GLOBAL KNOWLEDGE BRIEF

SECURITY IN A WORK-FROM-HOME ENVIRONMENT

IT must adapt to new threats and challenges

FASTPATH

The Institute of Internal Auditors | Global

Table of Contents

About the experts

Frank Vukovits CIA, CISA

Frank Vukovits is director of strategic partnerships at Fastpath Solutions LLC, building relationships with audit partners around Fastpath products and services. Prior to joining Fastpath, he was one of the founders and served as director of programming for the Microsoft Dynamics AX User Group, now the largest user group in the world dedicated exclusively to Microsoft Dynamics. Vukovits as a user has implemented and managed numerous ERP projects. Previously, he spent 12 years in corporate IT audit for GTE/Verizon.

Alex Meyer

Alex Meyer is the director of Dynamics AX/365 for finance and operations development at Fastpath Solutions LLC. He is a subject matter expert in Microsoft Dynamics AX/365FO security and presents sessions and webinars surrounding security and native controls in numerous ERPs. Meyer also writes frequently in a blog specifically for Dynamics 365 for finance and operations. He has a Bachelor of Science degree in computer engineering from Iowa State University.

INTRODUCTION

IT departments challenged by new threats

IT departments within organizations face a constant challenge in dealing with an ever-evolving threat landscape involving the technology used by its employees. The COVID-19 pandemic forced enormous changes in the modern workplace that made this challenge substantially more complex.

Even before this radical change, the stakes and potential losses were huge. According to the FBI, organizations in 2019 lost $1.7 billion to email phishing scams alone.[1] On an enterprise level, the risks were underscored in news reports that hackers stole the usernames and passwords, along with the IP addresses, of more than 900 VPN enterprise servers. According to ZDNet, the information was shared on a hacker forum frequented by ransomware gangs.[2]

Indeed, the threat landscape has grown greatly because of the work-from-home (WFH) scramble that ensued from the COVID-19 pandemic. Workers were suddenly displaced from their offices to their homes as organizations struggled to stay in operation. These employees, some of whom were not tech savvy, suddenly found they needed to become their own IT support desk, setting up their home office. At the same time, they were increasing their organizations' exposure to potential risk in the process.

In this knowledge brief, Frank Vukovits, CIA, CISA, director of strategic partnerships at Fastpath; and Alex Meyer, director of dynamics AX/365FO development at Fastpath, discuss solutions and suggest free resources to help manage the IT security challenges a WFH environment presents.[3]

1. Federal Bureau of Investigation, "2019 Internet Crime Report," February 2020, https://pdf.ic3.gov/2019_IC3Report.pdf.
2. Catalin Cimpanu, "Hacker Leaks Passwords for 900+ Enterprise Servers", ZDNet, August 4, 2020, https://www.zdnet.com/article/hacker-leaks-passwords-for-900-enterprise-vpn-servers/.
3. To access an on-demand webinar from Fastpath discussing home-security controls, go to https://www.gofastpath.com/iia-od-work-from-home-world-webinar.

THE NEW ENVIRONMENT

Work-from-home creates new threat landscape

Biggest threat involves devices

The sudden onset of the COVID-19 pandemic caused unprecedented upheaval in workplaces globally as organizations shuttered offices and sent employees to their homes to work. Indeed, the pandemic exponentially sped up the shift to full-time remote work. According to a Gartner Inc. survey of human resources executives worldwide, 88% of companies have encouraged or required their employees to work from home. Many of those employees are likely to continue working-from-home for the foreseeable future as economies recover to the new normal.

The shift to working from home has created a much broader and more complex threat landscape, Vukovits said. The biggest threat involves devices, such as laptops and printers, now being used by workers on their home networks. Although they continue to work with corporate assets, many workers are now reliant on their home network controls. To complicate matters further, employee home networks often are shared with other members of the family, such as school-age children who are working remotely, or other members of the household also working from home.

