IFB240 ASSIGNMENT 2

PART B

(Group 68)

Team member	Student name	Student number	Last digit
1			
2			
3			
4	Thien Tu Tran		

Introduction

Waterworks is a South East Queensland-based premium water service provider in the utility industry sector, supplying water and waste-water services for businesses between Noosa and the Gold Coast. Waterworks has requested a risk report, due to heightened concerns, about the use of managers' mobile devices for work. For this report, we have obtained information on an employee whose role is 'Manager of Commercial Delivery' and who uses their Samsung Galaxy S24 for work purposes with unrestricted personal use as well. This role is responsible for:

- Overseeing the end-to-end commercial process and contract management for the delivery of the Capital Plan
- Leading the development of end-to-end commercial models for capital and major projects
- Providing leadership and technical guidance to key stakeholders for Commercial Delivery
- Working with stakeholders to reach lasting, impactful partnerships with industry for the development of assets and infrastructure
- Communicating and maintaining positive internal relationships (Business, Infrastructure, Legal and Compliance, and Delivery Units) and external relationships (Development Industry, Participating Councils, and the Queensland Government)

(Unitywater, n.d.)

The use of the personal Samsung Galaxy S24 for Commercial Delivery Management allows the user to meet the mandatory networking requirements for such a role. The user can effectively communicate with stakeholders as well as other relevant internal and external parties. Additionally, the manager necessitates leadership in 'Commercial Delivery', requiring close collaboration and teamwork with internal business units. The Samsung Galaxy S24 enables communication with all work-related parties, making it an integral device to Waterworks function and continued development.

Due to sensitive information, role responsibilities, and the increased risk of unrestricted personal use, device security is critically important. The position requires communication and collaboration with vital stakeholders, including government bodies, meaning that the availability of the device is necessary to continue fast-paced business operations. Targeted vulnerabilities would aim to exploit all security goals, where the denial of access to the work phone would temporarily halt potential business operations through denial of communication. The modification of business information assets would cause catastrophic developmental and infrastructural issues if not detected as well as reputational catastrophe. Breaches of confidentiality involving contractual agreements, financial information, and employee personal information may cause detrimental reputational damage. Considering the device user's managerial role, a threat actor may target them for more elevated privilege but also cause business disarray for their breadth of responsibility. The risk is exacerbated by the vulnerability of unrestricted personal use, making the employee's phone susceptible to a greater variety of threats.

This report aims to investigate the risks of the use of a Waterworks manager's Samsung Galaxy S24 for both work and unrestricted personal use. The report will detail the identification and analysis of risks (given the context of its use), review a used application's privacy policy (Facebook), the associated risks and potential impact, and an evaluation of risks to prioritise them for treatment.

Context Establishment

I. A brief description of information assets

The Samsung Galaxy S24 Series was released on 31st of January 2024 (Samsung, 2024), with three models (S24, S24+, and S24 Ultra). The manager of Waterworks Utilities is using a US-version Samsung Galaxy S24 with 128GB of storage, which he owns and uses for both personal and professional purposes.

A. Hardware (Excellent description with correct, concise,comprehensive details)

Chipset	Qualcomm Snapdragon 8 Gen 3
Memory	8GB RAM
Screen	6.2-inch Dynamic LTPO AMOLED 2X
Cameras	Main camera: Triple (50, 10, 12 MP) Selfie camera: Single (12 MP)
Battery	Li-Ion 4000 mAh, non-removable
Communication Components	Network: GSM, CDMA, HSPA, EVDO, LTE, 5G WLAN: Wi-Fi 6E Bluetooth: 5.3 Positioning: GPS, GLONASS, BDS, GALILEO, QZSS NFC Yes USB USB Type-C 3.2, DisplayPort 1.2

From *"Samsung Galaxy S24"* by GSMArena.

B. Software

The Samsung Galaxy S24 128GB comes with the Android 14 operating system and Samsung's custom skin, One UI 6.1, providing a smooth and user-friendly experience (GSMArena, 2024). Due to the S24's robust app ecosystem, the phone caters to both the personal and professional facets of a utility manager's life.

Firstly, preinstalled applications that are especially handy for work include the Calendar for scheduling, Samsung Notes for fast memos, and the Secure Folder for securing critical business documents. The preinstalled Samsung DeX might convert the phone into a desktop experience for document management and mobile office needs, while apps like Microsoft Office Suite and Adobe Acrobat Reader enable the creation, editing, and sharing of documents and PDFs. Drop-box and

Microsoft OneDrive would function as cloud storage options for file management that is accessible from anywhere. To arrive on time at work or meetings, a navigation tool such as Google Maps is required, as it provides real-time traffic updates and instructions.

