ISSA

International Securities Services Association

Cyber Risk

Considerations for Remote Working

Introduction

The COVID-19 pandemic has had an enormous global impact, changing the ways in which financial institutions work in the short-term and forcing organizations to consider how these impacts will ultimately change how their workforce will operate in the future. The pandemic has tested some aspects of a financial institution's resilience and, as financial institutions, we have gained a better understanding of:

- Those operations that can be conducted remotely and those operations which must be conducted on-premise.
- Remote access capabilities and what is required to improve them.
- Third party and supply chain impacts.
- The impacts for employees on «how to work».

Given the current wave of outbreaks, a return to the offices for a majority of the workforce is not envisioned in the short-term. Further, once a safe and effective vaccine is available, there may be an interim period featuring some flexible openings of offices but with a continued high percentage of staff working remotely. Finally, even after an all-clear from public health authorities, we see the strong likelihood that the percentage of people working a significant proportion of their days remotely will be much higher than before the COVID-19 pandemic.

So, a greatly expanded remote working environment is likely here to stay. This greater remote footprint for our collective industry's staff has major advantages, but it also presents risks that need to be mitigated. Threat actors are quite aware that our collective working location footprint has greatly expanded and they could look for weaknesses in how a financial institution secures its remote access platforms and applications and look to exploit them to commit the same types of operational disruptions that were described in the 2018 ISSA white paper, ***Cyber Security Risk Management in Securities Services***. Thus, given the interconnectedness of the various players in the custody/securities services chain, it is critical that all financial institutions and their counterparties are aware of the key elements for properly securing their greatly scaled-up remote working platforms. ISSA is not making any new recommendations, nor are we aware of any securities servicing or capital markets associations that have published new frameworks or recommendations since March 2020. Rather, the Cyber Working Group members have worked together to survey the available security frameworks, focusing on their specific recommendations of best practices in securing remote working environments. Many of these existing frameworks were referenced in the 2018 ISSA white paper. This article serves to outline the main areas of security that these existing frameworks cover and to provide links to ISSA members to find discussions of specific recommendations in all these security areas.

January 2021

All ISSA members are invited to alert the Cyber Risk Working Group of additional best practices and frameworks they feel are relevant to the expanded remote working environment ISSA members are operating in by sending information to colin.parry.issa@six-group.com.

Enhanced Risks in the COVID-19 Environment

In 2018, ISSA issued a white paper entitled «Cyber Security Risk Management in Securities Services» where it outlined 9 areas that should form the foundation of all financial institutions' cyber risk mitigation programs. All these areas are applicable to the protection of institutions' remote access platforms that have been expanded for much broader usage during the COVID-19 pandemic. Those program areas include:

- Threat Intelligence and Information Sharing
- Vulnerability/Patch Management
- Penetration Testing
- Security Architecture
- Identify and Access Management (IAM)
- Intrusion Protection Management
- Security Awareness, Training, and Education
- Independent Reconciliation
- Third Party Risk Management

The adaptation of the work environment in response to the pandemic has also changed the threat landscape. Financial institutions now have a large percentage of staff working remotely, have adopted operational and oversight processes and required the implementation of new collaborative tools to foster an integrated workforce. It is important to understand how these changes have impacted and will continue to impact financial institutions' operations and those cyber risks that financial institutions should be aware of when reviewing the overall operational impacts.

Phishing

Phishing represents the most common injection vector for malware (ransomware) into corporate networks. By tricking an individual to click on a malicious link, a threat actor can gain an initial foothold into the network and, from there, expand access across other systems and information (also known as lateral movement). The public concern with COVID-19, combined with the global nature of its impacts, increases the probability that individuals will click on links that look to provide information about the pandemic or provide a means to donate to charities assisting those in need. While many organizations have seen little to no uptick in the number of phishing attempts, the percentage of these emails which are rooted in the COVID-19 pandemic (e.g., COVID heat maps, information sites, donations) make up the overwhelming majority when compared to other click bait. The shift to remote working has placed additional pressures on employees. Childcare, home schooling, and other stresses decrease the attention to details and may increase the likelihood that employees click these links.

To address these risks, financial institutions should consider referring employees to reputable sites where information regarding the pandemic may be found. This could include providing access to these links through an internal site. Financial institutions may also want to adjust their phishing training courses to encourage the reporting of phishing attempts and the prompt reporting of accidental clicks on these links. These actions provide information security teams with additional time to response or recover from these events.

