

Impacts of Human Behaviors on Cyber Security

¹Bandar Alfahidi, ²Anas Almehammedi, ³Abdullah Hasan

^{1,2,3}Dept. of Computer Science and Engineering, Taibah University, Saudi Arabia

Abstract

As organizations keep investing in cyber security technologies generously due to growing demands for that technologies, human weaknesses remain a basis of data breaches across organizations network. Human weaknesses are still a hard challenge to overcome if organizations want a robust cyber security shield. In this research we tried to address human limitations that lead to data beaches or cyber-attacks against workplace network depending on literature reviews in the same field of the research. First, we write about cyber security as a technical matter where organizations invest huge budget to implement needed software and hardware to protect their information assets. Then we talk about cyber security as a human matter. After that we address human behavior related to security starting with improper practices related to password. The next topic is leaking information by employees or insiders intentionally or unintentionally. Next, we focus on the risk of accessing organization network using personal WIFI-enabled devices which suffers from lack of security software and updates and how they may be exploited penetrate the network. Then we talk about social engineering as a threat. Next topics are reaction to suspicious activity, cyber Awareness for employees as a shield, and cyber Security policy.

Keywords

Cyber Security, Cyber Security Policy, Awareness, Human Factor.

I. Introduction

We should be very thankful to technology, quality of life has been obviously improved, in the event of an emergency. In fact, the technological revolution has significantly improved how we live, how we arrange travelling, how we communicate, how we easily get knowledge and learning, how we are treated in hospitals and most importantly how we manage our lives. The technology, which includes wired and wireless networking, software, personal computers and smart phones, supports our day to day life and becomes so necessary and without it our life is inconceivable. That makes our world so complicated, very connected and unfortunately very dangerous because a lot of our personal data and information are needed to take advantages of that technological revolution. Those data include personal information, credit cards numbers, user ID's, passwords, confidential files ... etc. The need for cyber security increases day by day but it's not that easy. Cyber security is a process and practices not just a product to buy or just a system with strong passwords. We cannot neglect humans in the cyber security processes. Unfortunately, Humans is considered the weakest link in that processes. Security is not just blinking and modern devices or software with good interfaces with many claimed security functions. Humans who access systems are crucial elements and must be considered as a source of threats or a shield for protection. With the human factor as such a pervasive element in businesses and critical infrastructures, it is not surprising that human resources have an impact on the success of the efforts to secure businesses [1].

II. Cyber security as a technical matter

Internet is fundamentally insecure, so security is developed as a defensive solution to protect any interconnected systems from cyber threats and attacks. Network, devices, applications and data centers are examples of systems that are vulnerable to threats. As internet rapidly grows cyber security becomes more specialized to include applications security, network security, cloud security, data loss prevention, identity and access management, mobile security and end-point security. An effective cyber security approach should be adaptive and dynamic, and that approach should include people, processes and technology that complete each other. Technology help processes work together, and security tools are used to carry out cyber security defensive. Analyst firm IDC published its first Worldwide Semiannual Security Spending Guide Oct. 12, forecasting that global cyber-security spending will reach \$101.6 billion by 2020. [2] Spending that huge money on cyber security tells us how much organizations concern about cyber security and it must be planned and implemented for every single system. Costs of security breaches can be due to detection, investigation and recovery. Of course, the amount of needed money varies by organization size. Unfortunately, spending money on poor cyber security can be expensive. More costs may occur if we take in our consideration stolen business information by competitors, loss of reputation and the organization might be prosecuted according to data protection legislation. Sure, we don't strive to gain absolute security because it's impossible to reach. Each security corporation or information technology company has its own security layer system or defensive tools. i.e. for cyber security to be done right, it should be done in layers to get good level of security and to put many security devices in front of our critical assets. In these layers, we have an internet facing router at the beginning and after the that we will put firewalls for further inspections and Intrusion Prevention System (IPS). Then Intrusion Detection System (IDS) is put in place. After that load balancer and web servers in order. So, any attempt to attack must go through all that layers. All this is a technical control to help in cyber security. We also need a dedicated system that helps us to protect our assets away from that harm of malicious software. I mean antivirus system which include servers and licenses for all clients of organization. Nowadays, anti-viruses' functions are expanding to include protection from browser hijacking, key logger, ransom ware, backdoors, trojans, DDos attacks etc."