Shadow IT

Shadow IT is hardware or software that is not supported by an organization's IT department. The term often carries a negative connotation because it implies that the IT department has not approved the technology or does not even know that employees are using it. In the past, shadow IT was often the result of an employee's desire for immediate access to hardware, software or a specific web service without going through channels. With the consumerization of IT and cloud computing the meaning has expanded to include personal technology that employees use for work or cloud services supported by a third-party provider or in-house group.

Source: www.techtarget.com/network

If the company has a bring-your-own-device policy, the employee may be accessing company assets on a home computer, but the policy may not address home networks linked to the company's network through a VPN. In addition, even if the computer is company-issued, it may not have gone through the usual IT department security protocols.

Home modems, routers, and printers — often still using their default passwords — also are vulnerable. Many employees on their own download software without their IT departments' knowledge or consent – "shadow IT" – such as Zoom or other web conferencing platforms, or apps needed to do their jobs. This exposes their companies to potential security issues. Zoom, for example, has scrambled to issue a number of updates to address security flaws, underscoring the importance of educating people as to why software updates are important.

Large companies have an advantage in this situation because many can afford to give employees critical security awareness training. These companies also can assign a computer to an employee for home or office use. Smaller companies, however, can find it challenging to educate employees about security awareness and/or keep an effective device inventory. Such inventories should include information such as whether a device's security is up-to-date and if it contains any vulnerabilities that could potentially be exploited. If a company struggles to maintain the resources to track device capability in such detail, the potential for risk significantly increases.

Legacy companies — which either are in the process of digital transformation or have just gone through it — are also particularly vulnerable to security issues. These companies often make quick assumptions about the technology, and assumptions about cloud security, in the rush to make the transformation. A company's cloud system may be secure, but that does not mean the applications the company is using — and the software behind them — are secure.

Dealing with all these new responsibilities can be frustrating for employees, who must address concerns and resolve problems for which they may not be trained or may not have time to solve in an already crowded workday. In addition, IT assistance is often not readily available.

"We like to think that people are technical in today's world, but a lot of people aren't. And just because you can click a couple icons and click okay and type some stuff doesn't make you technical," Vukovits said.

BUILDING A PLAN

Companies need to think holistically

Tone starts at the top in addressing security

Companies need to think holistically, across the entire organization, to build an effective culture of security. Visualize it as Four Rings of Security, Meyer said (Exhibit 1). The database is at the center, surrounded by the application used to interface with the data, which is in turn surrounded by the network/infrastructure that connects the application to the database. The user — the largest threat area — is the outer ring.

Organizations need to ensure controls are in place across all four rings, especially in this new environment. Pre-COVID, all four of these rings were inside the organization. Now, the two outer rings are in the home environment.

Importantly, in building an effective security culture, the tone starts at the top and needs to flow through the organization. Executive buy-in, which sometimes can be a stumbling block, is critical. The data protection elements in the European Union's General Data Protection Regulation are good concepts with which to start.[4]

Communication is important in the WFH environment. The human resources department can get involved in communications and training, including onboarding new hires. "It's a company-wide initiative to work from home. That means HR needs to be involved, IT needs to be involved. How are you educating the business?" Vukovits said.

4

Exhibit 1: Four Main Rings of Security

4. User

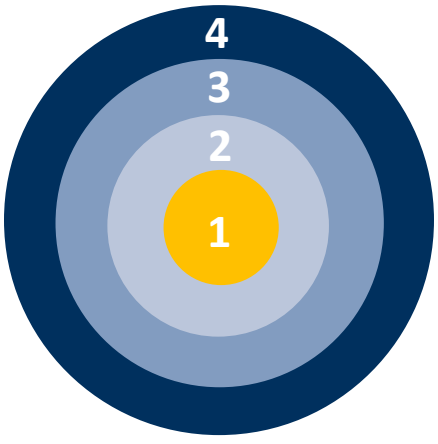
3. Network/infrastructure

2. Application

1. Database

In the current work-from-home environment, companies need to ensure effective security is still in place with each ring.

