Dealing with the Cybersecurity Challenges of Coronavirus

By Thomas J. DeMayo, Principal, Cyber Risk Management

The coronavirus has grabbed the attention of the world by inciting fear and uncertainty into people's lives and bringing into question the operational stability of a business should employees be unable to leave their homes. As the world struggles to contain the coronavirus and businesses prepare for the potential impact to their operations, we offer the following cybersecurity considerations to help safeguard your business and workforce.

Social Engineering

Issues or events that trigger emotional distress or curiosity are key topics for cybercriminals to use in creating social engineering campaigns. A social engineering campaign is an act through a social mechanism – be it email, phone calls, text messages, etc. – that are designed to manipulate the victim into performing an action, e.g. clicking on a link, opening an attachment, or disclosing information. For these types of attacks to be successful, they must trigger an emotional response with the target. The coronavirus scare is the perfect mechanism for cyber criminals to leverage and trigger that emotional response.

Remind your employees to be cautious of emails with links or attachments that reference the coronavirus or status thereof. The following scenarios are examples of how the virus could be leveraged to manipulate your employees:

- An email from a spoofed news outlet claiming a cure has been found or a pandemic has been declared. A link is supplied to access an article for the victim to click to read the additional details. While the act of clicking alone may sound benign, that is enough for the cyber criminals to infect your systems, steal data, or hold you hostage with ransomware.
- An email claiming to be from Human Resources or the COO with an updated work from home policy in response to the virus. The memo is provided in an attachment that needs to be opened. The act of clicking on the attachment and opening the document could be enough in and of itself to become compromised.
- A message from a fraudulent charity soliciting donations to find a cure or help those impacted. As with any time of crisis, people will try to create fraudulent schemes to steal money.

Remind your employees that when receiving any messages that reference the virus to ***Pause, Inspect, and Think*** (PIT) before acting. Remind and encourage them to control their emotions and not to let their fear or curiosity drive their response. It is critical that you also have someone who the employees can reach out to if they have questions about the communication and want to confirm the legitimacy. If you have standard methods of communicating significant issues, such as posting the information to your intranet, remind employees of these methods.

Remote Work Force

Over the past week, many businesses are minimizing office staff and requiring employees to work from home. Conferences are being canceled and meetings are moving into the virtual spectrum. Many businesses have a business continuity plan, but a lot of businesses still don't. For those that have a plan, remote access strategies will be put to the test. For those that don't, the urgency to create one will be pushed to the forefront and defined on the go. If you haven't already defined and verified your remote access solution, be sure that you factor in security. While you certainly need to operate, you don't want to expose the business to being compromised or trigger an inadvertent data breach. For example, allowing employees to take copies of data on removable drives from the office location to work from home may result in data loss should the drive be misplaced.

The following should be considered as part of your strategy:

- If your employees access sensitive data, they should be provided a company-controlled and secured laptop, inclusive of encrypted hard drives. While ideally everyone will have a laptop to work remotely, that may not be a financial reality or a necessity. If you need to prioritize, focus on the high risk employees based on the sensitivity of the data they need to access.
- Any remote access or cloud based application should leverage multi-factor authentication. This is particularly important if you embark on a rapid deployment of a remote desktop software such as LogMeIn or GoToMyPC to allow employees to utilize their own equipment at home to connect to their at-work resources.
- If you have the resources, offer to have your IT department perform a security check on employees' home devices if the ultimate decision is that they need to work from home using their own equipment.
- Try to limit the options for employees to save data out of secured locations to their own devices. The capabilities will depend on the solution you implement.
- Ensure you establish and communicate clear expectations of the work-from-home strategy. While you may not be able to implement the ideal set of technical controls to manage risk, you can ensure your employees play their role and know how to work efficiently and securely when not in the office. Empower them with the knowledge of the risk so they know how to manage it.
- Once the crisis begins to subside, require and communicate to employees that any saved data to non-traditional locations during the course of the crisis be securely returned to the company and removed or destroyed from those other locations.

Going Forward

This is without question a scary time with potentially devastating consequences to human life and the operational stability of businesses. However, know you are not doing it alone. If you need assistance in establishing a secure work-from-home protocol or creating a cybersecurity program designed to be resilient regardless of the issue, we are – and will remain – available to assist you.

Part of our mission to provide "value-added" services is only possible if we can ensure your success in the process. We strive to be your trusted advisor not only through the good times, but also through the more challenging.

Contact Us

Thomas J. DeMayo, Principal, Cyber Risk Management
CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE

PKF O'Connor Davies, LLP
665 Fifth Avenue, New York, NY, 10022
212.867.8000 or 646.449.6353 (direct)
tdemayo@pkfod.com

www.pkfod.com

About PKF O'Connor Davies

PKF O'Connor Davies, LLP is a full-service certified public accounting and advisory firm with a long history of serving clients both domestically and internationally. With roots tracing to 1891, twelve offices in New York, New Jersey, Connecticut, Maryland and Rhode Island, and more than 800 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O'Connor Davies is ranked 29th on *Accounting Today*'s 2019 "Top 100 Firms" list and is recognized as one of the "Top 10 Fastest-Growing Firms." PKF O'Connor Davies is also recognized as a "Leader in Audit and Accounting" and is ranked among the "Top Firms in the Mid-Atlantic," by *Accounting Today*. In 2020, PKF O'Connor Davies was named one of the 50 best accounting employers to work for in North America, by *Vault*.

PKF O'Connor Davies is the lead North American representative in PKF International, a global network of legally independent accounting and advisory firms located in over 400 locations, in 150 countries around the world.