COVID-19 CONTENT SERIES

EVOLVING CYBER RISKS IN A COVID-19 WORLD

Toby DeRoche, CIA, CCSA, CRMA, CICA, CFE

The Institute of Internal Auditors
INTERNAL AUDIT FOUNDATION™
Wolters Kluwer

Table of Contents

About the Expert

Toby DeRoche, CIA, CCSA, CRMA, CICA, CFE

Toby DeRoche, CIA, CCSA, CRMA, CICA, CFE, is a solution consultant at Wolters Kluwer. His professional background includes identification and documentation of weaknesses that result in heightened business risk, while recommending solutions to such situations. Throughout his career, Toby has assisted numerous internal audit departments create, perform, and supervise financial, operational, and compliance audits to evaluate control frameworks, financial systems, and operating procedures.

INTRODUCTION

The COVID-19 pandemic unleashed a perfect storm of events that exposed organizations to increased cyber risk vulnerability with both emerging and atypical cyber risks. Employees are juggling job responsibilities with concern for the safety of themselves and their families. The workforce has transitioned to remote work with little or no preparation and training. Organizations are focused on surviving with massive revenue reductions and global economic upheaval. With this much chaos, hackers and other cyber criminals have an opportunity to capitalize on our vulnerability. The increased risk is so significant that even the U.S. Federal Bureau of Investigation (FBI) and Department of Defense (DoD) have issued warnings for remote workers.

To help internal auditors remain vigilant regarding cyber risk both during and after the COVID-19 pandemic, this paper examines many of the situations that require heightened awareness. By no means is this an exhaustive list, but rather an effort to prompt your evaluation of cyber risks in today's environment and start thinking ahead for the post-pandemic world.

REMOTE WORK EXPOSURE

Organizations spend enormous effort creating a secure IT environment to protect their network and data. The moment employees relocate from the office to their homes for work, much of the secure environment is bypassed and a host of new exposure points opens. A typical home for a family of three can have an amazingly complex network with multiple desktop computers, laptops, printers, tablets, phones and other mobile devices, gaming systems, home alarms, thermostats, smart speakers, and other devices. By introducing remote work, the situation expands with additional laptops and company phones. "With the increased telework capability comes an increased attack surface for our adversaries. They are already taking advantage of the situation and the environment that we have on hand," said Essye Miller, deputy CIO for the Department of Defense.[1] From an organizational point of view, your digital footprint just expanded exponentially, and so did your cyber risk.

Network Security

As a first step, all employees must secure their home network. By securing their Wi-Fi, it is more difficult for anyone with malicious intent to spy on network traffic. The network password should be revisited to ensure it meets complexity guidelines. Many network passwords were established by internet service provider technicians as phone numbers or addresses and never changed. With basic home networks, remote workers will still be cut off from the firewalls, security patches, and backups that come from being in the office.

To access any organizational data, employees should be required to use a VPN with multifactor authentication. If you use a remote desktop to access organizational data, only specific IP addresses should be whitelisted by your IT department.

One of the threats to network security comes from downloading third-party software. Remote employees often struggle when they feel cut off from the tools and access they had in the office. They may even try to find ways around these limitations with free software options. For example, they want to have face-to-face conversations like they had in the office, so they might download web conferencing tools, like Zoom or Bluejeans. Unfortunately, some of these platforms can be hacked,[2] exposing your organization to cyber criminals. Communication tools should be restricted to only those approved by your IT department.

Personal Devices

In some cases, the decision to move to remote work must be made quickly. Either by design or by necessity, employees may need to use personal devices to complete their work. Those devices may not meet your security measures, especially when handling confidential data or personally identifiable information (PII) from

[1] DOD Warns of Cyber Risks as Employees Work From Home

[2] Zoom Meetings Keep Getting Hacked. Here's How to Prevent 'Zoom Bombing' on Your Video Chats

employees and customers. If your organization does not have a bring your own device (BYOD) policy,[3] one should be established immediately. The policy should address approved device types, use of VPN, end point controls, mobile wiping of data, support expectations, password rules, and encryption. Many employees are surprised to learn that companies often reserve the right to perform a remote data wipe on their personal mobile device if they used that device for work and then end their employment. Make sure the policy is very clear and everyone understands it.

Phishing Schemes

When employees use personal equipment or cannot gain access to the network with a work laptop, there may be limitations with pushing out security patches or updates. If this is the case, work with your IT security team to discuss disallowing personal equipment and other methods for pushing out updates to organization-managed devices.