In the current situation, employees should be suspicious of any emails asking them to check or renew their credentials even if they seem to come from a trusted source. Employees should try to verify the authenticity of the request through other means, and not click on suspicious links or open any suspicious attachments.

Institutions should inform employees to be very suspicious of mails from people they do not know - especially if the emails ask to connect to links or open files. If an employee is in doubt the advice should be to phone the institution's security officer.

Mails that create an image of urgency or severe consequences are key candidates for phishing - in these cases it is recommended that institutions ask their employees to always verify via an external channel before complying. This skepticism should extend to mails sent from people the employees know, but asking for unusual things, and should be verified by phone if possible before taking action.

Remote Working

Prior to the pandemic, most financial institutions had provided remote working capabilities for a subset of their employees. The pandemic shifted large portions of the workforce to remote working solutions, causing financial institutions to enhance or increase remote working facilities. The workforce displacement created by the COVID-19 pandemic has increased financial institution's potential attack surface area through the extension of the computing environment to numerous home networks. Furthermore, corporate networks have increased exposure to these home networks and to other devices that may be connected to these home networks (e.g., Internet of Things (IoTs)). In addition to this exposure, security teams have less access to these devices (including for privacy reasons), which may decrease the effectiveness of some security programs designed to protect these employees.

Further, an individual's own behaviour affects the network security. While many institutions have implemented processes that do not allow access through home networks that have not been updated with the most current security patches or brought up to minimum requirements set by the institution, not all institutions have implemented these measures. In these circumstances, only the individual knows whether the home networks have been patched to the latest standards, or that their home networks adhere to best practices (e.g., changing the default passwords and settings on wireless routers). Additionally not all devices can be updated by the user themselves such as IoT devices for example. In this case the manufacturer's approach to security and patching is inherited.

Remote working will continue to be a part of an organization's network access solution. Therefore, financial institutions may want to consider providing their workforce with instructions on how to protect their home networks and devices from malicious actors and/or best practices for responsible device use.

Endpoint Devices

Many security programs and services have preventative and detective controls that operate independently from employee engagement. Vulnerability Management, intrusion detection and prevention, anti-virus/Antimalware and other security services require devices to be on or connected to the corporate environment for optimal control effectiveness. In a remote working environment, where devices do not have a persistent connection to the corporate network, vulnerability and patch management programs may need to be altered to identify and repair security vulnerabilities. The shift of the network perimeter to home networks may also lower the effectiveness of intrusion detection systems as these devices are not connected to an employee's home network. For example, employees may work different hours or from different locations changing expected patterns of network traffic to the computing environment. Endpoint security may require greater user involvement for the enforcement of controls. As a result, financial institutions may also consider providing guidance to their workforce to protect the devices (e.g., modems, wireless routers, WLAN, VPN) on their home networks and free / public wireless networks when not at their home location.

Financial institutions may also be providing access to critical applications that were normally only accessible from on-premises networks. Financial institutions may consider implementing strong user authentication to remotely access these applications. Additionally, financial institutions may consider increasing the testing and monitoring frequency of their external network environment to align with the increased need for resilience of this infrastructure.

Third Party / Supply Chain

The pandemic highlighted potential weaknesses in the resilience of third party and supply chain services. As an example, the increased demand for IT remote access devices and systems (e.g., laptops, VPN concentrators) created elongated timeframes for the delivery of these devices and systems. Financial institutions have and continue to focus on the resilience of their operations to numerous hazards including pandemics. Further, financial institutions are required by rule to test their financial and operational resilience to business-impacting events. While there are third parties that are held to these same standards, there are others where these requirements may not exist. As a result, financial institutions must develop strategies to understand the resilience of these third parties and the strength of the supply chain through pandemic and other operational hazards (e.g., cyber).

Third party concentration risk may be increased significantly across the industry and within financial institutions due to the reliance on the same single vendor of tokens for dual factor authentication and the potential use of the same

Internet Service Provider (ISP) at home by the majority of employees in each geographic location. As a result, financial institutions may consider the impacts of an ISP outage, the potential impact to operations and any mitigating options that may be available.

Short- to Long-term Solutions

Business continuity solutions that were designed to be short-term workarounds may need to be revisited to become long-term solutions. For example, printing from home and vendor / contractor remote access may not have been acceptable for some financial institutions prior to the pandemic. Given that these activities may be required for an extended duration, financial institutions may want to consider additional controls or safeguards to protect their information. In addition, they should reinforce policies for responding to security incidents and personal data breaches are in place and that staff is appropriately informed of them.

