# Launching into Cyber Security

## Unit 9: Individual Essay

**Table Of Content:**

## Introduction:

Cybercrime is on the rise in such scale and complexity, that is affecting almost everyone whether private individual, businesses, or public services. According to the Department for Digital, Culture, Media & Sport (2021) Cybercrime costs the UK billions of pounds every year to the point that it is now categorize as national security threat. It is anticipated that cybersecurity market in the healthcare industry will exceed £27.1 billion by (Global Market Insights Inc., 2019)

Cyber-attacks are committed by cybercriminals who most often are trying to take advantage of programming, web applications mistakes or websites and web server exposed. Therefore, it is important to create a secure object-oriented design to facilitate security-based decisions.

This paper aims to critically explain and apply the concepts and principles of secure object-oriented design to enable business security-based decisions in the healthcare sector.

### 1- Benefits of the web-based appointment and scheduling management information system

Medical appointments have been made traditionally over the telephone or in person. These traditional methods of appointments required sometimes patient to wait on phone lines for quite sometimes in order to speak and book an appointment with the scheduler or to go in person to the healthcare centre. With technologies advancement and the emergence of internet, patients have now a more flexible way to book appointments and the same relieved administrative staffs.

The web-based appointment and scheduling management information system, enables patients to make their reservations and requests online via any devices that can be connected to internet such as smartphone, tablet, laptop etc. a good example that can be used is Dr iQ, used by the NHS to book appointment with your local General Practioner. The app is friendly user and can be easily downloaded on Google Play or Apple App Store. The web-based appointment is a quite flexible system and has many benefits such as time saving, information is centralised, can be used to book appointment at any time (24hrs), cost saving for both patients (fuel or public transport fees) and healthcare facilities (need for extra workforce such as scheduler, translator). Figure 1 below shows the impacts of web-based appointment and scheduling management information system after implementation

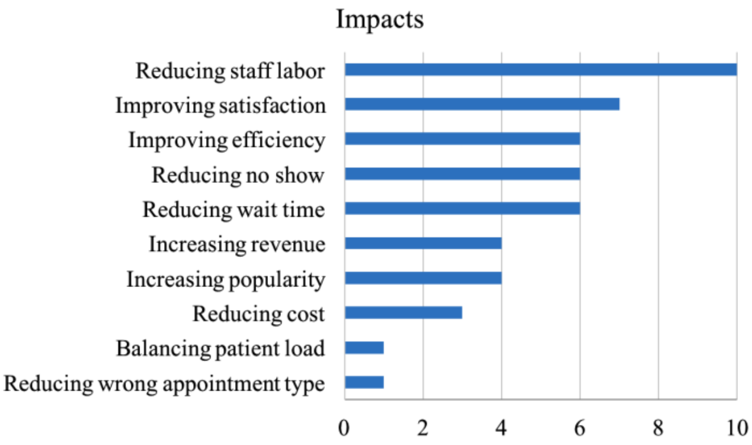

Figure 1: Impacts after implementing web-based scheduling systems (Zhao et al., 2017)

## 2- Potential problems including potential cyber threats to the web-based appointment and scheduling management information system

Although we mentioned above all the benefits of implementing web-based appointment and scheduling management information system, it is also important to highlight all the potential risks and cyber threats by adopting such system. According to Forbes Insights (2019) the volume of medical data has doubled due to the interconnection of medical IoT (Internet of Things), as more than 646 million IoT devices are currently being used in various hospitals, medical offices, and clinics.

While implementing web-based appointment and scheduling management information system is beneficial for both patients and healthcare facilities as stated above but is also open gateways to cyber criminals to gain access to sensitive patient data such as name, insurance cover, date of birth and more. In worst case information such as genetic information, blood type, past surgeries and many more. These types of attacks could jeopardise not only clinic operations but also patients' identities, health, and well-being.

With the technology advancement made this past 20 years, cybercriminals have also become more sophisticated and can attacks the system using various threats such as ransomware, Phishing & Spear, malware Distributed Denial of Services (DDoS) and more.

A good example that can used is WannaCry ransomware attacks in May 2017. During the cyber-attacks 19,000 appointments were cancelled, ambulances were re-routed because of the lost access to hospital information systems, and cost £92m to the NHS (National Health System) (National Health Executive, 2018).

