware or ransomware.

Phishing attacks aren't limited to those trying to install malware to disrupt systems or to steal information. Attacks are also being directed at individuals to obtain their personal information. In the US, emails are being sent asking individuals to verify their personal information so that they can receive an economic stimulus check from the federal government.

The FBI has noted other emails concerning:



State actors are also taking advantage of the pandemic though spear-phishing efforts. Russia, China, and North Korea reportedly have been the most active. The emails typically appear to include important information about the pandemic.

The number of phishing attacks has spiked with the spread of the pandemic. Some estimate that the volume of attacks has jumped by 40%. In Italy, where the pandemic has been particularly severe, the average number of phishing attacks since February 15, 2020 has nearly tripled the previous monthly average.

Interestingly, not all ransomware groups intend to take advantage of the pandemic. Suggesting that there might be some sliver of honour among thieves, the operators of the Maze, DoppelPaymer, Ryuk, Sodinokibi/REvil, PwndLocker, and Ako Ransomware infections have stated that they would not attack healthcare entities while the COVID-19 pandemic is active.

LOCKTON®

UNCOMMONLY INDEPENDENT

What should you do?

Educate your employees about how to recognise phishing emails on both mobile devices and desktop/laptops.

All emails related to the new coronavirus and the COVID-19 pandemic that invite the recipient to click on a link or open an attachment should be treated as suspicious. That is particularly true if they appear to come from governmental organizations or large companies with which the recipient has no connection.

Phishing attacks frequently originate in non-English speaking countries. Employees need to look for awkward phrasing and typographical errors.

As always, emails that seek personal information should be viewed with extreme scepticism. That is particularly true now with respect to emails concerning the pandemic.

Home is where the risks are

As of March 30, 2020, over 158 million people in the US, as well as the entire populations of the UK, India, and New Zealand are in lockdown. Many more countries throughout the world have adopted similar measures. Where it is feasible for employees to work from home, many are doing so. While this is the best way to avoid contact and maintain productivity, it also creates cyber risks.

The security of employees' home computers and home networks is usually beyond the control of their companies. The absence of necessary security on home networks also creates a heightened risk of system disruption. If an employee's computer contains malware (perhaps the result of a successful phishing attack), then depending on how the employee accesses the company's systems the malware can be transmitted to the company and result in system disruption.

What should you do?

- Educate employees about how to make home systems secure by:
  - Encrypting computer drives
  - Requiring strong passwords for wireless networks
  - Patching their software on a regular basis
  - Installing strong antivirus software that is regularly updated
- Require two factor authentication to access company systems
- Use mobile device management solutions to limit risks inherent in using personal devices such as mobile phones
- Train employees about what to do if they think their computer or their company account has been compromised
- Avoid public wifi
- Ensure virtual private networks (VPNs) and other secure remote working tools are configured for security. Avoid having default system administrator logins in place.
- In the longer term, if it hasn't been done, implement and configure remote access solutions to limit the ability to store sensitive information on the employee's computer and to prevent malware from migrating from an employee's home computer to the company's systems.

Remote working fundamentals

The Basics

- A computer
- A good internet connection
- Chat and conferencing applications
- A dedicated workspace
- A phone and camera
- Self-motivation and discipline
- A strict routine

VPN Access

Require VNZ access for internal networks as it encrypts your corporate traffic to avoid man-in-the-middle attacks or eavesdroppers.

Password Policies

Update password policies across the company.

Separate User Account

If your group members are is using their own devices, require a new user account to be set up for work use only.

Security

The best option is business-class endpoint security that may be managed by the company's IT team leveraging a firewall. Ensure multi-factor authentication is required and provide an encryption solution where using personal devices.

Payment card 'card not present' transactions

Lockdowns imposed to limit the COVID-19 pandemic have forced numerous businesses to close. Some are continuing to operate by taking orders by phone or email. Those businesses need to ensure they are following the same PCI-DSS protocols for payment card transactions required by the card brands that are used in physical stores. Following the standards will greatly reduce or remove the likelihood of fines or penalties being levied should there be a breach of cardholder data.

What should you do?

See **https://www.pcisecuritystandards.org/covid19** for more information.

The coronavirus data you may be catching

The COVID-19 pandemic is something most people have never seen before. It is frightening and confusing, and people often don't know what to do. In an effort to protect employees, customers, and others, companies may ask for data from individuals that they are not entitled to, and they may illegally share that with others.