III. Cyber Security as a Human Matter

Humans in an organization could be end users, IT professionals or cyber security specialists. Human may do error or failure include acts performed with or without malicious intention. Some causes for these human errors are lack of experience, lack of proper training, or incorrect assumptions. Regardless of the cause, even innocent mistakes can result large-scale harm. For example, a simple typing error can cause organization's website unavailable or internal servers out of reach. So, employees are considered one of the greatest threats to an organization's assets and data. Furthermore, human mistakes can lead to exposure of classified data, deletion or modification of DB tables, or storing data in unprotected locations [3].

IV. Human behaviors related to cyber security

Now we will address some human behaviors that are related to cyber security. Organizations must be aware of that behaviors and what risks they may result in case of breach.

A. Using Improper Password

As one of the leading types of cyber-attacks, ransomware is expected to dominate cybercrime in 2020. According to PreciseSecurity.com research, weak passwords were one of the most common cybersecurity vulnerabilities in 2019, causing 30% of ransomware infections in 2019 [5]. According to Google new study, password reuse is one of the main barriers to have safer internet. There is a gap between cyber security and internet user perception in case of determining passwords. According to google Chrome management, two in three people reuse passwords to be used in many accounts. That's due to easy management of passwords and scattered accounts for different systems or websites [6]. Also using weak password is another dangerous behavior that affects information security. Using such weak passwords in bank accounts for example put financial transaction on the internet at high risk to be hacked. Some practices to use weak passwords are as the following:

- Using guessable structure passwords
- Using passwords that has just dictionary words
- Using passwords that has just numbers
- Using some commonly used passwords. According to a report by Teams ID the most commonly used passwords are "password", "123456" and "12345678" [7].

The unspecialized end user should be aware how to set strong passwords. Most of them don't realize the importance of using strong passwords that combined of letters in different cases, numbers with special characters to build very strong passwords to protect their vital data. Here are suggestions for good passwords:

- Don't follow grammatical structure while using long passwords. A long easy-to-remember passwords doesn't mean a strong password.
- Use passwords that consists of combinations of numbers, small letters and capital letters. Using a password consisting just digits or just letters is too risky that might be guessed or hacked.
- Personal data should not be included in passwords, such as birth date, names, mobile, address ...etc.
- Password is strictly private. i.e. should not be told or shared with anyone.

Now many organizations use 2-step passwords for authentication which means more strong passwords. This is a brilliant way to authenticate user during login [8].

B. Sharing password

Sharing passwords with others is a risk but people still tell others their passwords. This happens sometimes for example to access your friend smart phone using his passcode while he is driving. Also sharing passwords between people in the house is so common. Who's doing such dangerous cyber behavior? Time magazine gathered and analyzed data of end users with ages. Sharing password behavior is related somehow to age according to that data as the following:

- 64% of people between 18 and 29-year-old share passwords

- 70% of people between 30 and 49-year-old share passwords.
- 69% of people over than 50-year-old share passwords.

Sharing passwords closely means you have nothing for hiding which is good. Nevertheless, it means how much you ignore risk from security and privacy perspectives. In Time magazine data, among shared passwords, 74% of passwords are told verbally and 15% of them are shared using paper and pencil. While SMS are used to share 5.8% and 4.4% of passwords are shared via e-mail. On the other hand, just 2% of that shared passwords are shared using secure password sharing services. Also, that study shows that 73% of people admit that sharing password is a dangerous habit and they are unlikely to modify their passwords after sharing. This is a big problem when using passwords over wi-fi or financial accounts due to 59% of people use same passwords for many online accounts. This means giving a person your password of Netflix can probably mean you've telling him your iTunes or Twitter password too [9]. Misuse of authorities of systems is another risk of shared password especially for passwords of system superusers or administrators. The case will be worse if the company uses single sign on (SSO). A survey done by Centrifly® said that about 60% of privileged accounts are shared by IT professionals with their colleagues. Moreover, an estimation was done by Forrester® says that 80% of security breaches was committed due to sharing of privileged passwords.

