

CSG3309 IT Security Management

White Paper



Family Name: David Selvam

Given Name: Visahl Samson

Student Number: 10498743

Name of Lecturer: Gaven Henry

Campus: PSB Academy, Singapore

Due Date: 30th March 2020

Contents

[Executive summary 2](#_Toc36326205)

[Introduction 2](#_Toc36326206)

[Human error 2](#_Toc36326207)

[Human error causes and impacts 3](#_Toc36326208)

[Data breaches occurred due to human error 4](#_Toc36326209)

[McCumber cube 4](#_Toc36326210)

[Education 4](#_Toc36326211)

[SETA programs 4](#_Toc36326212)

[Simulated attacks 4](#_Toc36326213)

[Policy 5](#_Toc36326214)

[Password policy 5](#_Toc36326215)

[Information disclosure policy 5](#_Toc36326216)

[Technology 6](#_Toc36326217)

[Employee Monitoring software 6](#_Toc36326218)

[Cryptography and Encryption 6](#_Toc36326219)

[Identity and access management 7](#_Toc36326220)

[2-factor authentications 7](#_Toc36326221)

[Upcoming landscape 7](#_Toc36326222)

[Conclusion 7](#_Toc36326223)

[References 8](#_Toc36326224)

# Executive summary

This whitepaper explains one of the information security threat, human error. A short brief about human error has been explained. The impact of the human error on the organization section explains how the primary reasons such as ignoring policies and poor information security practices result in security incidents. Security breaches due to the human error section explain how one of the biggest data breaches in history which is Target data breach occurred a result of human error. The next section explains how the McCumber cube model can be applied here to place countermeasures for this threat. In McCumber approach education section explains how the SETA program and simulated attacks can be useful. The policy section explains how password policy, information disclosure policy will be effective against human error threat. Finally, the technology section briefs how employee monitoring software, cryptography, identity and access management, and 2FA will be effective. The upcoming landscape part provides a brief about a few future cybersecurity predictions. Finally, the conclusion section briefing why human error should be a primary point to consider in information security.

# Introduction

In this technology era, information security plays a vital role everywhere from industrial to business. Maintaining information security in an organization enables it to function and ensures continuous operations. The information security threat the requires more attention in John Dough’s Pizza is human error. The reason behind choosing this as the primary threat is 3 previous security breaches in John Dough Pizza are fully due to human error while others as partially due to human error. Moreover, the secret survey results indicate that the employees are not happy with the management which can result in an entirely new threat known as an inside threat. This report covers what is human error, how it impacts the organizations, and how this can be significantly reduced.

# Human error

In cybersecurity chain, the human is the weakest link from the very beginning. Also, a survey conducted by a reputed organization (Swinhoe, 2019) in 2019 proves the fact remains unchanged even now. In information security, human error can be classified into 2 categories either intentional or unintentional. The intentional one can occur due to another threat known as insider threat which has some motivations behind it whereas unintentional has no motivational or any pre-planning it might be due to many reasons such as not knowing how a particular technology works, or absence of awareness.

According to research conducted by Kaspersky (Kaspersky, 2017), in 2017 nearly 49% pf malware/virus attacks are consisting of human error as contributing factors. In these attacks 53% are due to careless/uninformed employees, 36% of social engineering/phishing attacks, 38% is accidental hardware loss by the employee. Furthermore, as per Verizon’s 2019 data breach investigation report (Verizon, 2019), 34% of the data breaches are due to the threat of human error.

## **Human error causes and impacts**

The above-stated statistics show that how much human error contributing the data breaches. So, now the organizations must find how these happen and how severely it can affect it. Several reasons can cause human error.

The primary one is ignoring and/or not aware of workplace policies. In this scenario, the employee would have probably now aware of information security policies of the organization so the employee would have certainly violated the policy resulting in a security incident.

Another reason would be not aware of common security practices. Information security awareness includes classifying phishing/spear-phishing emails, malicious email attachments, poor passwords, etc... Without this basic information, security awareness employee would potentially become a prey to the attacker/hacker. Because currently in cyber field attackers not targeting the company’s executive/board members rather they’re targeting low-level employees. Recently in the USA, it is reported (Lindsey, 2020) that hackers are targeting the potential employees to spread malware on the organization’s system.

The third primary reason would be negligence. This may include failure to do the work properly. Mostly, this factor would be unintentional, but it delivers a significant impact to the organization.