Secondly, the manager might use industry-specific applications such as SCADA (supervisory control and data acquisition) systems for real-time monitoring of the water distribution network, or GIS (geographic information systems) apps like ArcGIS for mapping and spatial analysis of utility assets (SCADA, n.d.; Esri, 2019). A CRM (customer relationship management) programme such as HubSpot or Pipedrive might be invaluable in handling customer enquiries and work orders, easing the energy company's day-to-day operations (Sevilla & Mcallister, 2024). Microsoft Teams, Slack, and Trello are examples of programmes that may be used for team communication and project management.

Lastly, the manager may pursue personal interests by using applications like Spotify for music, Netflix for entertainment, and numerous social media sites like Facebook and LinkedIn to maintain contacts and professional networking. Health-tracking applications like Samsung Health, when combined with a Galaxy Watch, might provide a unified picture of health parameters, which is useful for managing a busy lifestyle. Smart home apps such as Nest or Philips Hue would allow for remote management of home surroundings, guaranteeing that comfort and security are only a tap away. Banking applications like CommBank add to this arsenal by enabling safe and speedy financial transactions and administration, which is critical for both quick personal banking and effective monitoring of professional expenses. Online shopping is made effortless with apps like eBay and Amazon, enabling the manager to purchase anything from office supplies to personal items.

C. Data

As a manager in the water utility industry, the data stored on his Samsung Galaxy S24 would likely encompass a diverse array of files and applications relevant to both their professional responsibilities and personal life. Noticeably, all work-related data is preserved within cloud-based storage.

- Contacts: the device might contain a substantial number of contacts including friends, family’s members, colleagues, and stakeholders within the industry, which easily reaches into the hundreds. Let’s say he has 500 contacts, which would take up approximately 20MB.

- Music and Media: Depending on the manager’s personal preferences, personal use could see a mixture of streaming apps that don’t store files locally, but the overall size of these apps are still tangible, potentially occupying anywhere from a few gigabytes to several dozen. Let’s say the manager is a music and movie lover, and he has downloaded a ton of music or movies to watch them offline when he in the no internet zone, so the size would be approximately 12GB

- Documents and Notes: He might have a lot of documents and notes related to work, such as reports, project plans, voice recordings, etc., which are likely to be extensive but not significantly large in terms of storage, possibly adding up to a few hundred megabytes.

- Photos and Videos: These often consume the most storage on personal devices, and it's no different for the manager’s Galaxy S24. With a historical collection of multimedia transferred

from his previous phone, the storage dedicated to visual memories could easily reach significant proportions. This extensive archive likely includes a blend of personal moments and professional documentation such as site visits and inspection footage, amounting to around 40GB.

- Work Apps: He might have installed various work-related apps, such as project management tools, communication apps, and utilities industry-specific apps, cloud storage apps. The size of these apps can vary greatly, but let's say they take up about 10GB in total.

- Personal Apps: He might also have personal apps for social media, entertainment, fitness, banking, online shopping, etc. These could take up another 10GB

II. An overview of the usage of the device

The predominant functions of a phone are accomplished through the use of applications, colloquially called 'apps', these apps and the business behind them operate on collecting information generated by the user, with either the user activity giving the app the information or by the application collecting said information in the background.

The predominant apps installed on the Samsung Galaxy S24 128GB:

- Google Photos
- Commbank
- DropBox
- FaceBook
- Geo SCADA mobile
- Fruit Ninja
- Google Chrome
- Google Maps
- Microsoft Authenticator

On the other hand, the rarely used apps include Google Photos and Fruit Ninja. The types of information collected and stored by these applications vary greatly but are not limited to, names, email addresses, home addresses, phone numbers, political or religious beliefs, sexual orientations, financial information, bank account Balance, contact names, contacts email address, contacts phone number, temporary authentication codes, network Information, PLC device information and status and geographic locations, both approximate and precise (see *Appendix 4* for more details). A further in depth analysis of each application has been completed and can also be found in *Appendix 4*. When analysing these applications two key fields are isolated: criticality and sensitivity.

Although the information collected is necessary to run these applications, the information stored and collected through them can be seen as potential targets for malicious actors or areas at risk of an accidental leak, in either case, this would pose a breach of the first fundamental cyber security goal, confidentiality. As work material is contained within the device a breach in confidentiality could mean the exposure of privileged information such as proprietary schematics or designs, providing business competitors with the opportunity to replicate similar works, costing Waterwork its individuality in the market space, and costing them long-term value. This is to say nothing of the personal information of the user that could also be exposed, leading to impersonation attacks or further social engineering attacks, causing lengthy and costly interruptions to their personal life.

