ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 9, September 2019

Assessing the Reliability of Selected Systems' Security Solutions in Communication Networks

Achunike, U. V[1], Egbuna, F. C[2], Omerenna, K. C[3].

Lecturer II, Dept. of Computer Science, Liberal Bilingual Institute of Togo, IBLT, Lome, Togo [1]

PhD Candidate, Dept. of Electronic Engineering, UNN, Nigeria[2]

Production Technician, Culinary Dept., Nestle Nigerian Plc[3]

ABSTRACT: Most enterprises conduct businesses with external clients, like customers and partners, deploying various kinds of networks— internet, intranets, and extranets for the purpose of information exchange. Managing a series of networked client systems secured in terms of their data, applications and services is critical. Thus, this study examines the use of two selected systems' security solutions: password authentication and staff security training for combating diverse system security challenges. Data was obtained through secondary sources. Statistical multiple regression model was used for the data analysis while the stated hypotheses were tested using the *F-Test* and *T-Test* techniques. Findings review that the potencies of the two security solutions towards secure systems is significantly minimal. The study recommends that organizations deploy other security solutions for avoidance of information technology security-related incidents within their communication networks.

KEYWORDS: Enterprises, Security, Information technology, Passwords Authentication, Staff security training and Communication networks.

I. INTRODUCTION

Over the years, many information security experts have proposed a number of methodologies for curbing the increasing cases of security breaches and attacks in companies' communication networks. Organizations, either big or small cannot afford to permit classified data to be accessed by unintended persons. With the growing online attacks on critical communications infrastructures by hackers justified this study and a thorough re-examination of the situation. Understanding the efficiency of security solutions for user systems is one of the key goals of scientific research on systems protection. An analysis of the security procedures is sure approach in combating systems threats within working environments. In the past few years, businesses increasingly rely on Information Technology, IT in the form of hyper-connected network of information and communication systems.

Client or *User system* refers to personal computer, PC that uses services offered by the servers. These users or client workstations can send requests to servers and equally process information from servers in a networked environment. Securing user systems requires that individual users be authenticated before access is given to use system resources. User identification (user Id) refers to the systems' ability to identify every PC user via passwords, or auxiliary devices like smart cards and hardware tokens [10]. In this 21st century, the strong password protocols alone are insufficient to address phishing attack [12]. The combination of username: the public identifier for the user account; and the password: the secret key which unlocks access to that account is enough security for most people on stand-alone computer systems. But for systems on a communication network, an additional protecting factor is essential. A physical device referred to as 'hardware token' permits the owner to access a computer or a network by generating a number which uniquely identifies the intending user to the service. While security tools are seen as indispensable to organizational security program, it is however, imperative that cultural change through security awareness trainings be

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 9, September 2019

well incorporated. In [5] L. Zink stated that this can be implemented by ensuring every employee is equipped to play a role in securing oneself, her company and its assets from both logical and physical security vulnerabilities. Security awareness will enable all employees to work together to guarantee a successful sustainable security posture for the company. In [6] M. Drolet agreed that for safety of data, people in an organization should have the right training and a working understanding of the information policies, in addition to latest security software tools, and more robust security programs.

A. *Problem Statement*

A lot of enterprise system users neglect to utilize even the most basic computer security solutions available in spite of the current threatening security challenges relating to computing. They feel that security is someone else's job. With the rapid growth of the internet and the reality of electronic commerce; many corporations have become highly dependent on digital information systems for ease of business. Many businesses are now conducted over online platforms. The situation where an intruder with a compromised password of an enterprise user gains unlimited access to all her online service accounts is worrisome. Identity theft takes various forms—exploiting weak passwords, key stroke capture, phishing, Trojan software, social engineering, and password sharing [10]. It is increasingly recognized that user authentication and adoption of security awareness programs for staff are among key factors in securing computers in industries. Nowadays, communication networks constitute the core component of governments and private establishments' IT infrastructures globally [7]. A source of worry at the present is the potential attack on the information and client systems belonging to these critical infrastructures. The trust of this study is to uncover if the selected security tools (of strong password authentication and staff security training) are capable of offering maximum protection against most ICT-related incidents and destruction of data in enterprises guarantee optimal security of business operations within working environments.

