MONETARY AND CAPITAL MARKETS

Special Series on COVID-19

The Special Series notes are produced by IMF experts to help members address the economic effects of COVID-19. The views expressed in these notes are those of the author(s) and do not necessarily represent the views of the IMF, its Executive Board, or IMF management.

Cybersecurity of Remote Work During the Pandemic[1]

Due to the COVID-19 pandemic, many financial sector firms and authorities have moved to teleworking arrangements that are based on remote access to systems and data that may be critical. Given the widespread shift to working remotely for a prolonged time and the inevitable vulnerabilities in this process, new and more cyberattacks are expected to emerge. Firms should consider implementing strong remote access security controls if they have not already done so. Similarly, if not already in place, regulatory authorities should consider issuing additional guidance, based on international technical standards and good practice.

I. POTENTIAL INCREASED SOURCES OF VULNERABILITY

Most financial sector firms have already been using remote access facilities, however, installed capacities may not have been enough to support most of the workforce simultaneously, which increases potential security risks. IT departments are under pressure to upgrade capacities fast and this results in changing or replacing existing systems with little time to do thorough security tests. Vulnerabilities in the remote access infrastructure and access protocols may remain undetected and can be exploited in cyberattacks.

Cloud technologies are increasingly implemented and used to quickly deal with higher capacity needs. Under time and resource pressures, inherent security risks coming with the usage of cloud services might not have been properly assessed and existing controls might not be fully effective in the new environments. This risk is also present using cloud service providers that are generally regarded as providing secure infrastructure, because user organizations themselves are always responsible for certain aspects of cloud security (such as setting up proper access controls).

Employees unfamiliar with working remotely and under stress caused by the pandemic, can become easy targets of phishing and social engineering attacks. Over the past few weeks there has been an increase in cyberattacks designed to trigger a response by exploiting our natural sensitivity to COVID-19 related

[1] For more information, country authorities may contact Nigel Jenkinson (njenkinson@IMF.org), Division Chief of the Financial Supervision and Regulation Division of the Monetary and Capital Markets Department (MCMFR).

information. Examples include clicking malicious links and downloading malware infected attachments or applications.

Insecure endpoints and weak remote access authentication are two main elements that increase the risk of such attacks succeeding. Examples of insecure endpoints are notebooks or other mobile devices without the latest security patches installed. Password based authentication without a second factor is considered weak in the context of remote access. However, enforcing strong password requirements remain an important issue to be addressed.

Functions dealing with critical systems and data that are normally not allowed to be conducted off premises, for example treasury operations, might need to be carried out remotely during the pandemic. Existing controls might not be enough to protect critical functions, system and data.

Technical and policy measures that focus on information security are key in mitigating the cybersecurity risks of remote access. While not specific to remote access, strict information security policies (including data access control and extensive logging and monitoring policies) underpin remote access security. Some firms have had weaknesses in the implementation of such policies and are therefore more likely to be successfully attacked during the pandemic.

II. RECOMMENDATIONS

Authorities and firms should quickly and effectively implement good practices and international technical standards applicable for secure remote working, if these were not already in place. While some existing technical standards specifically address controls for remote working (e.g. NIST 800-46 Rev 2 or BSI IT-Grundschutz Compendium), others describe generic controls that are relevant for working remotely (such as COBIT 2019[2], or the ISO 27000 series). Examples of key topics that should be prioritized by firms and authorities are: (i) robust authentication of users and devices[3] and strong encryption methods; (ii) secure remote access devices; and (iii) network security monitoring.

Remote access services and user profiles should be only activated when required. Where no business need exists, remote access should be disabled, to reduce the attack surface.

Cloud usage should be based on detailed risk assessments. Based on these risk assessments, considering the criticality of systems and data transferred to the cloud, effective security control mechanisms should be implemented making full use of the cloud facilities that support this (such as asset access controls, identity and access management, and logging and monitoring).

Teleconferences should be run on vetted platforms and protected from unauthorized access. As a much higher amount of sensitive information is transmitted and shared over teleconferencing facilities, doing a vulnerability assessment before large scale deployment is crucial for proper information security. In addition, teleconference participants should be authenticated by both technical and procedural means, for example using PINs and reconciling actual participants with the corresponding invite.

Additional awareness campaigns on cybersecurity should be launched for all employees. As every system is only as strong as its weakest link, all employees need to understand the increased threat level

[2] For example: controls BAI09.02, DSS05.02, DSS05.03 and DSS05.06

[3] In terms of user authentication, using two factors is strongly recommended. Devices at both ends of the connection should be authenticated, for example using digital certificates.

stemming from phishing and social media campaigns during the pandemic. Helpdesks should quickly support users in case of suspected security incidents.

Robust controls over configurations at both ends of the remote connection should be implemented to prevent potential malicious use. For example, employees should not have administration rights on firm-owned notebooks,[4] security hardened configurations and up-to-date endpoint security solutions should be in place, connection security parameters should be set according to good practices and should be locked, and the corporate remote access infrastructure should be tightly controlled. Security scans of devices establishing a remote connection are good practice and remote access should only be granted to compliant devices.

Firms should implement additional security controls for critical functions that are normally not allowed to work remotely. For example, users who perform such activities should only be able to connect using firm-owned and controlled devices that are fully patched and configured to a high level of security and sensitive data should not be allowed to be stored locally.[5]

Supervisors should reinforce the message that remote work increases cybersecurity risk, which must be addressed with strong controls. It is suggested that authorities issue further guidance that outlines the risk and references to existing relevant guidance (if there is one in place) and provides further detail if needed, for example along the lines of this note.[6] Supervisors should be aware that if there is no ex ante guidance and the cybersecurity risk management practices of firms are not sufficiently mature, then several key controls may be missing or ineffective and improving the situation will be difficult under the current circumstances. In this case, strengthening of management controls and oversight of employee activities, and awareness campaigns can try to compensate to an extent.

[4] On privately owned computers that cannot be appropriately controlled by the firm, for example in a Bring Your Own Device (BYOD) setup, it is strongly recommended that employees work under unprivileged user accounts.

[5] Mandatory use of appropriately configured terminal servers, or jump servers are examples to effectively restrict local data storage.

[6] See the IMF Departmental Paper “Cybersecurity Risk Supervision” for a broader discussion of recommended supervisory practices. Accessible at https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/23/Cybersecurity-Risk-Supervision-46238.