Naif Arab University for Security Sciences
Journal of Information Security & Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

Overview of the Impact of Human Error on Cybersecurity based on ISO/IEC 27001 Information Security Management

Amar Yasser El-Bably*
Egyptian Police Academy, Egypt

Received 07 Apr. 2021; Accepted 29 May. 2021; Available Online 01 June. 2021

Abstract

Information security is the practice of protecting information by mitigating the risk of cyber-attack, and typically includes preventing or reducing the possibility of unauthorized/inappropriate access to data, unlawful use, disclosure, disruption. This concept of information security covers as well various procedures aiming at minimizing the negative effects of such incidents and threats. These threats might be originated from the human behavior which may lead to a wide damage of the organization data assets. Thus, the primary focus of information security is on the balanced protection of confidentiality, integrity and availability of data while maintaining an effective use of the organizations' systems. International standards related to information security such as ISO/IEC 27001 emphasis on effective implementation of the information security policies and applications without hampering the productivity of the organization. This research seeks to draw a set of practical rules to be established within an organization in order to preserve cybersecurity objectives and protect dada specifically from human errors incidents. The drawn rules are based on ISO/IEC 27001 and its application within organizations will rise the employees awareness about their behavior to reduce the impact of such incidents on the organization' systems and data.

I. Introduction

Cybersecurity has become an essential part of all institutions and sectors, particularly the security and political agencies of countries, as it has become known that decision makers in the United States of America, the European Union, Russia, China, India and other countries have classified it as a priority in their national defense policies.

More specifically, cybersecurity refers to the sum of the technical, regulatory and management means used to prevent unauthorized use, abuse and recovery of electronic information, communication systems. The main objectives of cybersecurity are: to ensure the availability and continuity of the work of information systems, to maintain confidentiality and privacy of personal data and to preserve the integrity of the data.

Cyberspace based as a hypothetical domain on computer systems, internet networks and a huge stock of data and information, so that networks are connected via computers, phones and other smart devices without adhering to geographical boundaries. The term cyberspace appeared in the 1980s in one of the science fiction novels of the American-Ca-

Keywords: Cybersecurity, Information security, human error, Information security management, ISO/IEC 27001.

Production and hosting by NAUSS

* Corresponding Author: Amar Yasser El-Bably
Email: 3marelbably@gmail.com
doi: 10.26735/WLPW6121

nadian writer William Gibson. The current era is described as digital age as it includes tremendous technological developments that serve all aspects of public and private life, reflected in the service of the entire international community. This digital era is moving through information and communication technology, which has been accompanied by a major criminal movement. Indeed, the spread of information crimes through using viruses, spyware, tools that can be described metaphorically as: the germs used or fabricated (Synthetic Viruses) [1].

Modern technologies have proven that they are not able to control the behavior of human beings, and to ensure the safety of individuals, institutions, and states, which have become more dependent on them. The most advanced countries have sounded the alarm, and on many global platforms, to draw attention to that situation. Therefore, the organic imbalance affecting software and equipment can be easily exploited by experts in breaching the information systems [2].

Strengthening trust and security in the use of information and communication technologies (ICT) will strengthen the framework of reassurance. This latter includes information security, security of the safe guarding privacy and confidential protecting the citizen employed, which is a precondition for the establishment of electronic and intelligent government projects for the development of the information society ,which requires us to protect all information systems ,take all measures of insurance against all types of threats system on information and data, and use together to ensure the comprehensiveness of information security [3].

On the other hand, the risks related to the human element at all different levels are one of the areas of interest for information security agencies, as there is an opportunity for people from within to achieve what no one from abroad can theoretically achieve. Thus, the problem of detection difficulties remains if there is no performance system and powers that provide protection, warning and penetration detection systems, therefore electronic human security remains one of the most dangerous types of electronic intrusion and threats [2].

The process of identifying human risks begins by visualizing every risk that may affect the information, and at the level of users it is necessary for the enterprise to develop sufficient guidance to ensure a general and accurate awareness of information security issues. Raising the awareness of employees helps at establishing a culture of security among employees, which is divided between the obligation to observe the ethics of the use of technology and the procedures required of all when noticing any defect [3] .

The International Organization for Standardization (ISO) cooperates closely with International Electrotechnical Commission (IEC). ISO/IEC 27001 standard developed by ISO and IEC cooperation is a widely valued information security standard. This standard includes comprehensive list of security controls and objectives called Annex A. This latter consists from 14 clauses that include 35 controls categories and 114 controls. One main change in the latest versions of this standard is that the controls are no longer set as strict requirements to manage risks. Instead, the use of the security controls are optional and the companies have the ability to choose the suitable controls [15].