C. Leaking Information

Information leakage refers to the act of intentional or unintentional disclosure of information to an unauthorized party (Anand and Goyal, 2009) [11]. In practice, all organizations are vulnerable of insiders who pose threats to leak data and information due to their legitimate and unsurprisingly access to organization's valuable information, systems and assets. These insiders or employees will probably know how to achieve the greatest influence or impact without any evidence in the crime scene or little evidence. Information leakage published or distributed by authorized user or insider threats are continually succeeding in doing damage to organizations due to expose of organization's information which leads to great and significant loss and has bad impact on organization's image, profile and reputation. So, insiders are considered one of the greatest threats to the company and such information leakage should be inhibited if the organization or company want to be competitive and gain more competitive advantages in business. The protection of confidential data against leakage is a growing concern going by the leakage statistics. Clearly, the traditional method of protection using information security systems and policies and conventional security technique such as firewalls, VPN and intrusion detection systems continue to be misused and exploited by insiders and outsiders alike. Unfortunately, these techniques lack proactiveness in protecting top secret and confidential data. Digital data or information have three basic different states:

- Data in use: in refers to data being processed to be created, updated, deleted and viewed where human interacts with the system interface via different endpoints.
- Data in transit (in motion): it refers to data moving across networks or in memory (RAM) that is ready to be read, changed, or processed. This movement may be between from LAN to colludes, from mainframe to terminals, or from internet to organizations network. Data in motion also travelling across physical cables or via wireless networks.

- Data at rest: it refers to data stored any storage media or any form (hard drives, tapes, offsite backup, backup clouds, file servers ..etc)

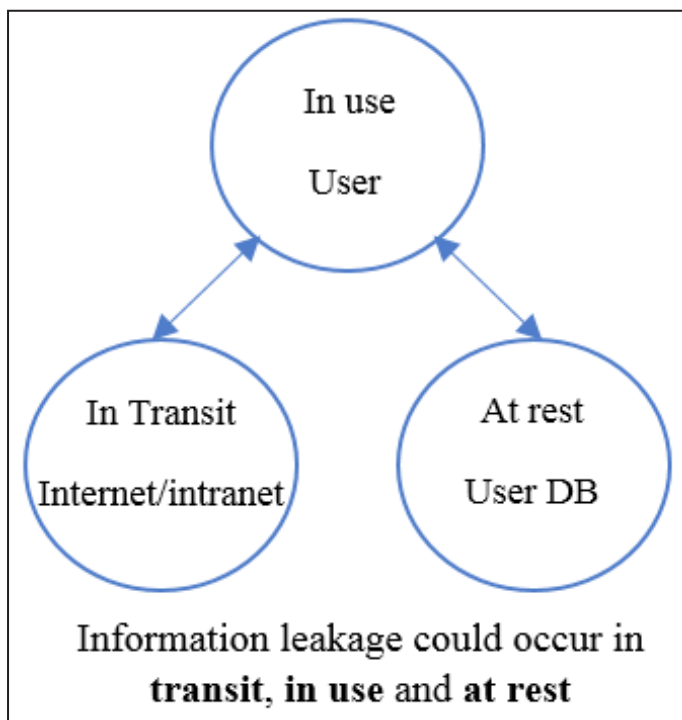


Fig. 1: Information Leakage in all Three States of Data

To leak information from within the organization, authorized insiders just need their usernames and passwords to access or retrieve a copy of such valuable information using IT devices or technologies such as laptop, e-fax, smartphones, e-mail, USB, printers or tablets. Then authorized users can share the stolen information with unauthorized malicious recipients. The impact of that treats is unimaginable and harmful.

D. Accessing Organizations Network Using Personal Devices

Employees can't go to their workplace without carrying their smartphones because they depend on them to manage their lives. According to a global mobile consumer study made by Deloitte in 2016 that found that 74% of respondents check their mobiles before sleeping within 15 minutes, 61% check their mobiles again within 5 minutes of waking up. Approximately %88 look at their mobiles within 30 minutes of getting up.

As long as smartphones and tablets become constant escorts, hackers always trying every way to break security of that wireless devices. Many people think that iPhone or Android smart devices are secure while they aren't. Owner of smartphones should configure security and privacy settings to guard its phone as much as possible. Using suitable and inexpensive tools, hackers can gain access to such smartphones that use the same wireless network. Based on Gardner research, %27 of organization data traffic will go through portable and mobile devices to the cloud. In addition, cyber-attacks against smartphones are increasing and evolving dramatically, so that cybersecurity of smartphones become a crucial segment of cybersecurity of organization.

Many organizations allow access to the Wireless VLAN in premises with just giving a password without concerning about how secure the laptop or smartphone is. These wireless devices may be used as an object of attack or subject of attack.

