The Human Factor
Report

Queens Medical Centre

ASMIS Report – The Human Factor

Contents

1 Introduction

Queens Medical Centre is a community clinic that has recently installed a web-based Appointment and Scheduling Management Information System (ASMIS) for patients to schedule appointments with specialists. The clinic's management is concerned about the government's patient data protection policy and the current high rate of cybercrime. The clinic's IT staff implemented an ASMIS, which is considered secure. The management knows that investing in technical solutions alone is insufficient to achieve optimal security and that human elements also need to be considered. This report looks at the various human factors that must be considered for ASMIS to be secure and usable.

2 The Human Factor

Human factors in cybersecurity refer to behaviours or occurrences that cause a data leak, and these elements are primarily the product of ignorance, carelessness, or improper access control. The cost of human errors adds up, and SMEs spend almost $3.33 million (IBM, 2022) on average on data breaches due to human error. Human error contributes to 88% of data breaches (CYDEF, 2021).

Companies must first recognize that their employees are their most valuable resource if they are to handle the human component of cybersecurity. Individuals have a tremendous capacity to defend against a cyber-attack when given the proper resources and education.

3 Threats due to the human factor

3.1 Phishing

Despite major improvements to email security over the years, phishing is still prevalent mainly due to two reasons:

- It is straightforward to craft and requires much less expertise.
- It is more efficient and scalable than trying to brute force into a network.

Users should be even more cautious in the coming years because the 0.1% of phishing emails that get past email filters still generate a substantial income for criminals, who will be sending out more of them (Auth0 - Blog, n.d.).

3.2 Usability vs Complexity

Complexity is the enemy of compliance (www.securitymagazine.com, n.d.). Complex security solutions lead to users finding shortcuts around it or the system's efficiency going down, and both are not desired outcomes. This would include users choosing weaker passwords, storing passwords insecurely and incorrect handling of passwords.

Figure 1: Data Breach Report (www.ekransystem.com, 2019)

3.3 Insider Threats

The second most common reason for a severe security compromise is careless or ignorant workers (Kaspersky, 2017). Figure 1 shows the most serious attack vectors where the human factor contributed most.