Based on this standard, this paper seeks at drawing practical steps to adhere to in order to reduce the human errors within companies that are related to cybersecurity.

The rest of the paper is as follows: Section II will highlight the human errors on cybersecurity. Section III will discuss reasons of human errors on cybersecurity , Section IV summurises a set of rules to strengthen the security of information centers and sites and achieve the desired security goal.

II. Human Error: Understand the Mistakes that Weaken Cybersecurity

Table I shows that the types of human errors when dealing with cybersecurity. The percentage of human error is always higher in the types of electronic intrusions : 43% of US and UK employees have made mistakes resulting in cybersecurity repercussions for themselves or their company, according to a Tessian report.

- With human error being a leading cause of data breaches today, the report examines why people make mistakes and how they can be prevented before they turn into breaches.
- When asked about what types of mistakes they have made, one-quarter of employees confessed to clicking on links in a phishing email at work. Employees aged between 31-40 were four times more likely than employees aged over 51 to click on a phishing email, while men were twice as likely as women to do so.
- 47% of employees believe that distraction is the main reason for falling for phishing scams and (41) of email, scams, and non-genuine brands.
- In addition to clicking on a malicious link, 58% of employees admitted to sending a work email to the wrong person, with 17% of those emails going to the wrong external party (especially via What Sapp messages contaminated with viruses and harmful links).
- This simple error leads to serious consequences for both the individual and the company, who must report the incident to regulators as well as their customers. Companies had lost customers as a result of sending a misdirected email, while 12% of employees lost their job.
- The main reason cited for misdirected emails was fatigue (43%), closely followed by distraction (41%). With 57% of respondents saying they are more distracted when working from home, the sudden shift to remote working could make businesses more vulnerable to security incidents caused by human error.
- Proof point worryingly found that 50% of respondents admitted to allowing family or friends to use their work-issued device. While the motives behind this may be harmless (the most common reason is to check email). The UK Information Commissioner's Office (ICO) stated that the vast majority (90%) of electronic data breaches in the UK in 2019 were due to human error [12]. Also, Kaspersky's IT security economics in 2019 report tells us that "inappropriate IT resource use by employees" is the most common cause of a data breach, with 50% of SMBs reporting these types of incidents [5] as shown in Fig. 1.
- For these reasons, the researcher believes that all users must comply to the cybersecurity policies seeking to maintain the principle of privacy and confidentiality of information and data within their jobs, and apply the rules and principles of information security within information templates, such as information security policies in the system (ISO / IEC 27001 Information Security Management) [3].

TABLE I

MAJORITY POINTS OF HUMAN ERROR IN CYBER SECURITY [2]:

Using weak passwords	Performing unauthorized system changes	Almost half of workers trust public wifi hotspots
Using personal devices for work purposes	Ignoring software updates	workers do not lock their smartphones
Using public Wi-Fi without a VPN	Disabling security features	workers share access to an employee-issued device with family and friends.
Plugging in insecure devices	Downloading unauthorized software	Misdelivery and misconfiguration are among the top causes of data breaches

A. Misdelivery and Misconfiguration as Causes of Data Breaches

- Verizon's 2020 Data Breach Investigations Report further sheds light on the matter and analyzes the causes of data breaches in a slightly different manner. It found that phishing is the top threat action variety in breaches, playing a role in more than 20 percent of cases. Other human errors (misdelivery and misconfiguration) were in the fourth and fifth spots respectively, each representing the top threat action in around 10 percent of breaches, in addition, the report found that some of the top malware vectors in data breaches are human error related. Email links download by malware, and email attachments held the first, third, and fourth spots, respectively.

- When it comes to the high-level actions that cause data breaches, error is the only one that continues to increase in frequency.

B. Password Reuse

Making it sit in obsolete practices, exposing in command, this has been written writing a password in place, and in order to get people to practice secure password practices, there are lots of numbers floating around about the prevalence of password reuse, but the fact of the matter is that it's far more common than it should be. Here is some data that shines a light on this issue which affects both personal and work accounts:

- The Google/Harris Poll study found that 66% of users reuse passwords across accounts.
- Microsoft found that 44 million users were reusing passwords across accounts.
- Another Google survey discovered 13% of users utilized the same password for every account and an additional 52% used the same password on multiple accounts.
- 72% of respondents to the HYPR survey admitted to reusing passwords.
- LastPass discovered employees were happily reusing passwords on 13 different accounts.
- According to the Ponemon Institute's The 2020 State of Password and Authentication Security Behaviors Report, IT professionals are the worst offenders, with 50% reusing passwords compared to 39% of other employees.