The tools to hack into wireless networks is easy to know and readily available, and much of them are searchable and accessible using just a search engine, making Wi-Fi hacking and man-in-the-middle (MITM) attacks easy to implement. That makes the data of the organization vulnerable to be intercepted or decrypted across the network. Hackers can also exploit WIFI weaknesses and cellular data protocols to snoop on data and emails, or to hijack users. Accessing smartphones of people logging to the enterprise systems gives attackers opportunity to access the organization database.

Other threats of using mobile devices come from employees or insiders. Many employees never update mobile security software. Also, they download many applications on their devices that leads to unintentional threats. They use that applications that can access enterprise assets or can harm computer network by spreading viruses or worms. Another issue is misusing of cloud services via mobile apps to convey organization data which may lead to information leaks.

Smartphones security threats will keep developing and advancing as long as organization data is access by enormous number of WIFI-enabled devices and the hacker will not stop the war.

Mobile security threats will continue to advance as corporate data is accessed by a seemingly endless pool of devices, and hackers try to cash in on the trend. It's difficult to make all users understand the consequences of faulty insecure mobile and to use best practices.

Making sure users fully understand the implications of faulty mobile security practices and getting them to adhere to best practices can be difficult. Many users never install basic security software on their smartphones like anti-virus, anti-spam and firewalls.

The employee behavior is crucial to help in prevention of threats from his smartphones by installing cyber security software, keeping OS updated and eliminating unnecessary mobile apps.

E. Social Engineering as a Threat

Social engineering is defined as "breaking an organization's security by interactions with people" [13]. Another definition for social engineering is "taking advantage of people's naivety via influence, persuasion and manipulation to obtain vital information" [14]. It is also described as "a skill set utilized by an unknown individual to obtain trust and access to an organization via someone in the organization and consequently guides them to alter IT system rights or access that ultimately grants the individual access rights" [15].

There is a consensus between researchers and scientists in the research community that humans are considered the weakest link in an information system. Attacking organization information systems and data using techniques of phishing which is a part of human vulnerabilities is becoming one the major cyber threat rather than attacking through technical or breaking information systems.

Social engineering essentially presupposes utilization of human common sense to gain over crucial or critical organization data and information (such as usernames, passwords, or organization directories) from unsuspecting or unaware workers employees. For example, this can be achieved through persuasive a person, through bluffing, to tell a password. This technique or way is usually utilized by hackers where technical means have failed to break the protection of a target system.

In terms of the business need, most organizations have put-up high-quality technology defense and protection software and

hardware, like firewalls, routers, intrusion detectors and many others to safeguard their information systems and networks against unauthorized access, while neglecting the social sides. It is clear that the greatest risk to information security in organizations is not technology-related, rather it is in action and reaction of employees and other organizational staff that accordingly results to security incidences.

A huge number of social engineering attacks happen to gain over information or access systems by exploiting unaware employees. These attacks go through cycle starting with information gathering from public resources such as website, address book, telephone directory, social media posts, jobs web page and so on. In the next step, the attacker tries to build a relationship with the targeted employee as he is helpful to him. If the attacker succeeds, he tries to exploit that relationship to trick the target employee to uncover sensitive information which can be either be the final goal of the hacker or the beginning of the next step. Finally, the attacker tries to hit the final goal that may involve another iteration of past steps.

In practice, it would be unattainable to stop social engineering breaches completely, the risks can be mitigated and the harm to systems and information can be decreased.

Social engineering attacks can be defended by multilayers approaches as the following:

1. Improving security in premises of organization that doesn't allow unauthorized employees to get in at all.
2. Building a strong security policy that must be reviewed frequently to be aligned with current state and new circumstances. More attentions must be implemented in the policy to safeguard against social engineering attacks include matters related to information release internally or in public, access approval, passwords, help desk, employee ID, shredding confidential documents, etc.
3. Response to Security Infringement which includes training against social engineering attack techniques, ongoing reminders about social engineering risks, and penalizing employees who constantly break policy controls.
4. Incidence Handling Procedures refer to actions to be take in the case of an attack [16].

F. Reaction to Suspicious Activity

In some cases, an employee may choose to disregard and not report unusual or suspicious activity (regarding to information breach), or he could gain access to critical information beyond the user's role and credentials through unethical manners. All these events disclose the organization to security risks with the misusing of sensitive and crucial information [13].

G. Cyber Awareness for Employees as a Shield

As information technology world is expanding and evolving constantly, the importance of educating employees about cyber security is increasing dramatically to sustain suitable human behavior to minimize security breaches and to enhance cyber security management [17]. A company must work to raise the awareness of cyber security among all stakeholders by spreading that culture and awareness. It can distribute and publish that culture through different digital channels, events, workshops, and training for non-cyber security professional. This awareness activities may discuss some demanded topics such as:

- Secure your mobile phone.
- Password security.
- Tips for Safe internet browsing.