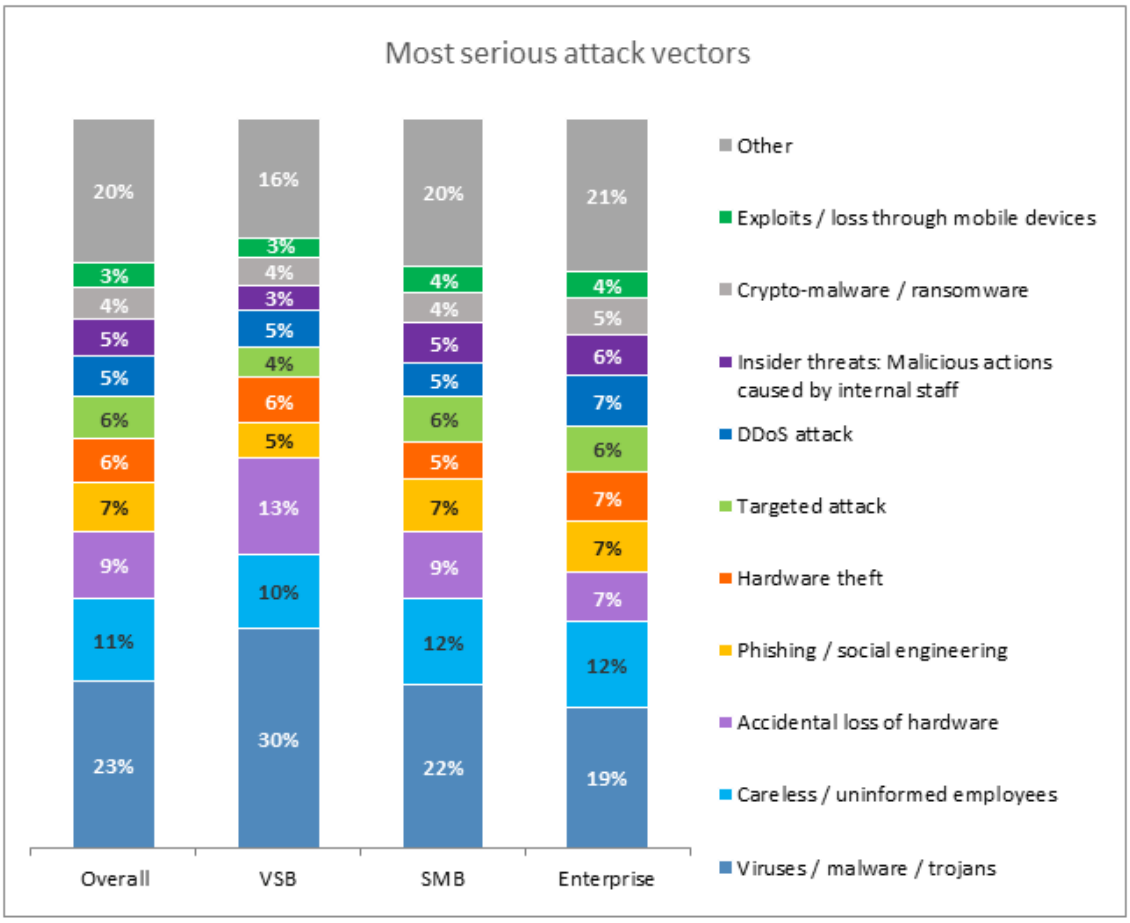

Figure 2: Most Serious Attack vectors (IT Security Risks Survey, 2017)

Businesses are increasingly falling prey to other "attack vectors" besides employee error. Internal employees have also contributed to security problems in the past year through malevolent acts. Employees acting against their organizations were reportedly involved in 30% of security incidents in the previous 12 months (Kaspersky, 2017).

Figure 3: Cyber Security trend (Jacqueline von Ogden, 2016)

The following are some other factors to consider:

- **Age is not a measure of know-how:** Users aged 31-40 are more likely to click on a phishing link than users ages 51+. Older users take great satisfaction in their closed networks and decision-making skills, enabling them to leverage their experience to detect something that does not feel right.
- **People are Afraid of Mistakes:** Users worry about missing an essential email, and if they are required to answer emails so rapidly, they are inclined to click phishing or ransomware links. Notably, tech and financial services users are most prone to click on phishing links (CYDEF, 2021).

4 Implications on ASMIS

Figure 4 shows the actors involved in ASMIS.