## **Data breaches occurred due to human error**

There are several data breaches occurred due to human error. The well-known and famous data breach that occurred due to human error is Target Data Breach occurred in the year 2013. Data breach studies (Xiaokui, Danfeng, Ke & Andrew, 2017) indicate that the data breach consists of several human error facts. Firstly, the malware has been planted into the systems in a sophisticated phishing attempt. Secondly, the security warnings have been ignored and no actions taken against the warnings generated by the monitoring software. According to reports, the total cost of this data breach is nearly 300 Million USD.

# McCumber cube

McCumber cube methodology can be used in organizations to reduce the risk and impact caused by human error.

## **Education**

### **SETA programs**

SETA stands for Security Education, Training, and Awareness. SETA program is an education program (Solms, S.H. & Solms, Rossouw. 2009) that aimed to educate employees to reduce the data breaches due to human error and increase the information security awareness among them. Implementing SETA programs is one of the recommended (M.G. Lee, 2012) method and is followed by many organizations at this moment. According to ISO27001 Clause A.8.2 (Calder & Watkins, 2015), an organization should enable this SETA program to not only its employees also to its relevant contractors, and third-party users also. Conducting SETA programs at least once in a year is a recommended measure.

### **Simulated attacks**

Simulated attacks that are designed by the organizations help to test employee’s knowledge of security practices. These are similar to fire drill exercises. In simulated attacks, the organization sends phishing/malicious email/email attachments to the employees to see how well the employees are identifying them and responding to them. This one also widely used in the organisation nowadays and one of the recommended methods to follow (Rapid7, 2018).

## **Policy**

Policies play a vital role in controlling/preventing the impact of human errors. The most recommended and important policies are password policy and information disclosure policy

### **Password policy**

The primary purpose of the password policy is to create a standard of making a strong password, protection of those passwords, and enabling frequently changing passwords. The password policy applies (Sans, n.d.) to all the personnel who are responsible for any account, any system that is being used inside the organization, network, and facility to store any information. The following is an example of a password policy according to NIST 800-63 (NIST, 2020) guidelines.

* Password should be a minimum of 8 characters when it being set-upped by people
* Password should be a minimum of 6 characters when it being set-upped by a service/system.
* The password should support all the ASCII characters including space.
* Chosen passwords should be checked with a password dictionary.
* Password should support at least 64 characters of maximum length.
* Minimum of 10 attempts before the lockout.

Apart from those NIST framework guidelines, there are some more options which can be added to the password policy,

* Passwords must be changed every 90 days.
* The password should contain at least one upper case letter, one lower case letter, one symbol, and one number. This will help to increase the complexity of the password.

### **Information disclosure policy**

According to ISO27001 Annex A.7.2 (Humphreys, 2016), organizations should make agreements whenever new employees join the organization. This also called a Non-Disclosure agreement which states what is the information that can be disclosed to the public and what is the information that cannot be disclosed out the organization. Also, the agreement should clearly state the actions to be taken in the event of a breach of the Non-disclosure agreements. Apart from that its important that the organization should take appropriate measures to aware its employees about the agreement.

Furthermore, an organisation can use data classification policy to make this work easier. Data classification helps the organization to classify in terms of confidentiality. A typical data classification has 4 levels (Irwin, 2019) they are, confidential (only higher management must access), Restricted (only particular job roles can access), internal (all the employees can access), public (everyone can access). Classifying the information allows an employee to aware of the information that they can disclose.

Apart from these two policies organizations can consider another policy for BYOD (Bring Your Own Device). Also, organizations are advised to run periodic internal audits/reviews to ensure security measures.

## **Technology**

The usage of proper technology will significantly reduce the occurrence of human error. Few technology measures that can be placed to prevent human errors are,

### **Employee Monitoring software**

Usage of Employee monitoring software is a basic mechanism that can be utilized by the organization to reduce the occurrence of human error. This facility allows to monitor every activity of an employee so if any security incidents occur information from the monitoring system can be used to find the root cause/where it begins. There are several ethical issues associated with this but using this with acceptable policies such as what data can be collected will be beneficial.

### **Cryptography and Encryption**

Encryption is the most recommended technology countermeasure to protect against threats especially human error. Organizations should use encryption while data at rest (Robb, 2017). Also, the algorithm going to be in place should be secure enough and in general, instead of creating a new algorithm, it’s wise to choose already existed one. Currently, in the industry, there are several vendors like IBM, Dell, McAfee providing their cryptography and encryption products.