- Email Security.
- Organization may also include employees' families as a sort of social responsibility.

H. Cyber Security Policy

Many organizations and countries are actively establishing cyber security policies to protect their critical information systems, crucial assets and vital data. Employees and insiders of an organization must be informed and educated to know the impact they might have on the cyber and information security of the organization [12]. Security policies are work programs, regulations or standards technical and material and other. Which is specific for information security in both activities and sectors that clarifying the path to information security. Like:

Acceptable use policy as a part of cyber security may include the followings:

- All organization's assets shall be used only for business purposes.
- All users shall not participate in illegal activities such as accessing unauthorized assets, hacking, introducing any computer contaminant or computer virus, committing acts, which may disrupt use of the assets.
- Employees must use organization's mail systems primarily for business purposes.
- Employees must not use organization's information systems to participate in Internet discussion groups, chat rooms, or other public electronic forums.
- Employees must not employ any electronic mail addresses other than official organization's electronic mail addresses for all business matters.
- Employees must not use instant messaging facilities when working with organization's information systems.
- Employees must not access Social Networking sites at any time using organization's computers or personal computers connected to organization's any networks.

Password policy is also an important part of security policy which may include the followings:

- Do not store written passwords or instruction on how to logon to networks with portable computers.
- Personal computers, and computer terminals shall not be left logged on when unattended; and shall be protected by password protected screen savers.
- Passwords or other access tokens for access to organization's systems shall never be stored on mobile devices where they might be stolen or permit unauthorized access to information assets.
- To achieve the minimum level of protection with user password, the following criteria should be enforced:
 - Minimum password length = 8 characters.
 - Password must have at least one non-alphabetic character.

Cyber security policy must meet criteria and conditions to enable the organization to punish and penalize employees who violate that policy without any fear of legal consideration. Those criteria are:

- Cyber security policy must be disseminated and distributed among all employees via internet, e-mail ...etc.
- Cyber security policy must be reviewed and read.
- Cyber security policy must be Comprehension and understandable by all employees (language must be considered).

- Compliance (agreement)
- Uniform enforcement

V. Conclusion

This research addresses human factors and human weaknesses that related to cyber security processes. It shows how cyber security is complex and it shows that cyber security has technical aspects and human aspects. We cover human behaviors that must be dealt with carefully by organization to eliminate potential data breaches. Using weak passwords is a famous behavior that let data to be vulnerable to risks and breaches. Strong passwords criteria must be forced by system administration with no exceptions. More strict criteria must be guaranteed on system administrators' passwords or critical positions on organization's management hierarchy. Sharing passwords must be prohibited and written precisely in cyber security policy. Another danger is leaking information which are so harm for organization's reputation. Leaking information is a crime and each employee must be aware about that and must know legal consequences if this crime was committed. Confidentiality and non-disclosure agreement must be disseminated and signed among all employees of organizations. Accessing to the network of organizations using personal devices without any restrictions exposes the corporate network to data breaches. WIFI-enabled devices must not be allowed to access workplace network unless they have security software and updated. Also, accessing to wireless network is only permitted using two-factors authentication to guarantee the identity of the device owner, i.e. eliminate anonymous users.

Social engineering is a big risk that threaten the workplace network and it's favorite weapon to hackers and attackers. Training programs and awareness activates must be deployed to minimize threat and increase employees' awareness to protect organization against such attacks.

Employees must be responsible and responsive against any suspicious activity that may affect data and information security. Improvement of employee awareness is a high priority task which can be done through training and awareness activities.

Variety of cyber security awareness activities must be performed across the organization to maximize the protection against any attack that may be noticed by employees. To gain higher success value of awareness activities they must be reviewed and improved periodically, and employees must be encouraged or enforced to participate in that activities.

A comprehensive and understandable cyber security policy must be disseminated among all employees. It must be reviewed and improved frequently to be aligned with new cyber security trends and technology. It also must be written in many languages to be easily read by all employees in the organization.

