Rise in working from home:

Cyber security implications and guidelines

Considering the COVID-19 crisis, many companies have hastily put together remote working plans without considering the cyber security implications and emerging risks. We have noticed an increase in cyber security breaches leading to data leakages and losses.

Are your systems secure enough? Analyze and take precautions before its too late.

Ever since the beginning of the pandemic, with the new norm of social distancing, we've seen an increase in companies reducing on the number of personnel that are required to go to the office premises and more people being required to work from home. Remote work requires remote access to business networks and comes with a range of cyber risks which need to be assessed and mitigated.

Organizations have to remain vigilant by assessing risks that working from home comes with. There is a need to look at the capacity and performance of networks and intensify employee awareness on the cyber risks they face.

What is remote working?

Remote working, also called telecommuting or work from home, is a working style that allows professionals to work outside of a traditional office environment. It is based on the concept that work does not need to be done in a specific place to be executed successfully.

Ever since the lockdown, there has been a spike on cyber-attacks targeting remote working employees, as hackers use coronavirus to prey on remote workers and stressed IT systems:

- More than one-third of senior technology executives surveyed by CNBC say that cybersecurity risks have increased as many of their employees work from home.
- Other experts say the true level of hacking risk is likely much higher than even these numbers indicate.
- About 85% of companies surveyed say at least 50% of their employees are now remote.

Remote working increases the cyber-attack surface of organisations as more business information are accessible remotely.

Organisations should consider the following counter measures as employees shift to remote working:

Update policies and procedures

It is likely that a number of organisations are not accustomed to the concept of having a large number of employees working remotely and may possibly not have in place the policies and procedures to support working remotely. It is crucial for organisations to have remote working and remote access policies and procedures. Policies should clearly stipulate use of mobile devices, use of home computers and devices to connect to the network, data privacy policies, inappropriate use of company resources by employees e.g. non-employees using an employees' work laptop. The policies and procedures should be communicated to all affected employees.

Assess capacity and performance of your network in handling increased remote connections

Major movie streaming service providers like Netflix had to reduce the quality of streamed movies to minimize impact on network performance due to increased viewership. The exponential increase in the number of employees working remotely may put a strain on the network. It is imperative for businesses to assess current network infrastructure capacity to handle the increased load, invest in extra capacity were necessary and continuously monitor performance of the network. If capacity and performance are not managed properly it may result in decreased network performance, frustrated employees and business disruption.

Ensure employees connect to your network through secure channels

Use of free Wi-fi to access company network increases the risk of online attacks. Employees should always use a virtual private network (VPN) when connecting remotely. VPN encrypts transmitted data to protect it from tampering and interception.

Ensure employees connect using stronger authentication mechanism

Implement additional layers of password protection. Encourage use of stronger and more complex passwords. Utilize Two-Factor Authentication (2FA). 2FA means the user provides two different authentication factors to verify themselves for system access. This makes it harder for cyber attackers to gain access to devices or accounts since only knowing their potential victim's password is not enough to get past the 2FA security control.

Ensure that the latest security updates and patches are applied regularly

Ensure that the latest security updates and patches are applied on your remote connection tools, on all computers and systems in your network. Updating software should be done regularly not only when there is a threat. In a blog post, Microsoft stressed the importance of doing this, writing: "As cybercriminals become more sophisticated, there is simply no way for customers to protect themselves against threats unless they update their systems."

Educate/train employees

Cybercriminals are already taking advantage of the outbreak to gain access to systems and personal information. Refresh your staff training on cyber hygiene and looking after personal and confidential information (e.g. education on phishing attacks, cooperation assistance during a data breach, not leaving physical documents lying around, taking care when working on laptops in public spaces). Create awareness among employees on emerging risks of connecting and working remotely. Educate employees on inappropriate use of company resources and ensure to be alert to avoid shoulder surfers.

Control computer usage

Restrict employee usage of computers to business use. Don't permit employees to use file sharing peer-to-peer websites or software applications, block access to inappropriate websites and prohibit use of unapproved software on company computers.

Secure all computers

Implement password protection and 'time-out' functions (requires re-login after periods of inactivity) for all computers. Train employees to never leave laptops or PDAs unattended. Restrict telecommuting to company owned computers. Configure your systems securely.

Stop unencrypted sensitive data transmission

Mandate encryption of all sensitive data transmissions. This includes data 'at rest', 'in use' and 'in motion'. Also consider encrypting email within your company if personal information is transmitted. Invest in Data Leakage Prevention (DLP) solutions. Configure email gateway to scan for malware, spam and spyware on all incoming and outgoing emails. Block accessing of malicious websites and downloading of suspicious files.

Manage use of Portable Media

Portable media, such as DVDs, CDs and USB "flash drives," are more susceptible to loss or theft. This can also include smartphones, MP3 players and other personal electronic devices with a hard drive that 'syncs' with a computer. Allow only encrypted data to be downloaded to portable storage devices. Invest in Mobile Device Management (MDM) solutions. Define and communicate Bring Your Own Device (BYOD) and use of noncompany issued equipment to access the organisation's network, systems and data policies and procedures

Technical support for remote workers

Organizations should invest in and implement remote access support tools that will enable Technical Support teams to assist employees remotely.

How can we help you?

At Grant Thornton Uganda we advise our clients on how to effectively manage cyber-risks, highlighting measures to secure and protect information stored and processed on computers. We help you build cyber resilience. Contact us to help you with below at very competitive fees:

- Systems Audit
- Vulnerability Assessment and Penetration Testing
- IT Policy Reviews and implementation
- End user IT Security training

Contact

Hemal Shah
Manager: Advisory
E hemal.shah@ug.gt.com

Ghazali Mohammed
Executive: Advisory
E ghazali.mohammed@ug.gt.com

Elison Twinomugisha
Assistant Executive: Advisory
E elison.twinomugisha@ug.gt.com

Grant Thornton

gtuganda.co.ug