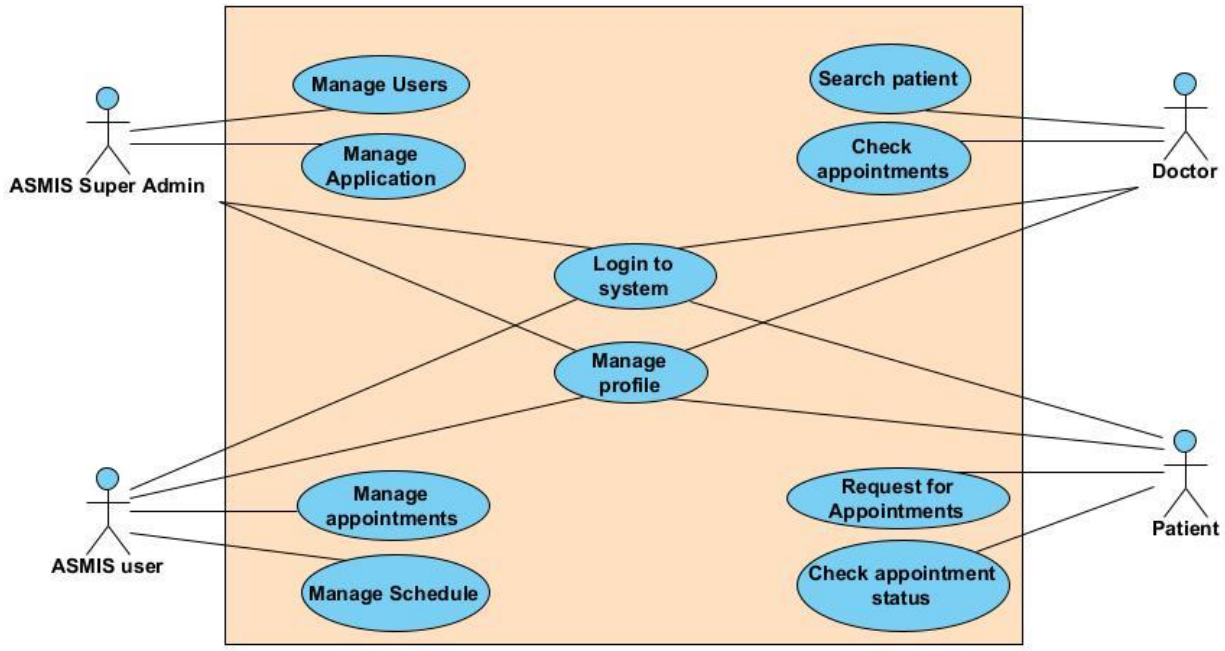

Figure 4:: ASMIS Use case diagram

A significant implication of phishing on the ASMIS system would be the loss of patient data. Queen Medical Centre would be held liable when sensitive patient information is in the public domain. In addition to monetary loss, heavy fines can be places for mishandling health-related information. As covered earlier, phishing is incredibly easy to craft, and this could be compounded by opting for usability over security. Especially when it comes to super admins and Doctors who handle the application and manage patient data, security must be given higher priority.

One of the most prevalent types of insider threat is staff negligence. Even though they might operate in a compliant manner, they might not realize the consequences of their occasional mistakes until much later. This also includes persistent non-responders. Some

employees, most notably higher-ups, frequently show habits that make them susceptible to targeted phishing assaults and are unresponsive to security awareness training (Redscan, n.d.).

Another implication of insider threat is reputation loss, which is challenging to measure. A breach in ASMIS, leading to sensitive patient data loss, will negatively impact the existing customer base. According to Cisco, 42% of the firms that experienced a breach lost approximately 20% of their existing customer base (Thompson, 2017).

References:

Auth0 - Blog. (n.d.). Why Phishing Attacks Work. [online] Available from: https://auth0.com/blog/why-phishing-attacks-work/ [Accessed 28 Jun. 2022].

www.securitymagazine.com. (n.d.). The human factor in cybersecurity. [online] Available from: https://www.securitymagazine.com/articles/96009-the-human-factor-in-cybersecurity? [Accessed 28 Jun. 2022].

CYDEF (2021). The Human Factor: The Hidden Problem of Cybersecurity. [online] CYDEF. Available from: https://cydef.ca/blog/the-human-factor-the-hidden-problem-of-cybersecurity/ [Accessed 28 Jun. 2022].

Kaspersky (2017). The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within | Kaspersky official blog. [online] Kaspersky.com. Available from: https://www.kaspersky.com/blog/the-human-factor-in-it-security/ [Accessed 28 Jun. 2022].

Redscan. (n.d.). Insider Threats | Cyber Security Threats. [online] Available from: https://www.redscan.com/solutions/insider-threats-cyber-security/ [Accessed 29 Jun. 2022]..

Thompson, S.M. (2017). Reading between the lines: the real impact of insider threat. [online] CSO Online. Available at: https://www.csoonline.com/article/3239070/reading-between-the-lines-the-real-impact-of-insider-threat.html [Accessed 29 Jun. 2022].

Jacqueline von Ogden (2016). 3 Ways to Mitigate the Human Factors of Cyber Security. [online] Cimcor.com. Available from: https://www.cimcor.com/blog/3-ways-to-mitigate-the-human-factors-of-cyber-security [Accessed 03 Jul. 2022].