An organization must invest in cyber security technologies as long as attackers and hackers' strategies are evolving and it must give a high priority to reduce impacts of human factors weaknesses by training, awareness and distributed practical and strong cyber security policy. Organizations must benchmark their cyber security practices with other peers or competitors to be at the front as possible. Training end-users against cyber-attacks must be considered in cyber security processes and have a fair budget if the organization wants to protect their information assets and to

Finally, since cyber-attacks and techniques are evolving constantly and dramatically, we suggest more researches of human factors that have impacts on cyber security. New solutions and techniques that fill the gap between cyber security and human weaknesses must be developed, reviewed and improved periodically because we are in a continuous and never-ending cyber war.

References

- [1] Orshesky, C., "Beyond technology – the human factor in business systems", *Journal of Business Strategy*, Vol. 24 No. 4, pp. 43-47, 2003.
- [2] Kerner, SM 2016, 'Global Cyber-security Spending to Top \$100B by 2020: IDC', *eWeek*, p. 1, viewed 4 March 2020, [Online] Available: <http://search.ebscohost.com.sdl.idm.oclc.org/login.aspx?direct=true&db=bsu&AN=118872249&site=eds-live>.
- [3] Whitman, M.E., Mattord, H.J., "Principles of information security. Boston, Ma: Cengage Learning", 2016.
- [4] Asish, M. S., Aishwarya, R., "Cyber Security at a Glance", 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Science Technology Engineering and Mathematics (ICONSTEM), 2019 Fifth International Conference on, 1, pp. 240–245.
- [5] Weak Passwords Caused 30% of Ransomware Infection' (2020) *Software World*, 51(1), pp. 24–25. [Online] Available: <http://search.ebscohost.com.sdl.idm.oclc.org/login.aspx?direct=true&db=asf&AN=141426158&site=eds-live> (Accessed: 7 March 2020).
- [6] Improper Practices Around Passwords the Focus of New Google Study' (2019) *eWeek*, p. N.PAG. [Online] Available: <http://search.ebscohost.com.sdl.idm.oclc.org/login.aspx?direct=true&db=bsu&AN=134644948&site=eds-live> (Accessed: 7 March 2020).
- [7] ADAMA, V. N. et al. (2018) 'Password Knowledge Versus Password Management', *I-Manager's Journal on Computer Science*, 6(3), p. 16. [Online] Available: <http://search.ebscohost.com.sdl.idm.oclc.org/login.aspx?direct=true&db=edb&AN=135838189&site=eds-live>
- [8] Kato, K., Klyuev, V., (2013) 'Strong passwords: Practical issues', 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), 2013 IEEE 7th International Conference on, 02, pp. 608–613.
- [9] Dominion Post, The (2018) 'A word on sharing passwords - don't', 27 January, p. A16. [Online] Available: <http://search.ebscohost.com.sdl.idm.oclc.org/login.aspx?direct=true&db=rps&AN=TDP180127A0161137280438-BH&site=eds-live> (Accessed: 9 March 2020).
- [10] Wai Peng Wong et al. (2019) 'Human factors in information leakage: mitigation strategies for information sharing integrity', *Industrial Management & Data Systems*, 119(6), pp. 1242–1267.
- [11] Anand, K.S. and Goyal, M. (2009), "Strategic information management under leakage in a supply chain", *Management Science*, Vol. 55, No. 3, pp. 438-452.
- [12] Ellefsen, I. (2014) 'The development of a cyber security policy in developing regions and the impact on stakeholders', 2014 IST-Africa Conference Proceedings, IST-Africa Conference Proceedings, 2014, pp. 1–10.
- [13] M. Bezuidenhout, F. Mouton, H. S. Venter, "Social engineering attack detection model: Seadm", *Information Security for*

- South Africa (ISSA) 2010. IEEE, pp. 1-8, 2010.
- [14] K. D. Mitnick, W. L. Simon, *The art of deception: Controlling the human element of security*, John Wiley & Sons, 2011.
- [15] M. I. Mann, *Hacking the human: social engineering techniques and security countermeasures*, Gower Publishing, Ltd., 2012.
- [16] Ghafir, I. et al. (2016) 'Social Engineering Attack Strategies and Defence Approaches', 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Future Internet of Things and Cloud (FiCloud), 2016 IEEE 4th International Conference on, ficloud, pp. 145–149.
- [17] Waly, N., Tassabehji, R. and Kamala, M. (2012) 'Improving Organisational Information Security Management: The Impact of Training and Awareness', 2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems, High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICISS), 2012 IEEE 14th International Conference on, High Performance Computing and Communication & IEEE International Conference on Embedded Software and Systems, IEEE International Conference on, pp. 1270–1275.