To make matters worse, there is a significant increase in phishing schemes targeting remote workers. Many of these are emails claiming to have personal protective equipment, such as masks and face shields. If your home-based employees are checking personal email on their work laptops, they could easily expose your network to malicious code from a phishing attack. All laptops sent home with employees should have firewalls and strong antivirus protections to prevent threats from entering your system and to detect, and hopefully remove, the ones that ultimately do get through.

Recent phishing attacks use COVID-19 fears to lure unsuspecting victims.[4] One group, calling themselves Mustang Panda, used phishing that contained a compressed Windows archive file that they claimed had statements on the pandemic from the prime minister of Vietnam. When the file was opened, it was an innocent looking Word document that was actually running macros in the background to initiate a command-and-control attack. Since the computer could sit behind the network firewall, the criminal now has access to network data or could choose to shut down the network entirely.

File Sharing Sites

As your employees are working away from the network, they will run into roadblocks. For instance, if they cannot get to your shared network drive, SharePoint, or Teams, they may have difficulty sharing files with coworkers. People will usually get creative and use the same methods they use at home. Using sites like Dropbox or Google Drive to share files is most likely not approved by your organization's IT security team.

[3] Create a Mobile BYOD Policy for the Coronavirus Pandemic

[4] Nation-State Hackers Using COVID-19 Fears to Spread Malware

PRIVACY LAWS

The increased exposure from remote working also puts your organization at risk for noncompliance to privacy laws, such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA). Again, thinking through a common scenario, an employee may not have a dedicated workspace in the home for working remotely. In this case, he or she may work in a dining room or living room with other family members. If this individual routinely handles confidential data, especially if the job requires discussing confidential information on calls, the risk of violating the physical safeguards section of HIPAA is extremely high.[5]

Risk exposure with confidential data is even more complicated if your remote workforce includes IT support staff who may be accessing client systems for troubleshooting. Troubleshooting often requires remote viewing of the client's desktop or sharing screen prints. These activities can easily cause unintentional data breaches, and if the remote worker is using a personal device, the data exposure can be even more significant.

With regulations like HIPAA, internal audit has an obligation to perform both routine and incident-based audits. We need to be prepared to act quickly to review the working environment for our remote workers to ensure an appropriate level of security is in place.

[5] Meeting HIPAA Requirements When Working Remotely

VENDOR MANAGEMENT AND SOC REPORTING

Outside our own organizations, we may also face increased third-party cyber risks. For software as a service (SaaS) solutions, we typically depend on service organization controls (SOC) reports to validate our technology vendor's control framework. If our vendors are also moving their workforce to a remote environment, we need to ensure their control environment is up to standard if we are going to rely on those controls.

Consider a basic control, such as physical security.

The service provider should have developed security policies and procedures that cover:

- Securing of physical access to and within the facility by employees, vendors, and visitors
- Standards for reception areas, perimeters, surveillance, security guards, and security patrols
- Standards for securing specified types of locations and assets
- Lock and physical security device standards
- Background investigations of employees, prospective employees, and vendor employees
- Issuance of access cards/IDs used to access facilities
- Removal of access by terminated employees/vendor personnel
- Investigation of physical security violations
- Movement of assets

The control could be perfectly designed for the vendor's facility, but when employees are working remotely, you simply cannot guarantee the same level of control. Friends, family, repairmen, and others will come in and out of the worker's home.

We should look for best practices,[6] such as:

1. Proactive security awareness training
2. Remote work policies
3. Requirements for end-user controls, like password strength
4. Network traffic monitoring

The goal is to ensure vendors have mitigated risks on their end so we can continue to rely on their control framework.

Cybersecurity Previously Identified as One of the Top Risks for 2020

Pre-COVID-19, The Institute of Internal Auditor's report, *OnRisk 2020,* identified cybersecurity as one of the top 11 risks likely to affect organizations this year. A key finding of the report cited cybersecurity as a critical knowledge deficit. Board members, executive management, and chief audit executives (CAEs) were aligned on this perspective and the high level of organizational relevance of the risk. The report recommends that risk management players should prioritize building their cyber knowledge base.

Source: *OnRisk 2020: A Guide to Understanding, Aligning, and Optimizing Risk*. Lake Mary, FL: The Institute of Internal Auditors, 2019.

[6] SOC 2 Academy: Access Controls for Remote Employees

THE PANDEMIC'S IMPACT ON CYBER CONCERNS

Decreased Focus on Cyber Risks

Remote workers are doing their best to stay engaged with work, but the health and well-being of their families and themselves will always take precedence. When parents are anxious about finding groceries, working with their children on their remote schoolwork, and dealing with the increased stress in life, following good cyber practices may not be their highest priority.

