PRACTICAL ACTIVITY 1 - SUBMITTED BY: ROSEMARY AGBOZO – CYBER SECURITY

INTRODUCTION

Using the CIA triad measures to decide precautions on information security issues that may arise from working from home. The focus when deciding the measures will be: Confidentiality (no unauthorized access), Integrity (no modification of data by unauthorized persons) and Availability (can be accessed anywhere and anytime by authorized persons).

IDENTIFYING THE HAZARDS

What are the risks/ vulnerabilities?

1. Hardware damage/access.

One threat to security is if the hardware the workers are using at home get damaged or stolen whiles sensitive data was being worked on. This is especially dangerous if the worker was working on their local device without using a cloud service which could automatically back-up for easy data recovery. If the device was stolen, the probability that the thief will have access to the data on the machine makes it a risk for sensitive data to be put out there. Also, if the worker is using a personal device, it may be available to all (friends, family and sometimes even strangers to the worker).

1. Phishing schemes. This is when hackers pose as a legitimate source (using via emails) to get the workers to provide personal login credentials or some sensitive information which can be in a long run used to hack into accounts, steal more sensitive data, perform identity fraud, and many others.
2. Password hacks. Some workers may have weak passwords which hackers can take advantage of as the workers start working from home. Also, workers who use repeated passwords, especially for both work and personal accounts can create an information security hazard/ risk.
3. File transfer attacks. Some files or data which may not be encrypted whiles in transit over a network may be hacked/ accessed. If workers keep sharing files over platforms that are not so secure, information could be compromised.
4. No updates to home router software. If workers/employees fail to perform security updates on their home router software, it may leave loopholes for attacks to be performed and their devices as well as company data may be compromised.

ASSETS AND STAKEHOLDERS

Who will be affected and how?

1. The company. Sensitive information about the company may become public information, which may affect the financial or economic value of the company. Also, attackers could use acquired data to blackmail the company into paying huge sums of money. The company may even lose reputation among their clients/ people who use their services.
2. The workers. The workers who have authorized access to the acquired data may feel the heat and will have to be accountable. In some instances, the worker who was the entry point may lose their job. The workers’ information may even become public.
3. The people who use the services that the company gives. Clients may lose trust in company if their personal data is revealed as a result of some attacks (a breach of privacy). Also, some clients may not be able to do their work if the attack on the company compromises the availability of the service.

PRECAUTIONS

After analyzing the risks, what are the precautions to be taken?

If possible, the company should provide work devices for the workers so they refrain from using personal devices that could be accessed by all. If not possible, workers should be warned to pay close attention on the people that access their devices.

Also, workers could be educated on how to identify phishing emails so as not to fall victim to phishing schemes and compromise company data. Workers should also be required to create strong passwords. A policy should be made that will ban workers from using personal passwords and repeated passwords for their work accounts. Also, they shouldn’t write passwords down randomly in the name of not remembering, they should, if necessary, use secure password storing applications.

The VPN used by workers should be enhanced by having a stronger authentication (multi-factor authentication). This should also not hinder the workers form accessing required data whenever and wherever.

Workers should compulsorily use secure email encryption platforms like Outlook when sending sensitive information via emails. Workers phones should be encrypted so sensitive voicemail information sent over phones are also protected. Also, workers should share files via secure file sharing platforms like Dropbox or OneDrive to better secure sensitive data, as these platforms provide end-to-end encryption.

Another precaution that can be taken is periodic security updates to the home router software to patch any security gaps before they are exploited by attackers. Also, routers with encryption should be enabled.