### **Identity and access management**

Allowing the employee to access only what they require for their job roles would be an appropriate strategy. Also, deploying identity and access management (IAM) in place would be helping to reduce the risk.

### **2-factor authentications**

Currently, usage of 2 factor/multi-factor authentication is emerging among the organizations to provide an additional layer of support. According to research reports (Sans & Preston, 2014), the intention of adopting to 2FA is significantly increasing.

# Upcoming landscape

According to the security organization’s future cyber-attack landscape predictions (Checkpoint, 2019), it is estimated that the phishing-based attacks will remain as a top attack vector and it will increase rapidly. another prediction (Jason, 2019) estimated that the Phishing vector will go beyond the email and launch through cloud application. So, when the attack vectors evolve the organizations need to keep their tactics up to date to combat them.

# Conclusion

Since this threat vector is from the human it cannot be eliminated rather the countermeasures can help to stop human error turning into potential security breach which may cause severe impact to the organizations. Also, in cybersecurity, technology is not a single solution to solve all the problems rather its everyone’s shared responsibility to keep the digital world safe.

# References

Calder, A., & Watkins, S. (2015). *IT Governance: An International Guide to Data Security and ISO27001/ISO27002*. London: Kogan Page Limited.

Checkpoint. (2019). 2020 Vision: Check Point’s cyber-security predictions for the coming year - Check Point Software. Retrieved from <https://blog.checkpoint.com/2019/10/24/2020-vision-check-points-cyber-security-predictions-for-the-coming-year/>

Humphreys, E. (2016). *Implementing the ISO/IEC 27001* (2nd ed.). Norwood: Artech House.

Irwin, L. (2019). What is information classification and how is it relevant to ISO 27001? - IT Governance UK Blog. Retrieved from <https://www.itgovernance.co.uk/blog/what-is-information-classification-and-how-is-it-relevant-to-iso-27001>

Jason, C. (2019). Cybersecurity Predictions for 2020. Retrieved from <https://www.netskope.com/blog/cybersecurity-predictions-for-2020>

Kaspersky. (2017). Retrieved from <https://media.kasperskycontenthub.com/wp-content/uploads/sites/100/2017/11/10083900/20170710_Report_Human-Factor-In-ITSec_eng_final.pdf>

Lindsey, O. (2020). Iranian Hackers Target U.S. Gov. Vendor With Malware. Retrieved from <https://threatpost.com/iran-hackers-us-gov-malware/152452/>

M. G. Lee, "Securing the human to protect the system: Human factors in cyber security," 7th IET International Conference on System Safety, incorporating the Cyber Security Conference 2012, Edinburgh, 2012, pp. 1-5.

NIST. (2020). NIST Special Publication 800-63B. Retrieved from <https://pages.nist.gov/800-63-3/sp800-63b.html#sec5>

Rapid7. (2018). *WHY YOU SHOULD LET YOUR SECURITY TEAM GO PHISHING*. Rapid7. Retrieved from <https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-whitepaper-why-you-should-let-your-security-team-go-phishing.pdf>

Robb, D. (2017). Top 10 Enterprise Encryption Products. Retrieved from <https://www.esecurityplanet.com/products/top-encryption-products.html>

Sans. Retrieved from <https://www.sans.edu/student-files/projects/password-policy-updated.pdf>

Sans, & Preston, A. (2014). *Global Information Assurance Certification Paper*. Sans Institute. Retrieved from <https://www.giac.org/paper/gsec/35160/impediments-adoption-two-factor-authentication-home-end-users/139464>

Solms, S.H. & Solms, Rossouw. (2009). Information Security Education, Training and Awareness. 10.1007/978-0-387-79984-1\_10.

Swinhoe, D. (2019). Humans are the weak link: Security awareness & education still a challenge for UK companies. Retrieved from <https://www.csoonline.com/article/3430596/humans-are-the-weak-link-security-awareness-education-still-a-challenge-for-uk-companies.html>

Verizon. (2019). Verizon: 2019 Data Breach Investigations Report. *Computer Fraud & Security*, *2019*(6). doi: 10.1016/s1361-3723(19)30060-0

Xiaokui, S., Danfeng, Y., Ke, T., & Andrew, C. (2017). Breaking the Target: An Analysis of Target Data Breach and Lessons Learned. *Arxiv*. doi: 701.04940v1