B. *Study Objectives*

- To offer theoretical and empirical insight into the security of user systems by utilizing strong password authentication and auxiliary security devices.
- To asses the up-to-date trends in security of user systems.
- To analyze the effectiveness of password authentication/user Id and staff security training in enterprise' networks.

C. *Research Questions*

In view of the above highlighted issues, the following research questions were relevant:

- 1: What is the relationship between the two internal security mechanisms (of password authentication and staff security training) and ICT security-related incidents in communication networks?
- 2: To what extent do strong password authentication and staff security training ensure protection of enterprise users?

D. *Hypothesis Formulation*

For the purpose of the study, some hypotheses have been formulated and tested:

H_o : The adoption levels and implementation of both password authentication/user ID and staff security training do not offer significant protection against ICT security-related incidents.

H_A : The adoption levels and implementation of both password authentication/user ID and staff security training offer significant protection against ICT security-related incidents.

E. *Study Delimitation*

The study will focus primarily on the effects of strong password authentication and staff security awareness training in enterprises across various sectors, such as manufacturing, real estate, electricity, transportation and storage, information and communication, in twenty-six European Union, EU countries. The size of employee ranges from large enterprises of 250 persons and above to small enterprises, with at least ten persons employed.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 9, September 2019

II. REVIEW OF RELATED LITERATURE

Various sectors of the economy—both public and private amass a great deal of confidential information about their employees, customers, products, research and financial status. As the threat landscape mutates, IT security professionals must to adapt to the evolving threats with the assumption that users are vulnerable— whatever PC type or brand. Hence, protection of the users in the networks from malicious intrusions is critical to the economic progress of every nation. User system security is concerned with processes and mechanisms by which sensitive and valuable information and services are protected from unauthorized usage or non-trusted individuals. Access required authentication with a username and password that was typically assigned by the system administrator, not the user [15].

a. *Management of Passwords Security*

The change caused by digital transformation of production processes is demonstrated globally at an unprecedented rate. Artificial intelligence, robotics, big data, blockchain and the Internet of Things, IoT which already with us, are products of the on-going change [11]. As many as 81% of hacking-related breaches over the past year leveraged stolen or weak passwords [14]. In [8] Ovum 2017 reports that 23% of employees are using social media credentials to sign in to business systems and apps (applications) in the workplace. People store and share sensitive company data on popular apps such as *Google, Dropbox, Evernote* and so on, but when poorly managed, pose a threat. Going by the *Intel World Password Day Survey 2016* [3], an average business user keeps track of 27 passwords to remember.

However, marketers, systems administrators, sales representatives manage several accounts. Beyond the enterprise-level apps, individual workers have dozens of passwords. Furthermore, in [9] *Psychology of the Password 2016 Report* estimates that the average 250-employee size company would now have some 47,750 passwords in use across their entire organization. Businesses are currently experiencing password proliferation and failing to manage them securely can have dire consequences. Password sharing is common. In the workplace, though, sharing of credentials and other sensitive data is also an essential part of getting the job done but in turn creates *loopholes* for illegal access to applications and sensitive data-files. There are some best practices in password management, especially for online authentication and transactions. These techniques increase the chances of keeping online accounts secure from hackers. First, use a randomly generated complex and unique password — a unique password for every online account. The password should be complex and of a greater length. A *strong password* must meet basic features. It should consist of:

- At least eight characters
- A mixture of upper and lowercase characters
- A mixture of alpha and numeric characters
- A special symbol such as + ! @ # $? % & *

Second, enable multi-factor authentication. This helps prevent unauthorized access of online accounts and could sometimes send alert for compromised password. Lastly, passwords should be changed regularly — ideally every 60-90 days. To succeed in password management, strong password protocols must be coupled with spoof-resilient password-entry interfaces where users can safely enter their passwords [12].

b. *User Systems Authentication*

Authentication is the process that attempts to establish the identity of a user and is followed by an authorization process that grants whatever privileges may be appropriate to that identity. Common examples of authentication include logging on to a workstation in a corporate network (using a username and password), withdrawing cash from a bank cash dispenser (a bank card and personal identification number, PIN), and online shopping (an email address and password) [10].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 9, September 2019