## 3- System and a threat modelling technique that can be used to identify and mitigate potential cyber threats

Seidl et al (2015) defines the Unified Modelling Language or (UML) as a collection of the best practices which have been proved to work over the years in the use of modelling languages. In short, the UML is a set of various diagrams agreed-upon used to assist software developers in defining, designing, visualising, and documenting software systems, the technique can also be used in various industries (Visual Paradigm, 2019).

However, Phillips D. (2018) pointed out some developers believe that UML is a waste of time by arguing that the UML diagrams don't benefit anyone as they will be obsolete before the implementation of system, also that keeping the diagrams up to date is very challenging. But he also argues that UML is very useful for brainstorming sessions as it eases the communication with various stakeholders.

UML diagram can be divided into two categories, structural diagrams, and behavioural diagrams (Seidl et al, 2015). This paper will mainly focus on behavioural diagrams.

### 3.1) A System:

The primary goal of system design is to enhance the system architecture by providing the necessary information and data for its implementation (Leka, A.J, 2017). He continues by pointing out that It also specifies the components, modules, interfaces, and data that make up a system to meet certain requirements.

### 3.2) Used case Diagram

A use case is an approach used in system analysis to plan, explain, and define, clarify a system requirement. A use case diagram in UML is to show various ways which a user could interact with a system, it also outlines the specific functions of the different users of a system. The figure 2 below illustrates the use case diagrams for the various users in the system.

The system illustrates that, the ASMIS will have a homepage (Main use Case) from which all the users of the website could access their specific sections. Patients could create a profile and log in. Doctors would log onto their portals from the, and Administrators would log from the same page to manage the system. This separation of login ensure that no unauthorized person can access the system. Therefore, if a cybercriminal tries to gain access an alert will be sent to the Administrator page to raise the security on the system and access will be denial automatically. In other words, The Administrator has complete control over the website and oversees all the user modules as shown in the Figure 2.

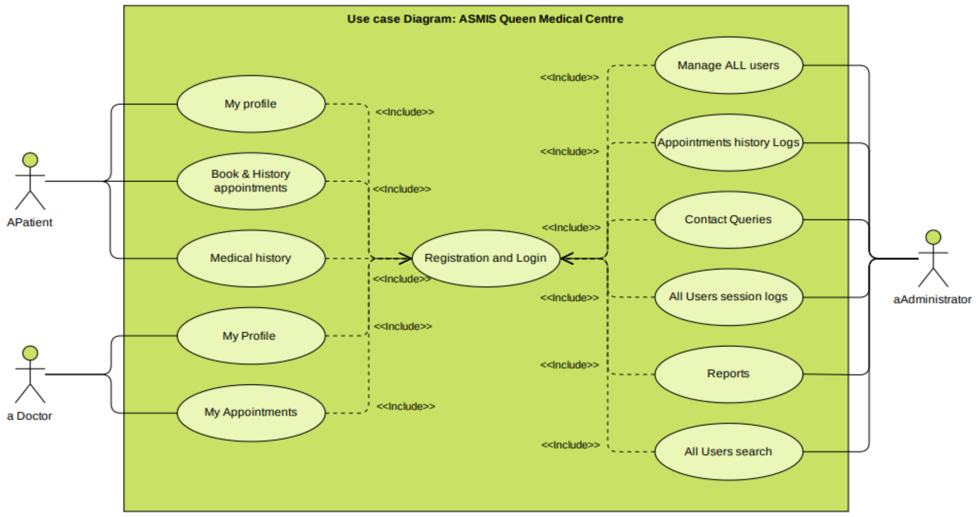

Figure 2: Use case diagram show users access to the system.

Having said that, administrative privileges access should be limited to few users in order to avoid people with bad intend (insider) to gain access easily to the system. Harries and Yellowlees (2013) in their studies highlighted that 70% of criminal activity are done through resentful employees' account. Therefore, the clinic should monitor very closely the lifecycle all user accounts, so privilege should be revoked to all account not in use. Furthermore, two accounts need to be set up for all users requiring administrative privilege. One that give access only local machine an another which enable the user to check work emails, browsing internet.