C. Employee Actions lead to Cybersecurity Incidents

- Staff may make mistakes that put their company's data or systems at risk – either because they are careless and accidently slip up – or even because they do not have the required training to teach them how to behave appropriately and to protect the business they work for as illustrated in Fig 2.
- Despite the prevalence of automated systems, the human factor can jeopardize major industrial processes, and employee errors or unintended actions lead to more than half of cyber security incidents in industrial networks.
- Organizations and governments are short of professionals to deal with new threats, and organizations are also concerned that OT/ICS network operators are not fully aware of behavior that could cause cyber security breaches [11].

III. Reasons of Human Errors on Cybersecurity

Users represent a real threat for many reasons, including that the limits of institutions, government and service agencies in the govermental institutions continue to expand as the number of employees increases. This increase of various employees makes their personal and professional uses meet in the points and terminals of the institution in which they work. As a consequence, work computers have become more personal and thus store applications that are not related to work, which will introduce the institution to spyware, hackers and other threats[10].

There is also an increased latent risk due to curiosity among users in information centers, known as internal social engineering. This latter might be in the form of e-mail messages designed to defraud employees, in order to perform malicious and hacking operations that have a significant impact on the security of the government and security institution. The reasons for these intended malicious activities can be due to several reasons [10]:

- **Financial reasons:** the goal of misappropriation of instruments, shares, bonds or convertible securities, or data change, to find prohibited financial settlements as well as steal and resell information to rival parties.
- **Intellectual reasons:** these reasons are the most challenging motives where there is nothing to consider financial or emotional in them. The actor may do so to satisfy his intellectual curiosity or out of the challenge of disproving the line administration when they announce that it has a security system and cannot be penetrated, or dealing with terrorist entities and organizations or countries with interests that harm the interests of the nation.

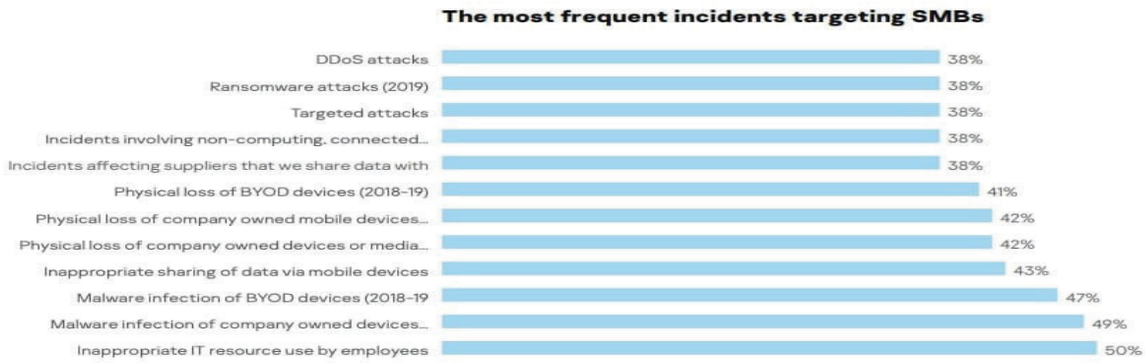

Fig. 1 Most of human error in cybersecurity [3].

- **Negligence:** is the most common way that facilitates information disclosure, due to the negligence of employees and their lack of awareness of the importance of maintaining the confidentiality of information and the serious consequences of hacking information security. As well as bein unaware of the data that consititue an asset to the company or unaware of who has the motive to exploit this valuable information from inside and outside the organization.
- **Risks of social engineering:** This goes beyond protecting employees from social engineering, which is a set of techniques used to get individuals to do something or disclose confidential information and used within internet fraud to achieve the victim's purpose, as the primary objective of social engineering is to ask simple or trivial questions (by phone or email with impersonation of an authority or a business that allows him to ask questions in this way without arousing suspicion).

