COMP3009 – REPORT OUTLINE

TABLE OF CONTENTS

INTRODUCTION

Like many others, I have used the NHS COVID-19 app to sign into locations across the UK and have pondered on the security strength that the NHS has employed within the app. Considering it was hastily built at the peak of the pandemic, buried exploitable security blunders are likely present. As seen before [4], rushing development can have devastating consequences for companies who don't (or can't) properly lay out relevant standards for their teams, especially for an app as tempting target as this one.

ASSET MANAGEMENT & RISK ANALYSIS

As an opening note, covering whose responsibility it should be to secure assets, the policy will enforce operational security as everyone's responsibility, including the specific responsible party at the time. Sometimes it only takes a few employees to be socially engineered for a company and its stakeholders to lose significant financial assets [10-11].

This can be regarded this as a critical vulnerability in the system, since humans are easier to influence than computers [28], resulting in crafters of social engineering being a continuous present threat to all company's [23]. Even if the app was 100% secure, an attacker could target dependencies that are required for basic functionality. An benign QR code in a shop could be replaced with a malicious one. Or an existing Bluetooth vulnerability [3] could be leveraged to gain access to multiple devices without having to break the app at all.

In evaluating the exposure (intentional or not) of customer data [1], the reputation of both the developer and NHS would be degraded if it was exposed [5]. Not only is this data valuable for the app's function, it's required to be under restricted access according to the Data Protection Act 2018 (GDPR) [8]. Under Articles

4(13-15) and 9 of GDPR [9], health related data is classed as sensitive and cannot be processed (operated on). Any potential policy will also include instructions on how to handle customer data during normal operations too. The app will also store location history from scanned QR code metadata and although location data is not classed as sensitive under GDPR [7], it's classed as personal data [8]. Companies can be fined an extraordinary amount of money for not securing either type effectively [29], which is why it's anonymised [12].

Commonly, a Data Protection Officer would handle the obtention and audit of customer data [13]. Hiring a DPO is not compulsory under some conditions but I'm doubtful that would be recommended under GDPR. Considering the NHS is a public body processing a large quantity of sensitive and personal data, they would be legally required to employ one [14] even though the data doesn't represent direct financial value to them.

I have also identified the codebase itself to be a financial and software asset. The servers that run the app in tandem with the code are physical, financial assets that tie into sentimental when holding customer data. Without a secure codebase there wouldn't be an app to run but the developer would likely lose money in this scenario, so I have classified it as a financial asset when evaluating from the context of a developer and a client. Furthermore, the servers that power the app can be physically attacked via USB ports or direct damage, potentially causing even more damage than a loss of code that would likely be backed up. With no physical backup server, the app would not have an environment to run on.

LAWS

The Data Protection Act 2018 (GDPR) will be studied in detail as its clauses and articles refer to user data, the main asset the app is protecting. I will not be talking about the Data Protection Act 1998 as that was repealed by the 2018 version [17], so it doesn't have a big impact on the app. After evaluating GDPR in Asset Management, I will be tying together the sections of the act with our assets in the final report.

I will also investigate the Computer Misuse Act 1990 [16] which is useful for looking at what would constitute as an offence against the app's systems, especially sections:

- 1: Concerns general offences along with the punishment an offender would be subject to should they commit one of these offences. This will be touched on briefly when evaluating what counts as an intentional breach of the policy from a hostile insider.
- 3: Similar to Section 1, it specifically covers impairment or alteration of computer systems and their data. Since the app needs data to function, any prospective security policy would need to take this section into account.

Finally, I'll be addressing other regulations that I believe will directly reflect the standards that I will be setting in the security policy. These include:

- NHS Confidential Code of Practice 2003 [18]. An NHS staff contract, it's as good as the law. Any employee who tampers with the app's data can be charged under this code and dismissed or arrested under GDPR [20].

- Human Rights Act 1998 [19]. Although largely irrelevant to this situation, Article 8 is of particular interest, upholding "respect for private and family life". However, it's open to some interpretation and conflicts with the NHS Code of Practice 2003 [18].
- Health and Social Care Act 2001 [21] and Health Service (Control of Patient Information) Regulations 2002 [22]. The two acts work in tandem [Section 1.2.a of 22] to define exactly when it's legal to disclose confidential patient information. Since the app would need to share positive test results across the network, warning others that have been in close proximity with the infected user, the acts would need to be referenced as the data is protected under GDPR.