### 3.3) Activity Diagram:

The activity diagram is a significant diagram that is supported by UML 2.0. Seidl et al (2015) stated that "*The activity diagram focuses on modelling procedural processing aspects of a system. It specifies the control flow and data flow between flow various steps the actions required to implement an activity".* The main advantage of this diagram it is easy to understand the logic of a system and it is simple. This model presents less information compared to other models as it only presents information at higher level. The figure 3 below illustrates the activity diagram approach to cybersecurity threats and risk mitigation for the clinic system.

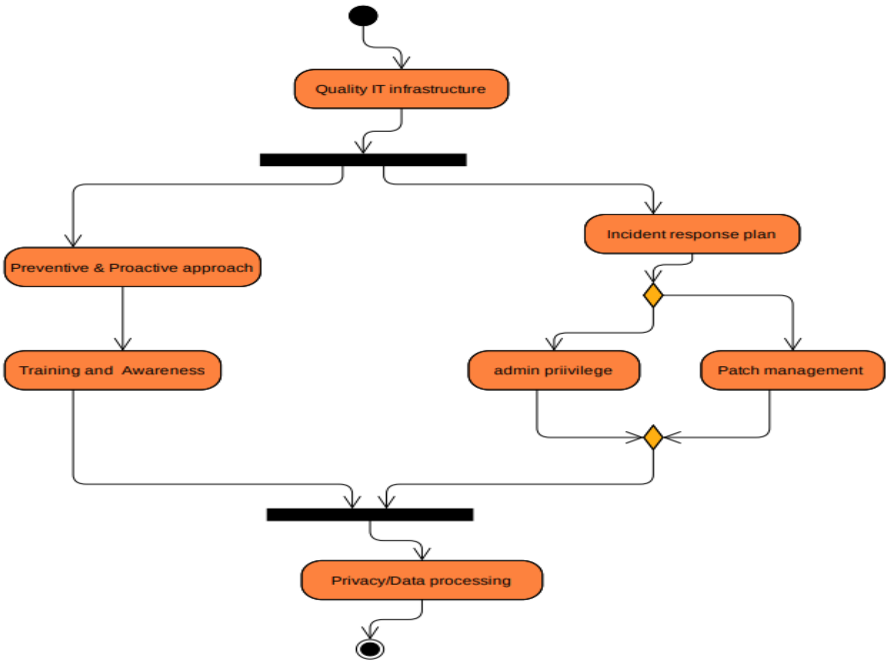

Figure 3: Activity Diagram

It can never be stressed enough that the foundation of every good start from IT quality or good infrastructure. From resources, support IT services such as software applications, networking tools, hardware platforms etc. Good infrastructure will automatically address the issue of prevention as the healthcare industry has been subjected to numerous attacks in recent. IBM in their survey "*Cost of a data breach report 2021"* highlighted that, the overall cost of data breach in the healthcare industry rises by 29.5. This only corroborate how important for hospital/clinic to invest at an early stage for their security to prevent cyber-attacks.

Training and awareness are a very important parts of the model as it is well known that the weakest link in the cybersecurity is the end users, therefore training and raising awareness to all users of the system is very important.

Incident response plan is a major key part in this model specially for a health facility. The Australian Cybersecurity Centre (2017) report provided guidance about incident response plan that can be put in place by any organisation.

- Offline storage in case of data breach, so data can be lost and prevent ransomware
- Regular testing the system
- Exercise real simulation attacks regularly

Administrator privilege as discussed above in the use case model should allowed to few people.

Patch management mainly to mainly involve detection, evaluation, and mitigation of IT system vulnerabilities the process consists mainly of monitoring potential threats and risk management.

Privacy and data processing is to address the General Data Protection Regulation (GDPR), the Data Protection Law Enforcement Directive 2018, as users when will include personal information during their registration in ASMIS. The GDPR regulation provide protection and rights to individuals about how organisation should handle data collected from users it is important the use of advance cryptographic tools such as:

- Key-Based Authentication – a system which use asymmetric algorithms to confirm user identity.
- Security Tokens – A tools which give extra layer of security to gain access to a network system.
- Zero trust distribution – The approach is simple all users must be verified, authorised and continuously checked. Zero trust also assume that networks can be cloud-based, local, both cloud and local and most importantly users can be located anywhere, therefore constant verification and authorisation are required (Crowdstrike ,2020)

And they're others cryptographic tools that can be implemented as the above list isn't exhaustive.