Several firms these days have moved from simple authentication, which uses only a password, to advanced authentication. Generally, advanced authentication describes two forms of authentication. First, a password: that the computer user knows and employs to authenticate. Second, a token or smartcard: that works as the authentication device. Smart cards store huge amounts of data, like access transactions, qualifications, and biometric templates. With Contactless technology, a smart card is wireless, has an embedded microchip and operates at 13.56MHz (Megahertz). Notwithstanding, a password, a passphrase, an encryption key, a multi-factor token are all subject to compromise when transmitted over the internet, on the other hand, a thumbprint or a retina scan (personal biological metrics) is more secure [16]. P. Wood suggested implementing stronger authentication through smart USB keys and mobile phone short messaging service, SMS texts for all remote users and for all privileged users and accounts [10].

c. *Security Awareness Program*

Everyone has a role in protecting the organization and their own job functions. In [6] M. Drolet reviewed that "employees are the weakest link" in cyber defenses, due to their vulnerability and possible mistakes. Sometimes, they lack understanding of compliance requirements and sensitive data handling. Yet, they can be a huge asset to any security team if they are given the right tools and trained properly. Security awareness program is aimed at training employees to help them make smarter security decisions within an establishment. It involves equipping employees with the knowledge they need to spot the threats and take appropriate action that aligns with the company policies, thereby improving the organization's security posture and mitigate risk. According to a research done by Computing Technology Industry Association, CompTIA, 96% of people surveyed recommended user training, due to the raising rate of breaches resulting from user error [2]. Providing employees with effective training will enable them to become better cyber security partners. Giving extra security training to security guards, helpdesk staff, receptionists and telephone operators, plays a vital role in blocking identity theft [10]. Moreover, for meaningful security awareness training programs, firms have to assess company needs, develop content, schedule and deliver training, and also test and track the impacts of the training.

III. METHODOLOGY

The data presented in this study were based on surveys conducted across various sectors within the EU by National Statistical Authorities on "ICT security in enterprises" in 2010. Thus, data source is from secondary data.

The total number of enterprises of the European Union 27, EU27 member states (without Estonia) formed the population of the study. Available statistics put the total strength at 1.6 million in the EU27 [4]. The sample size surveyed for the study was 149 900 enterprises having adopted simple random technique. Data collected from the study was classified into different groups with the aid of tables. The Analysis of Variance (ANOVA) was used to test the hypotheses.

IV. DATA PRESENTATION AND ANALYSIS

The data obtained from the study are presented below. The data in Table 1 shows the percentage of enterprises that adopted Staff security awareness and password/user authentication respectively and the percentage of ICT security-related incidents admitted in each member state of the EU. Calculations are based on the aggregates statistics of each European member state.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 9, September 2019

Table 1: Data Of EU-27 Enterprises (Percentage of Enterprises)

European Countries	I C T SECURITY		
	ICT-Related Incidents, ICT	*Staff Training/ Security Awareness, SA*	*Strong Password Authentication/User Identification, SP*
Belgium	15	52	52
Bulgaria	10	41	33
Czech Republic	26	54	40
Denmark	29	56	56
Germany	11	50	46
Ireland	20	64	64
Greece	29	52	33
Spain	26	50	63
France	9	29	33
Italy	19	67	66
Cyprus	29	84	43
Latvia	10	58	42
Lithuania	22	65	42
Luxembourg	12	36	62
Hungary	5	25	24
Malta	18	43	52
Netherlands	22	33	53
Austria	10	44	39
Poland	10	18	53
Portugal	40	57	55
Romania	19	53	29
Slovenia	9	62	64
Slovakia	20	53	20
Finland	28	80	53
Sweden	19	65	58
United Kingdom	6	48	53

Source: Eurostat (http://ec.europa.eu/eurostat/product?mode=view&code=isoc_cisce_ra)[4].

1. *ICT Security-related Incidents*

This section of the study evaluated the factors associated with ICT-related security incidents reported by the workforce. From the analysis, we found that there were considerable variations in recorded incidents among the member states represented in the study. Table 1 column 2 shows the percentage, % of enterprises that have experienced certain ICT

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 9, September 2019

incidents that resulted in unavailability of ICT services, destruction or corruption of data due to hardware or software failures. These incidents were due to attacks from outside e.g. denial of service attack; malicious software infection or intrusion. Figure 1 presents the aggregate comparative analysis of password authentication and staff training factors as adopted by enterprises. From figure 1, staff awareness training recorded an aggregate of fifty-two percent (52%) adoption than those who practiced the use of strong password authentication (48%) and other identification methods such as smart cards put together. Hence, training of the workforce was higher in implementation among enterprises than the latter.