SECURITY POLICY

Our security policy will include several sections that each deal with a specific case raised in our risk analysis and relevant laws. Generally, the policy will be easy to follow, applicable to everyone involved in supporting in the app who it would affect and detail the correct response in the event of a security incident or breaking of a clause in the policy. The following sections are of particular note:

- Personal who have access to sensitive and personal customer data held or processed by the app's systems. Consisting of as few people as possible, requests for elevated privileges within the app's system should be subject to an approval/rejection process. In order to keep critical systems confidential while ensuring informational and financial assets are not integrally damaged or made unavailable by unauthorised personal, it would need to be included.
- Lists national and relevant international regulations the policy will enforce. Mostly consisting of UK and EU laws, I will also touch upon the Computer Fraud and Abuse Act (CFAA) [26] when covering areas that stray into American operations and comparisons.
- Methods to secure data assets, including the protection of digital code and servers that power the app or third-party systems.
- Processes to onboard new users (and expel deprecated ones) from the app's systems. To keep account trees clean and avoid leaving potential security holes open by keeping unused user accounts, a process to retire user accounts of employee's who no longer require access to certain sections will be defined. Conversely, the process of onboarding users into the system will also be detailed. New users will go through a vetting period to establish that they're non-malicious actors and can be trusted with the information they will be granted access to [27].
- Finally, the policy will cover miscellaneous subjects that enable it to function as efficiently and cross-company as possible. Sections such as policy exceptions, accessibility of policy terms and classification of new datasets or actors will be described in the final report's policy.

AWARENESS PLAN

To prevent plausible deniability and ensure staff are trained against the security policy, the policy will include an awareness plan. The plan would be targeted all users that have access to the app's systems, educating them to the policy's standards of security. Training employees of general, good security practices (strong passwords, being suspicious of email attachments, etc) on a regular basis is the pinnacle

of preventing human error [31]. To balance out a potential overload of information, it will also define how often and how much information should be fed to staff over a specific time period.

To ensure those with access to app or customer data do not leak details accidentally, the plan will include instructions for dealing with restricted information, as well as NDA's or policies (e.g. the code of conduct) that staff will need to have, or already, signed. Having staff sign such a contract will ensure compliance and keep data security at the forefront of their jobs.

Finally, the awareness plan will be introduced as ongoing, not a one-off lesson [32]. All the points raised about security will be easily forgettable by staff [33] so the plan will have a rolling period of learning that doesn't define an ending. To keep the experience new each time, employees will be allowed to input their own ideas and activities into it. No-one would enjoy completing the same, plain assignment each time it was required so varying how staff learn these concepts is crucial to ensure a strong security awareness is maintained no matter the circumstances.

CONCLUSION

To conclude, this outline attempts to structure my final report and impress my thoughts and opinions on the task at hand based off existing laws and legislations. I believe that there is a lot of information missing but overall, it covers the major points that will be explored in more detail in the final report. As of writing this, the app has been installed over 5,000,000 times [34] so it is crucial to ensure the app has a professional and well-designed policy using lessons learned from previous experiences with security policies.

APPENDIX

1. Information Commissioner's Office (2019). *London pharmacy fined after "careless" storage of patient data* [Online]. Available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/12/london-pharmacy-fined-after-careless-storage-of-patient-data (Accessed 9/11/2020).
2. Cyber news group (2020). *How Is The NHS Covid-19 App Cyber-Secure?* [Online]. Available at https://www.cybernewsgroup.co.uk/how-is-the-nhs-covid-19-app-cyber-secure (Accessed 9/11/2020).
3. Insinuator (2020). *Critical Bluetooth Vulnerability in Android (CVE-2020-0022) – BlueFrag* [Online]. Available at https://insinuator.net/2020/02/critical-bluetooth-vulnerability-in-android-cve-2020-0022 (Accessed 9/11/2020).
4. ZDNet (2018). *Rushed privacy features result in sloppy security* [Online]. Available at https://www.zdnet.com/article/rushed-privacy-features-result-in-sloppy-security (Accessed 9/11/2020).

5. Ellen Neveux (2020). *Reputation Risks: How Cyberattacks Affect Consumer Perception* [Online]. Available at https://www.securelink.com/blog/reputation-risks-how-cyberattacks-affect-consumer-perception (Accessed 10/11/2020).
6. Indrajeet Deshpande (2020). *What Is Customer Data? Definition, Types, Collection, Validation and Analysis* [Online]. Available at https://www.toolbox.com/marketing/customer-data/articles/what-is-customer-data/#_002 (Accessed 10/11/2020).
7. European Commission (2016). *What personal data is considered sensitive?* [Online]. Available at https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en (Accessed 10/11/2020).
8. Which (2018). *What counts as personal data?* [Online]. Available at https://www.which.co.uk/consumer-rights/advice/what-counts-as-personal-data-according-to-gdpr (Accessed 10/11/2020)
9. Which (2018). *Data Protection Act 2018 (GDPR)* [Online]. Available at https://www.which.co.uk/consumer-rights/regulation/gdpr-data-protection-act#collecting-your-personal-data (Accessed 10/11/2020)
10. BOJANA DOBRAN (2018). *RSA SecurID Cybersecurity Attack* [Online]. Available at https://phoenixnap.com/blog/famous-social-engineering-attacks (Accessed 10/11/2020)
11. Eric Chabrow (2011). *'Tricked' RSA Worker Opened Backdoor to APT Attack* [Online]. Available at https://www.bankinfosecurity.com/tricked-rsa-worker-opened-backdoor-to-apt-attack-a-3504 (Accessed 10/11/2020)
12. UK Government (2020). *NHS COVID-19 app: privacy notice* [Online]. Available at https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-test-and-trace-app-early-adopter-trial-august-2020-privacy-notice (Accessed 10/11/2020)
13. Nate Lord (2020). *What is a Data Protection Officer (DPO)? Learn About the New Role Required for GDPR Compliance in 2019* [Online]. Available at https://digitalguardian.com/blog/what-data-protection-officer-dpo-learn-about-new-role-required-gdpr-compliance (Accessed 10/11/2020)
14. Information Commissioner's Office (2020). *Data protection officers* [Online]. Available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers (Accessed 10/11/2020)

