Chapter 1- BACKGROUND/INTRODUCTION

As different organizations and businesses scale-up technology adoption, security to the information and data are becoming a concern. The advancement in technology have risks to information security. The traditional security measures (such as the use of passwords) to protect access to data are becoming less effective. With their ineffectiveness, data and information is exposed to risks.

This made the use of multi-factor authentication such as two-factor authentication (2FA). With this approach, information and data is secured by a combination of two pieces of evidence to be granted access. It involves the use of the traditional piece of evidence (password) and a second measure such as one-time password, applications-based authentication, time-based authentication and biometric authentication.

21

The aim of this research is to outline the importance of implementing two-factor authentication mechanisms in organizations, businesses and learning institutions to ensure maximum security to data and information is provided. The improved security measure works towards guaranteeing information security.

The research will give a detailed analysis of the different types of two-factor authentications, what components they have and when one measure is more preferred over the other. Comparison will be done on the advantages and disadvantages of types of two-factor authentication. Also covers the type of attacks that are preventable through implementing a 2FA mechanism and the use of 2FA to prevent malware.

1.1 Background

Organizations need to implement correct cyber security measures to secure information and data. Security and privacy controls need to always be in place to guide employees and other stakeholders on how to handle data. Differentiating work and personal assets in the workplace and not using either work assets for personal use or using personal assets for work use is a key policy that should be observed. The NIST Cyber Security Framework and the NIST Security and Privacy Controls Catalog (NIST SP 800-53) outline a series of Information Security control that guides dos and don'ts (Gordon et al., 2020).

Among the NIST Security and Privacy Controls measures is Authentication. The NIST framework proposes the use of safe, secure and reliable security control measures to guarantee confidentiality, integrity and accessibility of information. A multi-factor authentication approach, to replace the traditional authentication (the use of password) has been recommended. With this, anyone to access data or information will need to correctly match more than one security piece to gain access. A two-factor authentication approach serves in achieving this goal.

1.1.1 Two-Factor Authentication (2FA). Two-factor authentication is a combination of two security pieces to give an extra layer of security used to make sure that people trying to gain access to an online account are who they say they are. While a user will be required to input a username and password (primary authentication measure), an additional security check will be required for them to gain access. This can be presented in the form of the following three categories. Includes answers to a set of security questions or a personal identification number (PIN). This could be a credit card, a smartphone, or a small hardware token that provides the

second security layer. The main goal is to ensure the person trying to access is the right person, this might include a biometric pattern of a fingerprint or a voiceprint.

The two-factor mechanism ensures that a compromise in one of the security components does not grant access but rather a combination of the two can only give access. Even if a password is compromised, one will need a fingerprint, a pattern or a smartphone to gain access.

1.1.2 Information Security. Information security, also referred to as InfoSec are processes, techniques and procedures created and implemented in a business/organization to prevent access, use, disclosure, disruption, modification, inspection, recording or destruction of information by unauthorized personnel, entities, systems and processes (Neil & Heather, 2006).

Confidentiality. seeks to ensure only authorized personnel, entities, systems and processes have access to information. Having a compromised password to a system or platform breaches the confidentiality of information security.

Integrity. covers how accurate and complete information/data is. Not updating records for students who have completed studies as graduated/competed but having such status remain as in-progress breaches the integrity aspect of InfoSec.

Availability. seeks to ensure information is available when needed. When authorized human resource staff is unable to access the contact information of a specific employee in an organization represents a breach of the availability aspect (Neil & Heather, 2006).

1.2 Problem Statement

Data breaches can lead to both financial and reputational damage in any organization, business, institution or individual. Additionally, unauthorized access can have far-reaching consequences to the affected parties. Password guessing and brute force are major attacks that cybercriminals use to gain unauthorized access.

This research proposes to evaluate the effectiveness of two-factor authentication in ensuring security to data, information and systems. After establishing the importance of two-factor authentication, the research will outline the cyber vulnerabilities which could be exploited by a cyber-criminal in absence of a two-factor authentication mechanism. The research will also outline the various types of two-factor authentication mechanisms and the advantages associated with each of them. While there are different cyber-attacks, the research will examine the various attacks which can be reduced through implementing two-factor authentication as a security measure.

1.3 Significance of the Research

The information from this research can be useful in determining how to implement two-factor authentication mechanisms in systems and other applications. Developers of social media platforms and other applications such as cloud services will need the research outcomes to establish the level at which two-factor authentication can be used to ensure data safety for customers and users of these platforms and services.

1.4 Research Questions

1. Which are the various available two-factor authentication measures?

2. Which cyber-attacks can be prevented through the implementation of two-factor authentication mechanisms?

3. How is implementing two-factor authentication key to promoting information security

4. In which areas do two-factor authentication measures are necessary to deter cyber-attacks?

1.5 Barriers and Issues

A barrier to the research will be comparing the different types of two-factor authentication measures to determine the level of effectiveness for each measure. While the overall effectiveness will be determined, the effectiveness for each type of two-factor authentication will be a challenge in the research. It might need more direct research on each type of 2FA measure to determine the measure's effectiveness.