The workforce displacement created by the pandemic has created an environment where business areas have had to adopt how they deliver services. In addition, the risk and oversight functions, accustomed to working closely with business operations in an office setting, may not be in sync with how the business operations have shifted to accommodate this new normal. Therefore, business operations may need to review and update their documented business processes. Concurrently, risk and control functions may need to evaluate and update testing procedures to align with the new business controls or new guidance and best practices.

Electronic Signatures

The global pandemic has changed the way that the financial services sector interacts with its clients and counterparties. Activities that have traditionally been conducted in person must now have an efficient and secure electronic option for execution. Securities servicers often require signatures from their clients and counterparties to execute instructions from these entities. It is imperative that both the client and counterparty together with the securities servicer can trust the authenticity of the signature and have assurance that the document has not been accidentally or maliciously altered once the signature has been provided. One method that securities servicers may consider for completing this function is the use of an electronic signature. The most secure form of an electronic signature is a digital signature. While both electronic and digital signatures offer security features linking a signature to a document, electronic signatures do not always have the secure coding provided by digital signatures and depend on the vendor implementation of the electronic signature framework for its security features. Digital signatures embed the security features into the document which allows all parties to determine if a signed document has been altered.

Securities servicers should understand both the type of signature and security features offered by the vendor when selecting a provider for this service. In addition, security servicers should provide directions, in writing, to all clients and counterparties regarding their criteria for accepting any form of electronic signature and for which document types they will be accepted.

Collaboration Tools

The removal of the workforce from a corporate office setting created an environment where expansion of collaboration tools is required to enhance productivity. In-person meetings facilitate opportunities for employees to work together towards a common goal. An office setting also provides and fosters a corporate culture and defines organizational norms. To foster closer working relationships and maintain the corporate culture, many financial institutions introduced video conferencing and other collaborative tools. Each of these applications comes with its own set of security features. Financial institutions must evaluate these applications for their computing environment and business need. The Box below provides a list of questions that financial institutions may consider when determining the best solution for their environment.

Considerations for Video Conferencing/Collaboration Tools

The workforce displacement created by the COVID-19 pandemic has increased the usage of remote working environments and underscored the criticality of utilizing, at least one, video conferencing and collaboration tool platform(s) to facilitate internal meetings, workshops, client meetings, industry meetings, virtual events and conferences. Each financial institution must balance the benefits and costs and risks of using multiple platforms to provide optimum coverage and flexibility for its staff. Depending on the current IT and security environments implemented by each financial institution, institutions may come to different conclusions on the selection of any video/collaboration tool. When considering each candidate platform from a business need and risk perspective, financial institutions may wish to consider each in terms of the use cases they have and the security features those use cases require versus the features resident in the tools and the features the financial institution will need to implement. The following questions may be helpful in this analysis:

1. Is the use case meeting or event only for internal users or a mix of both internal and external participants?
2. Have your legal and compliance functions required that in-meeting chats and recordings be archived?
3. Does the platform allow file sharing in the meeting to go through outbound data loss prevention or inbound malicious content checking?
4. Can the platform allow the meeting to be encrypted end-to-end to ensure internet eavesdropping is not possible?
5. Does the platform allow for both static meeting IDs and dynamically assigned meeting IDs?
6. Are additional meeting passcodes provided for if meeting invitations can be forwarded to any internal or external emails?
7. Does the platform allow for all participants being muted and video turned off when entering a meeting?
8. Does the platform support digital white-boarding while still meeting the same eDiscovery requirements as in-meeting chats?
9. Do your legal and compliance functions require that meeting recordings have speech-to-text transcripts to comply with eDiscovery and if so, does the platform support that?
10. Are different types of meetings like webinars and training classes categorized at the same level as other more confidential meetings such as board meetings?
11. What registration level requirements should participants have to join these meetings?
12. Is your intent to allow or prevent the sharing of the virtual meeting URLs on social media or other public channels?
13. Can phone dial-in only users be authenticated sufficiently to ensure they are an authorized participant?
14. Does this platform perform well under a Virtual Desktop Infrastructure (VDI) user scenario?
15. Can Single-sign on be deployed for centralized control of user access?
16. As a cloud provided application, does a disaster recovery scenario of a total internet outage require an on-premises workaround?

Once a financial institution determines which platforms it will support, it should give staff guidance on securely using those platforms and the most appropriate use cases for each as well as guidance on how to participate in industry business and events that are taking place on platforms not supported by the institution.