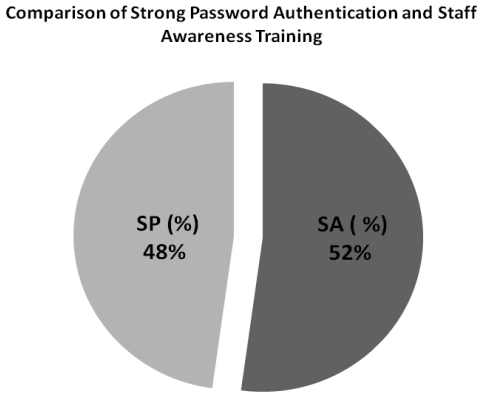

Figure 1: Comparing Strong Password authentication, SP and Staff Awareness security training, SA (percentage of enterprises that deployed each solution)

2. *Password Authentication/User Identification*

Identification refers to the ability to identify and distinguish between individual users. User ID, an authentication procedure is considered as common practice in many business enterprises today. Table 1 column 4 shows percentage of enterprises that have used strong password authentication or user identification and authentication via hardware tokens, by economic activity of each sector.

3. *Staff Training/Security Awareness*

Enterprises adopt various approaches aimed at raising staff awareness of ICT security policy and the relevant risks in relation to their ICT-related security obligations. From Table 1 column 3 displays the percentage of enterprises which have adopted any approach to make workers aware of their obligations in relation to ICT security, by economic activity.

4. *Test of Hypothesis*

The hypothesis was formulated to test the validity of the study. The data used for the testing of the hypothesis was derived from data questionnaire dispersed to the respondents in sectors across all economic activities as presented in Table 1.

H_o: The implementation of both password authentication/user ID and staff security training do not offer significant protection against ICT security-related incidents.

H_A: The implementation of both password authentication/user ID and staff security training offer significant protection against ICT security-related incidents.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 9, September 2019

Table 2: Analysis of Variance (ANOVA)

Source Of Variation	*Degrees Of Freedom (Df)*	*Sum Of Squares (SS)*	*Mean Square (MS)*	*Variance Ratio (F-Ratio)*
Regression	k = 1	SSR = 553.72	MSR = 553.72	
Error (Residual)	n– k = 24	SSE = 9,993.3	MSE = 416.39	F = 1.331
Total	n – 1 = 25	SST = 10,547		

Source: Pennsylvania State University, 2018 [13].

Step 1: To perform the test of significance, we use F-Test statistics.
Where MSR is the Mean Square Regression and MSE is the Mean Square Error

$$\text{F-computed, } F^{*} = \frac{\text{MSR}}{\text{MSE}} = \frac{553.72}{416.39} = 1.331 \qquad \text{Eq. (1)}$$

From eq. (1), F-computed, F^{*} is 1.331.

Step 2: Compare the observed F-critical with the F-computed values
Since F-computed, F^{*} (1.331) < F-critical, F_c (3.42)

Step 3: Accept or reject the Null Hypothesis, H_0
The hypothesis test showed that from the F –statistical test, the observed F-critical (3.42) was greater than calculated F-computed (1.331) at 0.05 level of significance. Therefore, we accept the Null Hypothesis, H_0. We accept the null hypothesis, H_0, which states that adopting both password authentication/user ID and staff security awareness training does not offer significant protection from ICT security-related incidents in corporations. The co-efficient of determination, R^2 (adj) was 5.25 percent. Therefore, we conclude that the two security approaches have no significant effect on data destruction or corruption in communication networks.

5. *Discussion of Result*
The findings revealed that the extent of the two security solutions (the password authentication/user ID and staff security awareness training together) had non-significant positive impacts in determining the availability of ICT services and protection of data in companies. This implied that their combined effort in preventing loss and data corruption was not statistically significant. Our interest is on the magnitude of the impact of the selected security methods used on the problem of unavailability of ICT services in enterprises.