## 4- The Cyber Security technologies:

There are various types of cybersecurity technologies which provides excellent security nowadays. It is also known that risk can never be zero, but it can be mitigating using technologies currently available on market.

### 4.1) Application Security:

Vmware (2022) defines application security as "*Application security is the process of developing, adding, and testing security features within applications to prevent security vulnerabilities against threats such as unauthorized access and modification.*"

There are various types of application security that can be implemented as cybersecurity for the clinic: Authentication – Authorisation - Encryption (to protect sensitive data after end user utilisation) - Application security testing (crucial process to ensure that other application are functionals).

### 4.2) Network Security

It is a designed process put in place to ensure that a network and data are protected, usable, and their integrity is not compromised. (Cisco, 2022). The approach englobes both hardware and software technologies. As for the application security, there numerous types of network security: Web-security - Emails security – Access control – Network segmentation – Anti-virus - Firewalls the list isn't exhaustive.

**4.3)** Device security is the process design to protect any wearable devices such as laptops, smartphones, tablets etc. its main goal is to prevent unauthorize user to access a system without authorisation. For this process to work properly a clear policy should first been put in place and enforced, password protection, avoid public Wi-Fi, and limitation of apps download.

## Conclusion:

Cyber-attacks on health facilities are a growing trend as cybercriminals are aware of the implication, and disruption that can cause from the patient, the clinic, and any other stakeholders. Therefore, is it imperative for health facilities to invest in their cybersecurity infrastructure. As part of the information security team, our duty is to equip and raise awareness to all end-users of the potential threats that they will be facing. In addition, the above diagrams model used in this paper to explain first end users interface relationship (Figure 2) and activity diagram for cybersecurity threats and risk mitigation (Figure 3) will help in the design and implementation web-based appointment and scheduling management information system.

References:

Cyber security breaches survey 2021 (n.d) GOV.UK. Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021 (Accessed: May 16, 2022).

Insights Team (2019) The hospital will see you now, Forbes. Available at: https://www.forbes.com/sites/insights-intelai/2019/02/11/the-hospital-will-see-you-now/ (Accessed: May 16, 2022).

National Health Executive. (2018). WannaCry cyber-attack cost the NHS £92m after 19,000 appointments were cancelled. [online] Available at: https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled#:~:text=The%20May%202017%20cyber%2Dattack.

Zhao, P. et al. (2017) “Web-based medical appointment systems: A systematic review,” Journal of medical internet research, 19(4), p. e134. doi: 10.2196/jmir.6747.

Visual Paradigm (2019). What is Unified Modeling Language (UML)? [online] Visual-paradigm.com. Available at: https://www.visual-paradigm.com/guide/uml-unified-modeling-language/what-is-uml/.

Phillips, D. (2018) Python 3 Object-Oriented Programming: Build robust and maintainable software with object-oriented design patterns in Python 3.8, 3rd Edition. 3rd ed. Birmingham, England: Packt Publishing PP. 5-10

Seidl, M. et al. (2015) “Introduction,” in UML @ Classroom. Cham: Springer International Publishing, pp. 1–9.

Lekan, A. J. (2017) “Design and implementation of a patient appointment and scheduling system,” 4(12), pp. 16–23. doi: 10.17148/IARJSET.2017.41203.

Harries, D. and Yellowlees, P.M. (2013). Cyberterrorism: Is the U.S. Healthcare System Safe? Telemedicine and e-Health, 19(1), pp.61–66. doi:10.1089/tmj.2012.0022.

Cost of a data breach report 2021 (no date) Ibm.com. Available at: https://www.ibm.com/downloads/cas/OJDVQGRY (Accessed: May 16, 2022)

Strategies to mitigate cyber security incidents (no date) Gov.au. Available at: https://www.cyber.gov.au/acsc/view-all-content/strategies-to-mitigate-cyber-security-incidents (Accessed: May 16, 2022).

What is zero trust security? Principles of the zero-trust model (2020) crowdstrike.com. Available at: https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/ (Accessed: May 16, 2022).

What is application security? (2022) VMware. Available at: https://www.vmware.com/topics/glossary/content/application-security.html (Accessed: May 16, 2022).

Cisco, 2022. What is network security. [online] Available at: https://www.cisco.com/c/en_uk/products/security/what-is-network-security.html Accessed: May 16, 2022)