Existing Cyber Risk Frameworks

Along with Links to Sections Specifically About Remote Working Security Practices

The 2018 ISSA Paper identified a set of jurisdictional mandatory policies and / or regulations, as well as several existing cyber-related advisory frameworks / guidelines that can be seen as market «best practice». The ISSA Cyber Risk Working Group examined some of these frameworks, looking to uncover their emphasis on securing remote working platforms and any new guidance they have issued since the start of the pandemic. Below is what the Working Group found. It should be stressed that there are many frameworks and the one that works best for any one financial institution may be different than for other institutions based on their own architectures and security frameworks.

National Institute of Standards and Technology (NIST)

NIST's guidance relevant to remote working platforms is available here:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

Earlier this year, NIST issued a bulletin on their 2016 guidance, stressing that it is all still relevant for today:
https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2020-03.pdf

The NIST recommendations focus on four areas:

- Enterprise Telework and Remote Access Security
- Remote Access Solution Security
- Telework Client Device Security
- Telework and Remote Access Life Cycle

Plus, NIST has a Blog on securing virtual meetings, telework basics…
https://www.nist.gov/blogs/cybersecurity-insights/preventing-eavesdropping-and-protecting-privacy-virtual-meetings
https://www.nist.gov/blogs/cybersecurity-insights/telework-security-basics

Cybersecurity Infrastructure and Security Agency (CISA)

The CISA guidance has been updated based on learnings from the COVID expansion of remote working and includes:

- General Telework Guidance
- VPN-Related Guidance
- Video Conferencing Guidance
- Wireless Related Guidance

https://www.cisa.gov/national-cyber-security-awareness-month
https://us-cert.cisa.gov/ncas/alerts/aa20-073a
https://www.cisa.gov/telework

The US National Security Agency (NSA)

The NSA has issued two guidance documents and a recent article:
Compromised Personal Network Indicators and Mitigations
Performing Out-of-Band Network Management
https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2163484/working-from-home-select-and-use-collaboration-services-more-securely/

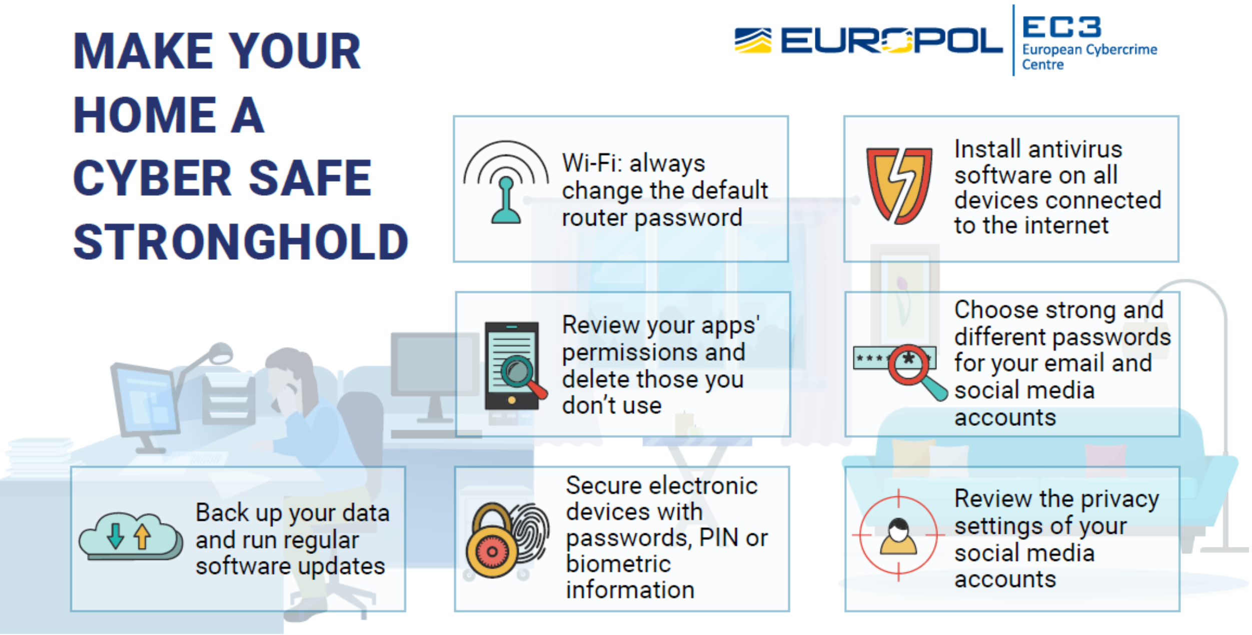
The UK National Cyber Security Center (NSCC) (small- and medium-size businesses)

https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/home-and-mobile-working
https://www.ncsc.gov.uk/guidance/home-working
https://www.ncsc.gov.uk/blog-post/secure-home-working-personal-it