The study revealed that most employees relied mainly on the use of passwords for validating their identities. However, a few others in the corporate world employ complex passwords as their own form of top security. P.Wood [10] identified passwords as the common means of authentication. Unfortunately, most users do not know how to construct a secure password, nor understand the risks involved. Also, the work recognized the fact that members of staff often use the same password in several different situations. As a result, anyone who steals the identity of a specific user becomes the user and has access to her system and sensitive corporate data.
For a comprehensive security of user systems in view of business threats, enterprises must incorporate additional tasks in their ecosystems that include security technology controls without ignoring organizational issues that drive information security risks [16]. With the growing cyber threats that is constantly changing IT security landscape,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 9, September 2019

businesses are waking up in discovering that end-users PCs are known sources of all kinds of invasion into the network architecture, and hence the need for their maximum protection.

V. CONCLUSIONS

In summary, information technology has been a force behind the advancement of several industries, and these advancements in technology would require further increase in the security apparatus of enterprises. On the basis of the findings of this study, the following recommendations are made to facilitate the efficient protection of user systems operating within the enterprise network environments:

- The management and policy makers should be properly guided in finding far reaching solutions to IT-related security breaches in the corporation.
- Information security administrators need to belong to some security networks groups, forum or societies for more enlightenment and notification about current trends and practices in the world of information technology.
- There is need for allocation of special funds to IT units annually or quarterly for the purchase of security facilities and periodic conduct of staff awareness training sessions.
- Other security tools - internal and external should be deployed including secure firewall services, routers, secure clients and servers systems, and third-party security applications and services.
- Further research will be required to extend the theoretical foundation of this work by identifying more security-related attributes and techniques that can address completely ICT issues indicated earlier.

REFERENCES

[1]C. Moore "Implementing a security awareness program – creating security conscious employees," Prince George's County Memorial Library System, UK, December 8, 2017.
[2]D. Lohrmann, "Reducing risk through next-gen cyber awareness training**"** CSO State of Michigan, Produced by The Security Confab, at La Jolla, California, pp4, April 15- 17, 2012.
[3]J. Bernstein, "People have way too many passwords to remember" Intel World Password Day Survey 2016, Intel, USA.
[4]K. Giannakour, and M. Smihily, "ICT security in enterprises" Statistics In Focus, Eurostat, National Statistical Authorities, ISSN 1977-0316, Luxembourg, Feb. 2011.
[5] L. Zink, "How to tailor security awareness training to employees' need," Security magazine BNP Media, Skokie, Illinois, IL, US., Nov. 2017.
[6]M. Drolet, "Infosec at your service: 4 steps to launch a security awareness training program," CDG Technologies, contributor Network, Boston, 2108.
[7]N. C. Ozigbo, "The adoption of information and communication technologies in the management of Nigerian oil and gas industry," International Journal of Humanities Social Sciences and Education (IJHSSE) Volume 1, Issue 7, July 2014, pp 179-190.
[8]Ovum "Close the password security gap: convenience for employees and control for IT" report, LastPass, LogMeIn, Inc, 2017.
[9]Psychology of the Password 2016 Report, "Password exposé: 8 truths about the threats and opportunities of employee passwords, LastPass, LogMeIn, Inc, 2016.
[10]P. Wood, "How To ensure Strong Password And Better Authentication" First Base Technologies LLP, Brighton, UK, Oct. 2015.
[11]Spain's Department of National Security, National Cybersecurity Strategy 2019, Prime Minister's office, June 2019, p18, 23
[12]S. Ruoti, J. Andersen, and K. Seamons, "Strengthening Password-based Authentication," Symposium on Usable Privacy and Security (SOUPS) 2016, June 22–24, 2016, Denver, Colorado.
[13]STAT 501 "Regression methods lesson 6.2 - the general linear F-Test, https://onlinecourses.science.psu.edu/stat501/node/295, Penn State Eberly College Of Science, The Pennsylvania State University. Aug. 2018.
[14]Verizon's Data Breach Investigations Report, 2017, Verizon enterprise.
[15]White Paper "Why your business needs enterprise-strength password management" Keeper Security, Inc., Suite 500,Chicago, IL., 2017.
[16]Y. E. Yeniman, "The importance of risk management in information security," Uludag University, Computer Technologies Department, Research gate publisher, Turkey, 31 May 2018.