An issue will also be around determining the drivers behind choosing one type of 2FA measure over another. While the availability of necessary tools could be a driving factor, in cases where all the types of 2FA measures can be used, understanding the choice of one over the other could be an issue.

CHAPTER 2 - REVIEW OF THE LITERATURE

Two-factor Authentication (2FA) is a multi-layer authentication method to mitigate risks of single factor sign-on (username and password only), such as password breaches and unauthorized access to trusted devices (Hwang et al. 2002). While research on 2FAhas primarily focused on improving the technological aspect of authentication and access control, it has become necessary to address existing weakness areas such as security and compatibility with the applications (Chayanam et al. 2012). The organization, business, usability and alignment still remain an area that needs to be more explored (Das et al. 2018a). As new authentication methods have been found more interesting to explore, previous studies also have intensively evaluated existing MFA on the aspect of speed and simplicity (user actions). The study revealed several loopholes in determining what could be established as MFA and what should not be considered as not.

In Stowell et al.'s work, "Designing and Evaluating mHealth Interventions for Vulnerable Populations: A Systematic Review", they begin their literature review by collecting a wide-range collection of papers related to mHealth (Kay et al. 2011) technology studies. Information such as demographics and types of studies conducted was gathered from each extracted paper. These findings are recorded, allowing them to understand the available literature thus paving way for future research. The study will provide a survey of available research that identifies the various types of two-factor authentication mechanisms and the cyber-attacks which can be reduced by employing the 2FA mechanism as a security measure. This will facilitate an informed approach in implementing two-factor authentication in applications and systems to ensure confidentiality, integrity and controlled availability.

2.1 Importance of Two-Factor Authentication

For a long time, security revolved around putting perimeter walls and strong gates, the new direction of information theft without any shot being fired the need to find ways of ensuring security to data and information. Unauthorized access may have extensive damages thus the need for controlled and possibly monitored access. Two-factor authentication plays a key role in ensuring access is only granted to the real owner of an account or a system.

Unlike single-factor authentication (traditional authentication) involving username and password, two-factor authentication offers a dynamic approach built from a variety of tools and policies. This guarantees comprehensive data and information protection without relying on one method of protection to access and use.

According to the Infosecurity group (Infosecurity, 2013) nine in every 10 passwords can be cracked within six hours. With advancements in technology, cybercriminals have sophisticated tools which can easily compromise the username and password authentication mechanism. Key logger attacks can copy a user's password thus giving access to unauthorized personnel. Such programs can be installed in a machine or another device without notice thus harvesting passwords to applications. A 2FA ensures even if the password has been compromised the actor will need to as well provide the second security piece which might be hard to get as it might be a biometric feature or a one-time password.

While the single-factor authentication can be shared in nature which is a risk, the two-factor authentication measures cannot be shared. To gain access to an account, the owner has to be present to provide the second piece of security. For instance, to access a bank application with

a 2FA measure of password and fingerprint, the owner has to scan his finger over the sensor to grant access. This greatly improves the security posture of such applications.

These are risks that can materialize when the two-factor authentication mechanism hasn't been used in granting access. They can occur in instances of single-factor authentication.

Password Theft. This is when an unwanted third party manages to steal or guess the password used to gain access to a platform of a system. It is majorly achieved through password guessing or brute force attacks. Actors can therefore steal or compromise information as they can log in to the target system without the user's knowledge.

Malware. This is a risk in which an unwanted piece of programming or software installs itself on a target system, causing unusual behavior without it being noticed. This occurs when a user hasn't set any authentication request to grant access to install software or a program. With 2FA implemented, no software will be installed without being noticed as access requests will be triggered.

Social Engineering. This is the method for attempting to deceive users into giving away sensitive details. Actors will use frequently visited websites such as social media platforms to deceive their targets in disclosing the information they are seeking.

Phishing Attacks. They rely on social engineering to achieve its goal by sending end user message or email which requests sensitive data, such as a password. While in some instances they may appear and look like official communication, they disguise to trick targets in disclosing this information which they use to gain unauthorized access. 2FA mechanism can prevent this form of attack as even if social engineering is used to falsely acquire the password, the second piece of security will be required.

CHAPTER 3 – METHODOLOGY

The research design is the overall strategy that is used to integrate the different components of a study in a readable and logical way, thereby, ensuring effective address of the research problem, it constitutes the blueprint for the collection, measurement, and analysis of data (Creswell, 2012). Literature analysis with the key source of data through the research. Journals and other publications will be studied to supplement the literature analysis. Data will be collected using literary analysis, reviews of relevant journals and publications touching both on cyber security space and Internet of Things adoption.