Europol

https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold

COVID-19 Updates | Activities & Services | Europol (europa.eu)



MAKE YOUR HOME A CYBER SAFE STRONGHOLD

EUROPOL | EC3 European Cybercrime Centre

Wi-Fi: always change the default router password

Install antivirus software on all devices connected to the internet

Review your apps' permissions and delete those you don't use

Choose strong and different passwords for your email and social media accounts

Back up your data and run regular software updates

Secure electronic devices with passwords, PIN or biometric information

Review the privacy settings of your social media accounts

Source: Europol

Switzerland: National Cyber Security Centre (NCSC)

Entry page for all Homepage (admin.ch)
Home Office - Secure use of remote access (admin.ch)

Switzerland: REPORTING AND ANALYSIS CENTRE FOR INFORMATION ASSURANCE **MELANI**
Semi-annual report 2020/1 (admin.ch) In this report key topic is COVID-19

Remote working guidance from MELANI,Switzerland:
Home Office: Securing Remote Access 24.03.2020 - Based on the increased use of Remote Access solutions, we would like to remind you about a few best practices in order to minimize the risk associated with these technologies. We believe that the risks are increasing with the number of Remote Accesses into an organizations network. Attackers know about the current situation and may try to use different ways of getting access into an organization's network.

Australasia

COVID-19: Cyber security tips when working from home
https://www.cyber.gov.au/acsc/view-all-content/advisories/covid-19-cyber-security-tips-when-working-home

Staying secure while working from home
https://www.cert.govt.nz/individuals/guides/working-remotely/

Information Security Forum (ISF)

The ISF is a leading authority on cyber, information security and risk management.
Their research, practical tools and guidance address current topics and are used by their Members to overcome the wide-ranging security challenges that impact their business today.
Information Security Forum
COVID-19 Recovery Resource Pack - Information Security Forum

For cyber professionals and risk management leaders, as with other business functions, a significant challenge lies ahead. Not only do security professionals have to join the organisational fight against the consequences of the coronavirus, they must adapt to a complex, volatile and unpredictable environment, possibly with limited resources.

The ISF COVID-19 Recovery Resource Pack has been put together to help cyber professionals adapt to the challenges ahead and manage the surrounding risks.

Gitlab

Gitlab is a technology company headquartered in the U.S. with about 1,300 employees, located in more than 65 countries. It was founded in 2014 as a 100% remote company with no offices and they have built up a Guide to All-Remote Working that they share publicly via their website. While ISSA does not endorse any individual company's security practices, ISSA members may find the topics addressed in Gitlab's Guide to All-Remote useful to reference when looking to enhance their own remote working security practices.
https://about.gitlab.com/company/culture/all-remote/guide/

Earlier this year, Gitlab updated the Guide's section on security of the remote environment:
https://about.gitlab.com/handbook/security/

Gitlab is Cloud native, all-remote native and they have not gone down the Corporate VPN/Firewalls/secured perimeter route. Instead, their strategy is "Zero Trust" Networking, looking to grant access to only authenticated individuals and authenticated devices that are seen as being operated in a secure fashion, whether that device is at an employee's home, or anywhere else. They discuss the objectives and the implementation steps and challenges and where they are in a series of blogs. ISSA is unsure whether this type of approach to securing remote access is an emerging best practice or not, but the Working Group will follow the news on it to determine if it begins to be implemented by financial institutions.

Gitlab's presentation on Zero Trust: https://youtu.be/DrPiCBtaydM

Gitlab references Google' similar practices. Google's White Paper on their own implementation of a new approach to enterprise security can be found here:
https://storage.googleapis.com/pub-tools-public-publication-data/pdf/43231.pdf

ISSA Working Group members have limited practical experience with Zero Trust. That said, our conversations with other industry participants suggest that there has been significant discussion of Zero Trust over the past several years, with some progress towards adoption. The pandemic has accelerated this trend as the significantly larger remote-working workforce poses a higher security risk.

It is unclear whether the expected «New Normal» following the pandemic will result in «Zero Trust» replacing VPNs and associated security methods in the future. The ISSA Cyber Risk Working Group will follow this trend closely and advise the ISSA membership of its findings.