South Florida Business & Wealth
https://sfbwmag.com/how-to-mitigate-it-risks-amid-covid-19/

How to mitigate IT risks amid COVID-19

May 20, 2020

by Kevin Gale

By Jose Antigua

Jose Antigua is director, Assurance Services, at Marcum, which provides tax, audit and advisory solutions, including IT risk mitigation efforts

As mandated closures led to companies converting teams into remote workforces and demand for online connectivity drastically increased, a new wave of vulnerabilities has emerged. The sources of these vulnerabilities can be grouped into three sources:

- People
- Processes
- Technology

We'll review these sources and highlight some of the immediate actions companies should consider to decrease risk to their information technology infrastructures.

People

Employees are likely anxious and uncertain about the economy, personal finances, health and safety of themselves and their loved ones, the state of the company they work for, and much more.

With heightened emotions comes an increased susceptibility to fraud. There have been increases in phishing scams, including emails that appear to come from the CDC with COVID-19 (coronavirus) updates and the Small Business Administration around loan opportunities and the CARES Act. Other scams circulating offer promises of unemployment insurance as well as those that mimic the types of emails that might come from an internal IT department. Furthermore, a recent cyber threat assessment released by Thales reported that "50% of the domain names created since December and linked to the theme of COVID-19 or coronavirus can lead to the injection of malicious software".

Another area of concern stems from many people taking on new tasks and/or completing tasks in new and different ways in the virtual workplace. While the idea of agility has been celebrated in business for the last several years, we're seeing a test of our ability to adapt like never before.

Employees might be logging into secure Virtual Private Network (VPN) networks or using a web mail version of their email that they're unfamiliar with. Sales efforts have moved online and meetings are being held virtually in nearly every context. Every new task comes with a risk of misuse or misrepresentation.

What should you do?

- Ensure you have email monitoring in place to detect unusual activities, including logins from unexpected sources (signs of malware) and potentially harmful content embedded in received emails.
- Conduct mandatory security awareness training, including a focus on phishing scams.
- Launch campaigns to remind employees and customers how you would typically communicate.
- Consider stronger data input controls. For example, use dropdown menus in systems as much as possible instead of free text. Furthermore, make sure important information is marked and made mandatory wherever appropriate.
- Limit the remote access granted to specific areas of networks. Not every user needs access to everything—especially when working in a remote environment.
- Conduct training on any system that has been modified or where the access might appear different to your user. This could be live or it could be in the form of recorded videos and presentations as well as step-by-step reference guides.

Processes

As alluded to in reference to employees, protocols and workflow might have changed out of necessity. You might have looked for quick fixes to access points and your IT infrastructure might now be compromised in some way. These could relate to back office processes as well as sales offerings and processes. If you created a new way for a customer to engage with your business (e.g. online ordering systems, download options, etc.), you might be gathering information and/or have the opportunity to collect data that you've never had before.

Quick decisions might have led to quick action by IT professionals without careful reflection on the unintended consequences. New vendors might have been introduced into your operations (e.g. video conferencing tools).

While many businesses are facing financial pressure in the midst of applying for loans, processes around accessing financial resources could also be impacted. You might look to transfer fund to and from other parties.

What should you do?

- Review any procedures that changed quickly and test them for security protocol, such as approval requirements.
- Make sure you have a management hierarchy defined.
- Maintain and backup historical data in case you need to reset due to any successful penetrations of your systems.
- Conduct due diligence on vendors and systems as quickly but also as thoroughly as appropriate. This might require asking for an independent third-party validation of those providers (e.g. SOC reports, PCI certifications, ISO certifications, etc.).
- Involve your IT and security focused professionals in decisions even when they are not directly tied to technology on the surface.
- Don't rely on default settings when implementing new technology.
- Require verbal and even video authorization for any transfer of financial resources and/or sensitive information.

Technology

Employees are leveraging home networks that could have already been or could become compromised. This allows for the interception of information, including confidential information, that could be stored locally or transmitted over that vulnerable home network.

Similarly, the debate around employees using personal devices has shifted to a new realty of large numbers of workers using home computers for to access company systems, including web applications.

Additionally, systems are potentially being pushed to their limits in terms of usage with new levels of demand placed on servers. While many companies might have planned from employees to work remotely for convenience, as an employee perk, or when dealing with minor ailments, they might never have considered the strain of an entirely remote workforce.

What should you do?

- Implement an automated screen lockout policy for workstations (i.e. machine timing out when unattended).
- Leverage a VPN in order to restrict the transmission of confidential information.
- Activate multi-factor authentication for web-based applications, file sharing sites, and other hosted systems.
- Activate and monitor logs in order to detect unusual activity.
- Consider updating firewalls and network and web application monitoring rules to include new threats stemming from new locations (i.e. workers accessing from home).
- Evaluate your capacity to accommodate an increase in remote access (i.e. network bandwidth, server processing capacity, etc.).

- Schedule system patching, including firewall updates.

Continue assessing and planning

The threats and risk mitigation techniques highlighted here are a sampling of what exist. They're intended as a bare minimum to ensure the safety and security of operations while embracing the "new normal." Senior management should look to collaborate across departments to ensure needs are being met and to engage with their IT professionals as they look to stay current with the latest techniques being used to penetrate businesses.

Jose Antigua is director, Assurance Services, at Marcum, which provides tax, audit and advisory solutions, including IT risk mitigation efforts. He may be reached at (954) 320-8054 or jose.antigua@marcumllp.com