Businesses, in turn, are dealing with drastically reduced revenue and trying to remain viable. Many have shut down all support functions, furloughed all but a handful of employees, and reduced the pay for those who remain. All hiring and spending is frozen for the foreseeable future. When financial risk is at its highest, cyber risk ranks lower in a relative assessment. IT security teams are often working with absolute minimum staff levels, so they are prioritizing where their time will be spent, and this will be stretched thinner by having to secure a newly remote workforce.

Cybersecurity in the New Normal

While the COVID-19 pandemic has had an immediate impact on the potential for cyber risk exposure, the risk is here to stay. The lasting effect of a mandatory remote work order across the world is likely to leave a lasting impression. On the positive side, traffic, fuel consumption, pollution, and many office operating costs are down. We are spending less on food because we don't eat out as often. Families are spending more time together. People are out walking and riding bikes.

With all of this considered, it's difficult to imagine everyone acting like this time never happened and returning to work as usual before the COVID-19 pandemic hit. As internal auditors, we have a duty to point out the increased risks to management. Our future work environment is probably going to be a hybrid of office-based and remote work. Our cybersecurity controls must be updated to reflect the current situation, and we must be prepared for the future.

32%

of CAEs indicated they **did not allocate any** internal audit resources to cybersecurity.

Source: 2020 North American Pulse of Internal Audit. Lake Mary, FL: The Institute of Internal Auditors, 2020.

CONCLUSION

As internal audit functions worldwide demonstrate agility, updating risk assessments and revising audit plans, a high degree of value can be derived from an increased focus on cyber risks.

Audit Areas to Consider Right Now

For auditors who will examine the impact of remote workers, we recommend the following areas:

- Review work-from-home policies that require the use of organization owned and managed devices.
- Review personal device or BYOD policies and disallow access to organizational networks and data by devices that are not whitelisted.
- If you do allow the use of personal devices, make sure the hardware has appropriate security controls, and these controls should be supported by a BYOD policy.
- Require the use of VPN with MFA to access the network.
- Require training on common security measures, like protecting devices and password complexity.
- Require training for handling personal information from both employees and customers.
- Review policies for using only approved web meeting and data exchange sites.
- Review with vendor risk management the critical SaaS vendors to ensure SOC reports are still valid in the updated work environment.
- Review the business continuity plan in case of a data breach caused by internal or external remote workers.
- Check with your risk management team to ensure you have cybersecurity liability insurance in case there is an exposure.
- Review the level of staffing and decisions made regarding staffing for IT security and support departments

Suggested Reading

- **The Future of Cybersecurity in Internal Audit**
- **OnRisk 2020: A Guide to Understanding, Aligning, and Optimizing Risk**
- **Privacy and Data Protection Part 1: Internal Audit's Role in Establishing a Resilient Framework**
- **2020 North American Pulse of Internal Audit**

About The Internal Audit Foundation

The Internal Audit Foundation strives to be an essential global resource for advancing the internal audit profession. The Foundation's research and educational products provide insight on emerging topics to internal audit practitioners and their stakeholders and promotes and advances the value of the internal audit profession globally. Through the Academic Fund, the Foundation supports the future of the profession by providing grants to students and educators who participate in The IIA's Internal Auditing Education Partnership Program. For more information, visit www.theiia.org/Foundation.

About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 200,000 members from more than 170 countries and territories. The association's global headquarters is in Lake Mary, FL. For more information, visit www.theiia.org.

About TeamMate

As part of the Tax and Accounting Division of Wolters Kluwer, TeamMate helps professionals in all industries at organizations around the world manage audit and compliance risks and business issues by providing targeted, configurable, and efficient software solutions. Solutions include TeamMate+ Audit, TeamMate+ Audit Public Sector, TeamMate+ Controls, and TeamMate Analytics. Together, this ecosystem of solutions provides organizations with the combined assurance they need to manage all aspects of risk identification and assessment, electronic working paper creation and management, controls framework management, and data analysis. For more information, visit www.teammatesolutions.com, follow us on Twitter, Facebook, Linkedin, or YouTube.

DISCLAIMER

The Internal Audit Foundation and The Institute of Internal Auditors publish this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The Foundation and The IIA recommend seeking independent expert advice relating directly to any specific situation. The Foundation and The IIA accept no responsibility for anyone placing sole reliance on this material.

COPYRIGHT