Source: Fastpath Solutions LLC



4. European Union "Complete Guide to GDPR Compliance," *GDPR.EU.* https://gdpr.eu/ (accessed August 2020).

SECURITY STARTS WITH EMPLOYEES

Workers are first line of defense

Family members now part of security environment

Security is more than a technical exercise. It involves people, process, and technology. All three need to work together to build strong controls for security and to implement a strong security program.

Importantly, employees need to understand they have a vital role in their company's security environment because they have become front line defenders. This extends to family members as well, because they have become users of the corporate network in the new environment. "You have to educate [employees]. They have to know from their boss, from their boss's boss, why this is important companywide. Because ultimately if they don't buy into it, they possibly are not going to do everything they are supposed to," Vukovits said. Some common tips for users and family members that will make home computers and home networks more secure include:

Multi-factor authentication

Multi-factor authentication (MFA) is a security mechanism in which individuals are authenticated through more than one required security and validation procedure. For example, a computer user's password is supplemented with a one-time password or code sent to the user's cellphone. Both are required for access.

Sources: Technopedia, Wikipedia.

- Run computers at the user level, which restricts access to the operating system, rather than at the administrator level.
- Do not share passwords or write them down.
- Use complex passwords or passphrases (Length offers more security than complexity).
- Use a password manager.
- Use multi-factor authentication (MFA) for both personal use and when using company devices.
- Lock the computer whenever you step away from it.
- Watch out for social engineering scams — someone claiming to be a higher-up in the organization, someone asking the employee to circumvent established processes.
- Secure home wireless networks
    - Change the default name and password.
    - Change the setting to make it non-broadcasting.
    - Encrypt using the WPA2 or WPA3 security protocols.

Additional tips

- Consider purchasing a modem and Wi-Fi hardware instead of using the equipment issued by the home service provider. These devices have firmware that gives the provider a support channel into the device.
- Change the default Service Set Identifier (SSID) — basically the name of the router — along with the default password.
- Establish a guest network that is separate from the home network used for work.
- Turn off visibility to other machines on your network,
- Avoid using USB sticks, instead use cloud services such as Dropbox or OneDrive.
- If possible, use the 5.0 GHz band rather than the 2.4 GHz band on home Wi-Fi router. The 5.0 signal is more secure because it has a smaller footprint.
- Disable WPS and UPnP. (WPS makes it easier to connect new devices to a network. UPnP is a set of protocols that allows devices to connect with one another to create private networks. Both have security flaws.)

All of these steps emphasize the importance of educating employees and raising awareness about the importance of IT security, as well as providing comprehensive help-desk support for employees.

WHAT EMPLOYERS CAN DO

External, internal threats need to be addressed

Security needs to evolve to keep pace with threats

Security is a continuing responsibility, not something suddenly taken on because employees are working from home. This is especially important because threats are constantly evolving. As a consequence, security also has to be constantly evolving, Vukovits said. A point to keep in mind, while the external threats make the news, a strong security program also addresses internal threats.

Microsoft has built protections into a range of products, including Azure and Microsoft 365, formerly Office 365. Companies should consider combining these into Microsoft Threat Protection, Meyer said. In addition, Microsoft has many apps that address security concerns. For example, the Microsoft Cloud App Center and the Microsoft 365 Security Center work to combine information into one dashboard that allows parties to see everything going on in the organization and form a risk perspective.

Questions to ask about employees' WFH environment

- What devices and apps — shadow IT— have employees or perhaps family members downloaded?
    - Did the employees follow the normal vendor process?
    - Were the devices or apps security checked?
    - Who is administering access?
- Have employees been provided with the encryption tools they need?
- Are employees being given support as tools are rolled out?
- Are employees being educated why a particular tool is being used and how to use it?
- Has backup and recovery been established for at-home devices?
- Have privacy and security guidelines been updated to reflect the WFH environment?