Data may also be used in unusual ways. For example, technologies are being developed that may make obtaining data on individuals who may have been exposed to the virus, much easier. A Malaysian company announced in February 2020 that it had developed an artificial intelligence risk profiling product for tracking Chinese travelers. It isn't difficult to imagine that such a product could violate privacy laws in some countries.

What should you do?

Companies need to think carefully about collecting and sharing information that is legally protected. While the COVID-19 pandemic is a unique phenomenon, it has not yet led to changes in the law concerning the collection, sharing, and use of private information. Accordingly, companies should continue to adhere to existing privacy laws. Lockton encourages companies to consult with legal counsel whenever questions arise in this regard.

Regulators are trying to help

Regulatory compliance has become more difficult for many companies as the pandemic has spread. Regulators are feeling their pain and are granting various forms of relief. Enforcement of data protection regulations, and in some cases the regulations themselves, are being temporarily relaxed in the US, Italy, Germany, France, and other countries around the world. Broadly speaking, the goals appear to be to allow companies to handle data in ways that promotes delivering healthcare to individuals and to facilitate tracking the spread of the pandemic. To date, the regulatory relief has been fairly narrow.

What should you do?

Now more than ever, companies need to pay attention to the data protection regulatory environment that they are in. While it seems fair to say that regulators will be understanding throughout the pandemic, it would be a mistake to relax compliance efforts in any area other than those specifically identified by regulators.

The Cyber Insurance Environment

Insurer performance

Insurers are facing many of the same challenges that their policyholders are grappling with. They are trying to figure out how the pandemic will affect them and what related insured losses they will have to pay. They are thinking about what changes they need to make to their policies and what they now need to do to correctly underwrite them. Like other companies, insurers are trying to figure out how to manage their workforce that is suddenly working remotely while continuing to provide an undiminished level of service.

At Lockton, we are working closely with our insurance carrier trading partners to ensure any changes in underwriting and coverage are analysed and addressed appropriately by our teams.

Insurer reaction to the pandemic

Insurers understand the financial and other difficulties that the COVID-19 pandemic is creating for individuals and businesses. In an attempt to help, some are temporarily suspending cancellation and non-renewal of policies due to non-payment of premium.

Coverage for cyber losses

Lockton continues to monitor claim activity and coverage positions closely. While many P&C lines are in question around coverage, many cyber perils covered under cyber policies will most likely be more straight forward given the nature of the trigger.

Cyber coverage

Many concerns have recently been around remote working environments. Employees working from home create a potential issue regarding whether their personal computer is part of a company's computer system for purposes of cyber coverage. 'Computer system', or words to that effect, are typically defined in a policy. Most policies seem to encompass remote working arrangements to fall under this definition. The definition of Insured also commonly includes employees working on behalf of the Insured. If any insurer takes a contrary position, that claim will be very challenging to resolve.

Cyber and technology-related business interruption

Nuances around other related coverages are not as straightforward. While we expect business interruption resulting from a cyber incident to be covered as in normal course, system failures resulting in interruption will depend on the extent of coverage in place as well as the facts around the circumstance. Civil actions may exclude coverage while technology failures under the Insured's control resulting in a system outage will most likely be covered, assuming that coverage is in place. (Note system failure business interruption coverage is not a traditional coverage and usually is sublimited or priced at a high premium, depending on the operations of an organisation). Although it isn't difficult to imagine circumstances that would paint this coverage issue in a heavy coat of gray paint, insurers are likely to be sceptical of arguments where the cyber event causing the loss is not clear.

Technology Errors & Omissions

Companies with technology E&O policies in place may see liability claims arising out of outages or degradations in their service due to inadequate bandwidth, staffing or other problems in their course of business. It is important for policyholders to review the definitions of Wrongful Act and Claim as well as the exclusionary language in the policy.

The information contained within this document is not intended to be legal advice and should not be relied up for such purposes. If you have any specific queries regarding coverage, Lockton strongly urges organisations to review their policy language with their Lockton Associates. For any organisations not purchasing dedicated cyber insurance policies, extra caution should be followed regarding coverage that may appear to exist under other coverage lines like property, E&O, D&O, casualty, or business owners policies.