Inside this Issue Vol 3: Issue 5/21

Have You Invested In Securing Remote-Working?

The new hybrid workforce is here which is a blended model where employees work both remotely and on company premises.

Is your remote working secure?

The coronavirus pandemic has changed the way people live, work, and communicate

Forensics & Cyber Security Newsletter

Your source of forensics, security and fraud insights

INTRODUCTION

The state of Cyber Security and COVID-19

The new hybrid workforce is here which is a blended model where employees work both remotely and on company premises.

In the old days, providing protection towards the IT infrastructure was done in two ways. That is physical security and logical security were implemented. But these measures have been challenged by the emergence of the new normal both remotely and at places of work. There is a noticeable laxity in the security measures provided for remote working environments. This is not the case for physical security at the organization.

Taking us back to when the pandemic first hit. Organizations were taken by surprise. Everyone was caught unaware and some firms took many days without resuming work. Only a few that had earlier adopted online solutions like financial institutions, manufacturing, and a few firms, were able to continue normal operations but remotely. Even those that had employees working remotely tasked their IT departments to quickly get their staff the basic IT equipment that they needed to work from home at that time. This was planned to take place for a short time till lockdown would be lifted and normal work resumed at company premises.

Now as we progress with the still existing crisis, IT departments are further tasked to come up with an approach that covers a permanent secure remote working connectivity to work-related resources.

—CYBER SECURITY

Is your remote working secure?

Remote-working (teleworking) is a must for several enterprises to survive in business today, following the COVID-19 pandemic crisis. There has been an unprecedented rise in virtual workplaces where employees are working from geographically dispersed areas, both within and outside standard business hours. Remote working has been fostered by various information and communication technologies that include e-mail, videoconferencing, teleconferencing, discussion groups, chat rooms, project management software, collaborative design tools, knowledge management systems, and message boards.

The coronavirus pandemic has changed the way people live, work, and communicate. Traditional leadership styles have been disrupted too. Every disruption brings opportunities and threats. Whereas Jane's employer was flexible and agile in providing the required capabilities in terms of a laptop and a smartphone to act as a modem to connect to the Internet from the home office, they forgot a critical element of security hygiene briefing for remote workers.

Working from home can give a false sense of security and comfort to the extent that some basic security procedures and practices are easily compromised than they would in a corporate and regularly monitored workplace.

> When Jane received a brand-new laptop and a smartphone as part of her home working package, she was elated. "Every crisis comes with a silver lining", she whispered to a friend as she packed her newly acquired gadgets as she moved her office to home.

> Security is the responsibility of the individual user. You must be careful whenever your computer or mobile device is connected to the Internet. As technology evolves, so do attack vectors and their sophistication. It is also important that you continuously keep updating yourself with new information in the cybersecurity landscape.

Because the threats against mobile computing devices are increasing, it is worth implementing these cybersecurity recommendations, selected from the NIST guide to telework and BYOD security;

1. **Limit access to the device.** Using some sort of authenticator (PIN, password, or biometrics e.g. owner's thumbprint) deters access to the employee's information and service by a person who gains unauthorized physical access to the device. It is also advisable to configure the devices to lock themselves automatically after an idle period.

2. **Disable networking capabilities except when needed.** Attackers can try to use necessary networking capabilities, such as IEEE 802.11, Bluetooth, and NFC on mobile devices to access information and services. You must disable each networking capability that is not being used.

3. **Keep devices updated.** Most mobile devices can be updated or patched to eliminate known security flaws. Follow the provided instructions to ensure that security updates are identified, acquired, and installed regularly, at least weekly.

4. **Encrypt data at rest.** If your device is stolen, some thieves may want to read the contents of the data on the device, and quite possibly use that data for criminal purposes. Most operating systems have their full-disk encryption mechanisms, and there are also numerous third-party applications such as VeraCrypt that provide similar capabilities. You should follow your organization's policy for encrypting all sensitive data when it is at rest on a device and removable media used by the device.