Steps employers can take

- Use a VPN for access to the company network.
- Use MFA for all services.
- Set up conditional access for users. Among other things, it allows an organization to grant users access only during certain time periods or from certain geographic areas.
- Establish a clear password protection policy.

- Enroll PCs and other devices into Microsoft Intune to manage and ensure compliance with company policies.

Many companies build security into existing company initiatives because security has a significant impact on company culture. If company policies and procedures are updated annually, the same should be true of security policies. The company should be the driver of change, not the employee.

CONCLUSION

IT faces challenge in being aware of new risks

Security is more than a technical exercise. There is no silver bullet that can eliminate all risk. However, many free resources are available to companies unsure where to start.

For IT professionals, the biggest challenge in a post-COVID world will be to admit they will have to look at things differently. They will have to be aware of new risks, focusing on areas that keep the company secure. For example, don't assume a product is secure just because it is from a reputable company or because it is in the cloud. (Recall the problems with Zoom's vulnerabilities.) IT departments will need to address how to secure company data downloaded onto a home computer, especially if that employee leaves the company.

A culture of security within an organization can be built without breaking the bank by shifting responsibilities among existing staff and changing priorities. Much can be accomplished by putting a WFH cybersecurity program together, developing an inventory of devices, educating users about what they need to do, and having tools to check what is running on employee machines. "It's about priorities; it's more about mindset than budget," Vukovits said.

APPENDIX: SUGGESTED RESOURCES

Microsoft resources

- Azure
  - Security Documentation
  - Infrastructure Security
  - Network Security Overview
  - Database Security Overview
  - Shared Responsibility for Cloud Computing
- Dynamics 365 Trust Center
- Making It Easier for Your Remote Workforce to Securely Access All the Apps They Need, from Anywhere
- Office 365 Plan for Security and Compliance
- Secure Remote Access to On-Premises Apps
- Secure Score
- Top Tips for Working More Securely From Home
- Top 12 Tasks for Security Teams to Support Working From Home

Tips for working from home

Computerworld. 12 Security Tips for the 'Work From Home' Enterprise

Federal Trade Commission. Online Security Tips for Working From Home

Malwarebytes Labs. Security Tips for Working from Home (WFH)

New England Institute of Technology. Top 5 Steps to Work Securely From Home

Additional resources

BKD CPAs and Advisors. Security & Agility for a Remote Work Environment

Center for Internet Security. CIS Controls Telework and Small Office Network Security Guide

Cisco. Defending Against Today's Critical Threats

National Cybersecurity Communications Integration Center

NIST. Cybersecurity Framework

SANS Institute. 2020 SANS Cyber Threat Intelligence Survey

Technology Record. Microsoft's Cyber Defense Operations Center Shares Best Practices

Verizon. Data Breach Investigations Report

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, Fla., USA. For more information, visit www.globaliia.org.

About Fastpath Solutions

Fastpath Solutions, LLC. has deep expertise in audit, security, and compliance, with multiple Certified Internal Auditors on the team. Fastpath has global partnerships with numerous audit firms and a client base of over 1,100 companies across 30 countries, supporting small to enterprise sized organizations and their risk management efforts. Fastpath Assure® is a cloud-based audit platform that can track, review, approve and mitigate access risks across multiple systems from a single dashboard. The platform comes with a pre-configured segregation of duties rule set specific to each ERP and works across a variety of ERP/CRM/HCM systems, including SAP, Oracle, Microsoft Dynamics, NetSuite, Intacct, Salesforce, JD Edwards, Workday, Coupa, ServiceNow, SailPoint, Zuora, Workiva, Jira, Zendesk, Acumatica, and custom applications. Visit us at gofastpath.com for more information.

Disclaimer

Copyright

October 2020

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 149
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.globaliia.org