IV. A set of Rules to Strengthen the Security of Information Centers and Sites and Achieve the Desired Security Goal, as Follows:

- Limit security responsibility to the first official of the information center or on his behalf, such as the security official of the information sites in the various security sectors.
- Non-officially charged persons are not allowed to work after official working hours, or to enter the information centers in general.
- A special record has been placed in the information center. Management of information center queries names of visitors, the reasons for their entry and the time of their departure, all should be noted daily by the director of the center or the security official.
- Ensure that people who wish to enter (information centers) only after verifying their identity, and the need to focus on the reason for their entry whether they are visitors or authorized to use the system or maintenance engineers etc.
- The need to hold seminars from time to time and in the presence of the Director of the Information Center to educate workers on the need to maintain the security and confidentiality of data, the safety of computers and accessories and the seriousness and importance of information and data.
- Monitoring the physical condition of employees, especially those working in important and sensitive locations within information centers and sites, because they may be prompted by bad material to disclose secrets and carry out the plans of other terrorist entities.
- The need to close all ports leading to information centers in order to be better able to control it, and to close this port after the end of official work period even if there are staff working at this time.
- Setting up confidential key code for each working person enables them to access only their respective files of interest without being able to access other files.

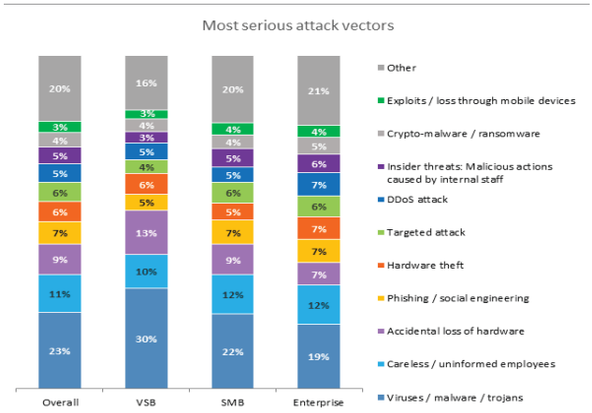

Fig. 2 IT Security Risks Survey 2017, global data[4]

- Design systems so that information and data can only be changed by a special committee for this purpose, so that each member has a portion of the keywords which no one else knows and therefore can open the system only in their presence.
- The need to control communication issues in terms of internal and external communications means and applications, document communication movements and protect communication processes and technical standards, and secret strategies, control, tracking and use of e-mail.

V. Main Information Security Controls Applied to Prevent Human Errors as per ISO Standard ISO/IEC17799

Information is a valuable asset that directly affects the progress or development of institutions, so when managed effectively, it allows institutions and sectors to operate with complete confidence, and there are controls for the security of information about the human element within the ISO quality standard for information security and I will mention the most important ones as follows:

- Information security controls for iso/iec17799 within the security or service institution of the human element [8].
- Information security controls for iso/iec17799 [11] within the security or service institution for safe areas.

From the previous standars we can draw practical steps to state how to prevent human errors as follows, as mainly illustrated in Fig 3:

Update your corporate security policy. Your security policy should clearly outline how to handle critical data and passwords, who can access them, which security and monitoring software to use, etc. Revise your security rules and check whether all current best practices are reflected in the document [15].

Educate your employees. make your employees aware of potential threats and explain how dangerous and expensive the consequences of their mistakes can be. You should educate your employees about risks such errors pose to the organization's security. Make sure everyone is familiar with the corporate security policy and is motivated to follow the rules [17, 18].

Use the principle of least privilege. the easiest and most reliable way to secure data access is to deny all access by default. Allow privileged access only when needed on a case-by-case basis. If users can only access data required for their work, you can prevent accidental data leaks and data deletion caused by employees who are not supposed to work with certain sensitive data in the first place [18].

Monitor your employees. do reinforce the habits of backing up important data and information and the data should be stored on a local flash drive inserted in their laptop, they should back it up to the cloud or another hard drive. If employees store their data primarily in the cloud, they should make sure that there is another copy somewhere without an internet connection with adequate security of the cloud using virus protection software, firewall and data encryption software with authentication for barometric security to increase the security as well as two-factor authentication with Smart phones and mobiles [16].

Promote good data-backup habits with so many employees working remotely, it is harder for organizations to manage backups and store data on the corporate network. Encourage employees to be responsible and back up their data regularly. If they store data on a local flash drive inserted into

their laptop, they should back it up to the cloud or another hard drive. If employees store their data primarily in the cloud, they should be sure to have another copy somewhere offline.

Encourage stringent cyber hygiene. all employees, especially those working at home, need to be regularly reminded to update the software on their devices and to enable all available security features, such as firewalls and anti-malware. Failing to install updated software and security patches is a well-known employee misstep that creates the gap for malware and ransomware to seize upon.

Limit the number of files employees can access. employees should only be able to access data and folders based on the "information security" principle. This is the concept of giving employees only adequate access to perform their required jobs. Until the employee could accidentally delete or destroy the files, they weren't supposed to be able to access them in the first place. Thus greatly reducing the risks caused by human error [17].

