Cybersecurity

risks to consider when the workforce returns

towergate insurance

Cybersecurity risks to consider when the workforce returns

The relaxation of work restrictions will result in additional cybersecurity concerns which arise from the rapid reintegration of remote workers returning to the workplace. Whether in relation to personal devices, unapproved personal applications, unattended systems, or human error, each create the potential for malware and/or sensitive data loss. We explore each category in detail.

Use of personal devices

The rapid switch to working remotely has meant an increased reliance on personal devices for work use. If compromised and then attached to an organisation's infrastructure, these devices represent a potential path to introduce malware into an enterprise network upon a return to the workplace.

In an ideal world, personal devices would not be brought into the corporate infrastructure upon returning to work, with any work performed on personal devices sanitised and migrated onto the organisation owned infrastructure. However, this may not always be feasible, organisations should plan for how personal devices can be integrated safely; options include segregated and monitored networks specifically for personal devices and commercially available solutions for securing devices.

Unapproved personal applications

It is often difficult for workers to keep from using work devices for personal use and this presents the issue of unapproved and unvetted applications operating on work hardware, such as teleconferencing software, cloud storage applications, printer or other hardware drivers etc.

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.

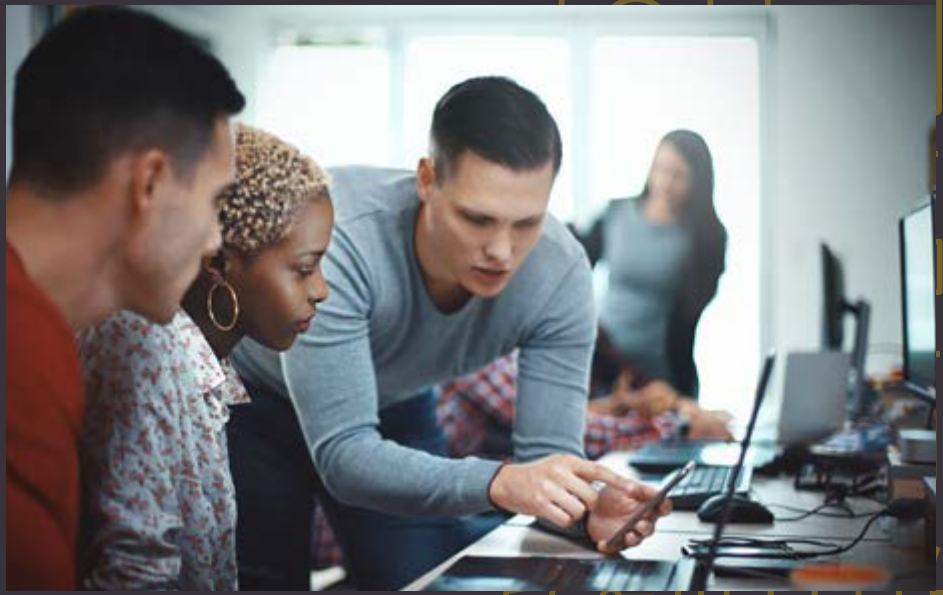
Organisations should have a plan in place to identify and secure devices that were used while working remotely. Inventory should be updated before returning to work

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 and practical, 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.

Reintroduction of unattended systems

Organisations may have ceased some or all IT functions during this period of remote work and those organisations 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.

Systems left online but unattended, 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

Human error still plays a leading role in the cyber vulnerability of an organisation and the opportunity to return to some degree of normality, coupled with a desire to recoup losses sustained as a result of the pandemic may result in increased human errors during the return to the workplace.

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, potentially with vulnerable devices, 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 utilisation 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 organisation's physical security concerns should be conducted upon the company-wide return to work.

RISK MANAGEMENT

Risk management and practical steps an organisation can take;

Establish visibility - organisations 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.

Protect executives - high-risk individuals or those with access to highly sensitive data, i.e. payroll/HR, should be trained appropriately and considered for enhanced security protection 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 organisation networks for months. Risk mitigation programs should be reviewed, and internal monitoring should include checks for data leaks.

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 costs, data breaches and their consequences, as well as providing the technical, forensic and legal expertise needed to mitigate and remediate intrusions.

Where cybercrime has occurred, Cyber insurance can cover such losses following fraud or social engineering, including extortion and the fraudulent transfer of funds.

Cyber insurance can also cover liabilities arising from a data breach or potential data breach including forensic and technical costs as well as Public Relations/Crisis Management support and credit monitoring of those affected by the breach.

For more information, call us on **01438 735251** or email **new.pro.liability@towergate.co.uk**

towergate insurance