5. **Back up data on your devices.** Most organizations have policies for backing up data regularly. If data is being backed up remotely to a system at the organization, then the communications carrying that data should be encrypted and have their integrity verified. Similarly, if data is being backed up locally to removable media such as CDs or flash drives and hard drives, the backup should be protected as well as the original data is.

6. **Do not connect the device to an unknown charging station.** Many charging stations enable people to recharge their mobile devices through direct-wired connections between a device's USB interface and the charging station. Unfortunately, someone may have altered a charging station, such as one in a public area, so that it attempts to automatically gain unauthorized access to the data, applications, services, and other resources on mobile devices that attach to it.

FIX YOUR CYBER SECURITY GAPS FOR RESILIENCE

summit consulting
Strategy. Risk. Training.

Based on the results
of the security assessment

We will provide you with practical recommendations to harden your security and stop revenue leakages, protect your intellectual property and achieve the security objectives of confidentiality, integrity and non-repudiation

Phase 3: IT governance review / agreed upon procedures and revenue assurance to determine your cyber hygiene and revenue leakages, if any.

Phase 2: White box (internal) vulnerability assessment - to determine threats posed by insiders

Phase 1: Black box (external) vulnerability assessment - to determine threats posed by outsiders

Assess. Fix. Monitor.

Assess your current cybersecurity maturity in three phases

CONTACT US

Summit Consulting Ltd 4th Floor Ntinda Complex

Plot 33, Ntinda Road Opp St Luke Church P.O. Box 40292, Kampala, Uganda.

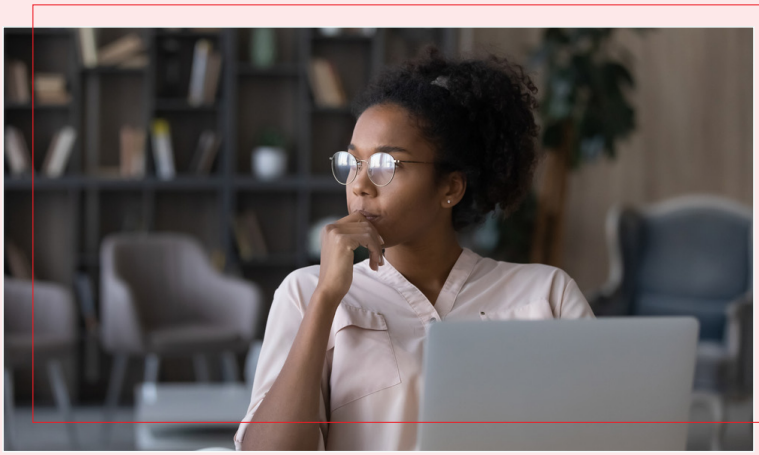
support@summitcl.com
+256(414) 231136

—CYBER SECURITY

Have you invested in Securing Remote-Working?

Personal devices connected to work-related resources

Taking us back to when the pandemic first hit. Organizations were taken by surprise. Everyone was caught unaware and some firms took many days without resuming work. Only a few that had earlier adopted online solutions like financial institutions, manufacturing, and a few firms, were able to continue normal operations but remotely.



> In the old days, providing protection towards the IT infrastructure was done in two ways. That is physical security and logical security were implemented. There is a noticeable laxity in the security measures provided for remote working environments. This is not the case for physical security at the organization.

Are organizations able to provide adequate security models to the new hybrid workforce?

According to the Cybersecurity Insiders report which points out a rapid adoption of unmanaged personal devices (BYOD) during remote working. Employees connect to work-related resources which increases the risk of uncontrolled access to intellectual property. This is in regard to the growing security threats such as malware and data theft.

While employees put into use their mobile handsets and other tech devices to accomplish their obligations, they contribute to the growth and expansion of remote working environments. This as well contributes to the challenges that IT departments face aligned to managing what resources these devices access.

As it is put in the summit Project Frontline of 2020, remote working and BYOD utilization has been experienced. The remote working was seen as a success where employee productivity and ease were seen to have hyped. However, this rapidly expanded the attacker surface to cybercriminals since there increased endpoint devices that are connected to work-related resources.

TO BE CONTINUED IN NOVEMBER 2021