CHAPTER FOUR - ANALYSIS AND FINDINGS

4.1 Analysis

This systematic application of statistical and logical techniques to describe the data scope, modularize the data structure, condense the data representation, illustrate via images, tables, and graphs, and evaluate statistical inclinations, probability data, and derive meaningful conclusions. Establish how two-factor authentications are effective in securing information, data and systems. Data were collected mainly from reviewing the literature, journals and related publications. After analyzing the data tried to find answers to the research questions formulated at the beginning of the research.

4.2 Findings

Upon analysis, unauthorized access was found to be a big threat in organizations, businesses and even individual setup (Preece, 2016). Security was found to put businesses off adopting emerging technologies such as cloud computing and the Internet of Things (IoT). This is partly because many organizations and individuals have not adopted 2FA but rather still use single-factor authentication to access applications and systems.

Up to 9 in every 10 respondents in a survey of 170, IoT industry leaders believe unauthorized access is the barrier to IoT adoption. Two-thirds of them stated that implementing 2FA is their top short-term priority thus showing not much concern and resources channeled towards cyber security within IoT environments (O'Halloran, 2020).

4.3 Types of Two-Factor Authentication

4.3.1. One-Time password. This is one of the common types of two-factor authentication measures. In every access request, a password is generated to a present phone number or email. Only a person with access to the email or phone number set to receive the one-time password can therefore complete the second piece of security. By doing so, it ensures even if a hacker successfully guesses the password, they will need access to a phone or email to gain access. A notable advantage to this type of 2FA is that it is an easier option to implement since many people have an SMS-capable phone number and it doesn't require installing an app. A disadvantage associated with one-time passwords is that while some people may not be comfortable giving out their phone numbers, a close person can get short access to the phone when trying to gain unauthorized access so as to redeem the code delivered to the phone.

4.3.2. App-Based Authentication. This is a phone-based 2FA option that uses an application that generates codes locally based on a secret key. Google or Microsoft authenticator are a few common applications of app-based authentication. Just like the one-time password, to gain access one will need to input the most recent code in addition to matching the correct username and password. The phone in which the app is installed doesn't need to be connected to a mobile network thus allowing it to grant access in any part. Losing the phone can however lead to losing the app unless printed backup codes or a saved copy of the original QR code.

4.3.3. Biometric Authentication. Involves using some part of physical makeup to authenticate. Common forms of biometrics used to implement this type of authentication include fingerprints, iris scans, facial scans. The user will first need to create and store an original copy of the physical makeup being used as an authentication measure. Biometric authentication is

performed by doing a comparison of the physical aspect present for authentication against the stored copy. A match grants access while a mismatch denies access to the system or application being accessed. An advantage to this form of 2FA is that the user has to be physically present for the access to be granted.

4.3.4. Push-Based Authentication. This is an authentication measure where a prompt is sent to one of the user's devices for attempted login. This prompt will indicate that someone (possibly you) is trying to log in, and an estimated location for the login attempt. A user can therefore approve the login if they are aware of it (themselves logging in) or reject it in case they have no idea of it. This is better than a one-time password and authenticator app as accepting or rejecting a prompt is more convenient than typing a code. The authentication's ability to generally display an estimated location based on the IP address serves as an improved security measure. One of the examples is OKTA Multi-factor authentication system.

4.4 Types of Attack Reduction by Authentication

Attacks from various sources can be reduced by implementing authentication measures such as two-factor authentication.

4.4.1. Phishing Attacks. These attacks use social engineering to achieve their goal by sending an end-user message or email which requests sensitive data, such as a password or credit card details. With a 2FA authentication measure, even with a password, the hacker will still need to provide the second piece of security which could include OTP, etc. Any application or platform which has implemented 2FA will therefore reduce the phishing attacks as stealing of password-only would not grant access to the unauthorized user.

4.4.2. Spoofing Attacks. Spoofing attacks occur through masking communication or identity so that it appears to be associated with a trusted, authorized source. A person or identify successfully identifies itself as another through falsifying data which leads to illegitimate access. As the key aspect of spoofing attack is false identification, with two-factor authentication the hacker will not be able to successfully falsify information as access is granted with the use of physical features such as 2FA measures such as app-based authentication or OTP.

4.4.3. Key logger Attacks. A key logger is a program or application installed in a computer that has the capacity to save and document all activities performed in the specific computer including internet searches, keystrokes, documents, emails, URLs and login credentials (Pawade et al., 2015). While key logger was created for legal reasons, criminals have used key loggers to access critical and sensitive information from unsuspecting targets. Hardware key loggers are devices manually plugged into a PC to record and save all activities performed within the PC. Adding authentication measures to the process of installing programs into a computer or system will prevent bad actors from installing key loggers. This is because they will need to input a password and probably a second authentication measure which could include OTP.

4.4.4. Man in the Middle Attacks. A man-in-the-middle attack (MITM) works by intercepting communication between two parties in a network. The attack can then modify the information being relayed thus giving a different message from what was intended. While this attack happens on a wireless network, having a strong encryption mechanism on wireless access points prevents unwanted users. Simply implementing authentication factors to access the network will ensure unwanted actors do not join the network thus reducing the risk of MITM attacks.