15. Packet Labs (2020). *What is Data Classification?* [Online]. Available at https://www.packetlabs.net/data-classification/#:~:text=Data%20Classification%20in%20Government%20organizations,%2C%20Confidential%2C%20Internal%2C%20Public (Accessed 11/11/2020)
16. UK Government (1990-2020). *Computer Misuse Act 1990* [Online]. Available at https://www.legislation.gov.uk/ukpga/1990/18/contents (Accessed 11/11/2020)
17. UK Government (1998-2018). *Data Protection Act 1998* [Online]. Available at https://www.legislation.gov.uk/ukpga/1998/29/contents (Accessed 11/11/2020)
18. DH/IPU/Patient Confidentiality (2003). *NHS Confidentiality Code of Practice* [Online]. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf (Accessed 11/11/2020)
19. UK Government (1998-2020). *Human Rights Act 1998* [Online]. Available at https://www.legislation.gov.uk/ukpga/1998/42/contents (Accessed 11/11/2020)
20. Corporate Information Governance (2019). *Confidentiality Policy* [Online]. Section 3.9 only. Available at https://england.nhs.uk/wp-content/uploads/2019/10/confidentiality-policy-v5.1.pdf (Accessed 11/11/2020)
21. UK Government (2001-2020). *Health and Social Care Act 2001* [Online]. Available at https://www.legislation.gov.uk/ukpga/2001/15/contents (Accessed 11/11/2020)
22. UK Government (2002-2020). *The Health Service (Control of Patient Information) Regulations 2002* [Online]. Available at https://www.legislation.gov.uk/uksi/2002/1438/contents/made (Accessed 11/11/2020)
23. Davey Winder (2018). *Social engineering: The biggest security risk to your business* [Online]. Available at https://www.itpro.co.uk/social-engineering/30017/social-engineering-the-biggest-security-risk-to-your-business (Accessed 11/11/2020)
24. Ray Dunham (2020). *Information Security Policies: Why They Are Important To Your Organization* [Online]. Available at https://linfordco.com/blog/information-security-policies (Accessed 12/11/2020)
25. Ray Dunham (2020). *Information Security Policies: Why They Are Important To Your Organization* [Online]. Available at https://linfordco.com/blog/information-security-policies (Accessed 12/11/2020)
26. Thomson Reuters (2020). *Computer Fraud and Abuse Act (CFAA)* [Online]. Available at https://uk.practicallaw.thomsonreuters.com/2-508-3428?transitionType=Default&contextData=(sc.Default) (Accessed 12/11/2020)

27. Michael Gegick, Sean Barnum (2013). *Least Privilege* [Online]. Available at https://us-cert.cisa.gov/bsi/articles/knowledge/principles/least-privilege (Accessed 12/11/2020)
28. Kaspersky (2020). *The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within* [Online]. Available at https://www.kaspersky.com/blog/the-human-factor-in-it-security (Accessed 12/11/2020)
29. It Governance (2018). *GDPR penalties and fines* [Online]. Available at https://www.itgovernance.co.uk/dpa-and-gdpr-penalties (Accessed 12/11/2020)
30. NHS (2020). *Answer questions about your main symptom* [Online]. Available at https://111.nhs.uk (Accessed 12/11/2020)
31. IT Governance (2020). *Cyber security awareness training for employees* [Online]. Available at https://www.itgovernance.co.uk/staff-awareness (Accessed 13/11/2020)
32. Trustwave (2020). *Establishing a security awareness program* [Online]. Available at https://help.securitycolony.com/help/i-want-to-set-up-a-security-awareness-program-where-do-i-start (Accessed 13/11/2020)
33. Scott Ikeda (2020). *Phishing Awareness Training is Far From Permanent; New Study Shows the Effects Last Only a Few Months* [Online]. Paragraph 3. Available at https://www.cpomagazine.com/cyber-security/phishing-awareness-training-is-far-from-permanent-new-study-shows-the-effects-last-only-a-few-months (Accessed 13/11/2020)
34. Department of Health and Social Care (2020). *NHS COVID-19* [Online]. Available at https://play.google.com/store/apps/details?id=uk.nhs.covid19.production (Accessed 13/11/2020)