VI. Conclusion

Technological advant is increasing rapidly. Organizations are more dependent on information and technologies to rise up their business. As the organizations grow, systemes within the organzation require a cerfull attention to maintain their securiyt. Information security is about acheiving the the three main goals : confidentiality, integrity and availability through different measures and mechanisms. Risks that threaten the information security are unlimited, but many of them are due to human behavior within the organzation. Therefore, internation standards are mainly procedures that aim to realse some sets to be followed by employees, and by this, a control of the human behavior within the oranozation is eached. This control reduces incidents that may lead to huge damages on the organization information security in general.

References

[1] Department for Digital, Culture, Media & Sport, "Cyber Security Breaches Survey 2019." July 1, 2019. [Online] Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950063/Cyber_Security_Breaches_Survey_2019_-_Main_Report_-_revised_V2.pdf

[2] Ponemon Institute, "The Human Factor in Data Protection." Jan. 2012. [Online]Available: https://www.ponemon.org/local/upload/file/The_Human_Factor_in_data_Protection_WP_FINAL.pdf

[3] "2020 User Risk Report," Proofpoint, California, USA. 2020. [Online]Available: https://az659834.vo.msecnd.net/eventsairaueprod/production-aisa-public/442f8d3e-be7445049ca67e2e7d20f348

[4] "Online Security Survey: Google/Harris Poll." Feb. 2019. [Online]Available: https://services.google.com/fh/files/blogs/google_security_infographic.pdf

[5] "The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within." [Online] Available: https://www.kaspersky.com/blog/the-human-factor-in-it-security/

[6] A. H. Mahmoud, *sariqat almaelumat almukhzanat fi alhasib alalii* [Theft of information stored in the computer], Cairo, Egypt: DAR ALNAHDA, 2006.

[7] H. M. Hemida, and N. A. Jad, *almadkhal fi dirasat albahth aljnayy* [Introduction to the study of criminal investigation], Cairo, Egypt: Police Academy, 1997.

[8] I*nformation technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*, ISO/IEC 27006:2007, International Organization for Standardization. Mar. 2007. [Online]Available: https://www.gso.org.sa/ar/e-services/gulf-encyclopedia/iso-iec-27001-the-foundations-and-principles-of-the-confidentiality-of-the-information-management-system/

[9] J. R. Vacca, *Computer Forensics: Computer Crime Scene Investigation*, Hingham, MA, USA: Charles River Media, 2002, pp. 422-425.

[10] H. Alawi, "Protection of intellectual property in the digital environment through the perspective of university professors: Mentouri University professors as a model," (in Arabic) *Cybrarians J.*, No. 12, Mar. 2007. [Online] Available: http://journal.cybrarians.info/index.php?option=com_content&view=article&id=392:2009-07-20-10-05-45&catid=150:2009-05-20-09-56-20&Itemid=55

[11] M. S. Gadelrab, M. Elsheikh, M. A. Ghoneim and M. Rashwan, "BotCap: Machine Learning Approach for Botnet Detection Based on Statistical Features," in *Int. J. Commun. Netw. Inf. Secur. (IJCNIS)*, vol. 10, no. 3, pp. 563-579, Dec. 2018.

[12] T*he foundations and principles of the confidentiality of the information management system*, ISO/IEC 27001, International Organization for Standardization, pp. 143-144.

[13] https://www.webometrics.info/en

[14] I*nformation technology — Security techniques — Code of practice for information security management*, ISO/IEC 17799, , International Organization for Standardization.

[15] A. Renvall, "Improving cybersecurity through ISO/IEC 27001 information security standard," M.S. thesis, Metropolia Univ. Appl. Sci., Helsinki, Finland, Nov. 26, 2018. [Online]Available: https://www.theseus.fi/bitstream/handle/10024/157277/Renvall_Aleksi_final.pdf?sequence=1&isAllowed=y

[16] M. McConnell, "Cyber Insecurities: the 21st Century Threatscape," in *America's Cyber Future Security and Prosperity in the Information Age*, K. M. Lord et al., Ed, Washington, USA: Center for a New American Security, June 2011.

[17] J. M. Liepman Jr., "cyberspace : The Third Domain," The Wright Stuff Maxwell AFB, AL, Air University, December 13, 2007. [Online]Available: http://www.au.af.mil/au/aunews/archive/2007/0223/Articles/Cyberspace%20Third%20Domain%20-%20Liepman.pdf

[18] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda," *The TQM J.*, vol. 33, no. 7, pp. 76-105, 2021, doi: 10.1108/TQM-09-2020-0202.