Cyber liability

Cybersecurity risks to consider when the workforce returns to work

The relaxation of stay-at-home orders and work restrictions will result in additional cybersecurity concerns which arise from the rapid reintegration of remote workers returning to the office. These risks are likely to impact even those organizations that were prepared for the switch to remote working. We have categorized these cybersecurity risks into four broad categories: personal devices, unapproved personal applications, unattended systems, and human error. Each category represents a vector for the introduction of malware and/or sensitive data loss from your organization.

Use of personal devices

The rapid switch to working remotely has meant an increased reliance on personal devices for work use. Additionally, the impact that COVID-19 has had on international production and shipping has made procuring new devices for work use even more difficult, necessitating business use of personal devices. Personal devices include not just personal phones and computers, but also USB storage devices and other peripheral devices which are able to store or transmit data. If compromised by hackers and then attached to an organization's infrastructure, these devices represent a potential vector to introduce malware into an enterprise network upon a return to the office and to so wreak havoc.

In an ideal world, personal devices would not be brought in as infrastructure upon returning to work. Any work that has been performed on personal devices would be sanitized and migrated onto organization-owned infrastructure. However, as this may not always be feasible, organizations should plan for how personal devices can be integrated into the workflow as needed. Options include segregated and monitored networks specifically for personal devices and commercially available solutions for securing mobile, laptop, and desktop devices.

Unapproved personal applications

Remote work can create an overlap between personal and work life. It is often difficult for workers to keep from using work devices for personal use. This presents the issue of unapproved and unvetted applications operating on work hardware. Such applications include (but are not limited to) teleconferencing software, personal cloud storage applications, printer or other hardware drivers, and video games. Additionally, the use of social media and general internet browsing on work-issued devices can increase the exposure to phishing and malware attacks. These applications present similar risks to personal devices but may be more problematic as they are present on devices which are likely to be considered trusted or secure by infrastructure standards.

Organizations should have a plan in place to identify and secure devices that were used while working remotely. Inventory should be updated before returning to work as well as during the process. Securing devices should involve identifying and fixing misconfigurations, patching, removing assets that shouldn't be online, malware scanning/cleaning, and if possible restoring devices from a known, good backup. All of this should take place before connections are made to any trusted internal portions of a company network.

If systems were left online but unattended or unmonitored, they may have been unwittingly compromised by hackers who are waiting for a company's return to work before deploying malware in the company network.

Reintroduction of unattended systems

From an IT perspective, another concern is the reintroduction of systems and services that were offline or unattended during the work-from-home period. Organizations may have ceased some or all IT functions during this period of remote work. Those organizations which had to shut down completely may have also taken pieces of IT infrastructure offline for the duration. If this resulted in missed security patches, these systems may be newly vulnerable upon their reintroduction. Additionally, if systems were left online but unattended or unmonitored, they may have been unwittingly compromised by hackers who are waiting for a company's return to work before deploying malware in the company network.

Before returning to work, any critical systems that were unmonitored should be completely scanned with an antivirus tool to ensure that no infections have taken place and logging should be checked for any evidence of intrusion. Security patches and configurations should be verified across all machines, especially those which were off or disconnected from infrastructure during the remote work period.

Human error

The opportunity to return to some degree of normalcy coupled with a desire to recoup losses sustained as a result of the pandemic may result in human errors during employees' return to the office. Human error can take the form of falling victim to phishing, unwittingly violating security practices, forgetting processes that have not been performed in months, accidental information leaking, etc. During this period, as people return to the workplace with the vulnerable devices we mentioned earlier, there will likely be uncertainty about policy and practices regarding personal devices and applications in the workplace. Additionally, phishing attacks under the pretence of IT or financial services may be more persuasive than usual and the pressures of returning to standard operations may encourage complacency. Physical security practices must also be considered, as employees are likely to be both out of practice and less prepared to deal with social engineering after a period of isolation.

Phishing education programs and training should be restarted. The utilization of phishing tests is useful to gather statistics on the risk of this breach method. Monitoring and continuous adjustments of email filtering rules should remain a priority. Additionally, training specific to the organization's physical security concerns should be conducted upon the company-wide return to work.

Additional recommendations

Some additional measures organizations can take to secure themselves are:

Establish visibility
Organizations should map out and understand their external digital footprint. This helps in assessing where they could have been and could still be vulnerable to attack. This includes threat intelligence work, which can be conducted internally or outsourced. A sweep of the surface, deep, and dark web may produce indications of company exposure or heightened threat actor interest.

Insurance protection
The COVID-19 pandemic has already hit many businesses financially, slowing down operations and impacting productivity. The last thing a company needs upon returning to normal operations is to be impacted by a cyber incident. Cyber insurance can cover downtime and identify the technical and legal expertise needed to mitigate and remediate intrusions.

Protect executives
High-risk individuals should be trained appropriately for the new set of risks they face. In addition, their digital footprints should be assessed and monitored to make it more difficult for them to be targeted. If compromised, their high privilege accounts make for more severe compromise.

Insider threat
The insider threat concern will be pressing, as employees may have conducted work outside organization networks for months. Risk mitigation programs should be reviewed and internal monitoring should include checks for data leaks.

AXA XL insureds have access to S-RM, one of our cyber security partners, who are able to advise on all things cyber security. S-RM can facilitate CISO workshops with your information security leadership to understand your organization's environment and provide expert guidance on cyber security plans. AXA XL insureds also have access to S-RM's Phishing Testing capability, which enables organizations to gauge their employees' cybersecurity awareness, as well as Incident Response Workshops and Plan Reviews, to ensure that your organization has a plan in place in the event of a cyber attack.

To learn more, contact your AXA XL Cyber underwriter.

S-RM is a global consultancy that helps clients manage regulatory, reputational and operational risks.

6450_05/2020