Although a personal device the Samsung Galaxy S24 is also used by the user for the completion of their work duties, applications such as Geo SCADA mobile, Microsoft Authenticator and Dropbox are accessed frequently as part of this work. Should the user lose access to these apps, their ability to work may be severely hampered and would breach the accessibility security goal, causing an unnecessary financial and time cost to Waterworks by forcing the users onto alternative devices and delaying tasks. Alternatively in a breach of the integrity security goal, if the information on these apps were altered from their correct state, it could cause extreme amounts of damage to physical equipment and electronics, critical records of contracts, policies, schematics and other reference material would become untrustworthy and require extreme amounts of time to verify or replace.

Risk Identification and analysis

I. A mobile application or device operating system

Title: Massive Android lock screen bug lets attackers access your photos and other personal data — how to stay safe

Author: Anthony Spadafora

Reference:

Spadafora, A. (12 Dec 2023) Massive Android lock screen bug lets attackers access your photos and other personal data — how to stay safe. *Tom's Guide*, Retrieved from: https://www.tomsguide.com/news/massive-android-lock-screen-bug-lets-attackers-access-your-photos-and-other-personal-data-how-to-stay-safe on 24 April, 2024.

Brief Summary: A severe security flaw has been discovered in Android 13 and 14, allowing attackers with physical access to a smartphone to bypass the lock screen and access personal data such as images, contacts, and browsing history. Discovered by security researcher Jose Rodriguez, this flaw exploits a feature in Google Maps, allowing unauthorised access to various personal data based on the user's configuration of the app. Despite Rodriguez reporting the issue to Google six months prior, it remains unpatched, posing a significant risk to users' personal data security.

Information Asset: The information asset at risk includes several personal and professional data stored in the device such as photos, contacts, browsing history, etc. These assets are at rest when they are vulnerable. Notably, multiple other information assets could be compromised in subsequent chain of events. For example, if the attacker has access to the Google account, they may also gain control over linked social media profiles, potentially posting malicious content, or messaging the user's contacts with scams or phishing links.

Threat: An attacker, with physical access to the device, exploits a security weakness to gain unauthorised access to personal data on Android devices via Google Maps. This action would compromise the confidentiality of these assets.

Vulnerability: A bug in the Android operating system (Android 13 and 14) that permits an attacker to bypass the lock screen security.

Security Incident / Attack: If Driving Mode is not activated, attackers can view and share recent and favourite locations, as well as contacts. Alarmingly, when Driving Mode is activated, this vulnerability can be compounded with another exploit, leading to more severe consequences. Attackers could potentially access and publish photos, and carry out extensive manipulation of the Google account, which possibly includes gaining full access to the victim's Google Account from a second device. This would be considered an active attack as deliberate action involving direct interaction with the system is required. An example could involve the water utility manager leaving his phone unattended in an

office during a site visit. An attacker, who may be masquerading as a contractor, could take this opportunity to discreetly access the phone. Using the Google Maps vulnerability, the attacker could bypass the lock screen and glean sensitive information such as upcoming infrastructure project sites or contact details of key stakeholders, which could be used for further exploitative activities.

II. User behaviour

Title: The $64k Question: How Does AI Phishing Stack Up Against Human Social Engineers?

Author: Kevin Townsend

Reference:

Townsend, K. (24 Oct 2023) The $64k Question: How Does AI Phishing Stack Up Against Human Social Engineers?. *SecurityWeek*, Retrieved from: https://www.securityweek.com/the-64k-question-how-does-ai-phishing-stack-up-against-human-social-engineers/ on 24 April, 2024.

Brief Summary: The study in SecurityWeek investigates the effectiveness of AI-generated phishing efforts vs those made by human social engineers. IBM's X-Force Red performed research on the impact of AI and human-generated phishing emails on employees at a healthcare organisation. The findings revealed that, while AI can generate phishing emails faster, human-crafted emails are more successful owing to their emotional intelligence, personalisation, and striking headlines. However, the difference in success rates was minor, with human phishing getting a click rate of 14% vs 11% for AI. The paper implies that as AI technology progresses, its efficacy in phishing may improve, creating a huge cybersecurity danger.

Information Asset: The information asset at risk from this type of active attack is confidential personal and company information. Any information contained in applications that are restricted by account credentials may be accessed. This includes banking information (commbank app), as well as ‘Waterworks’ event logs (GEO SCADA).

Threat: The threat posed by an active social engineer attacker. The use of manipulation tactics to influence a user into surrendering personal information and/or access to users confidential accounts.

Vulnerability: Insufficient user awareness in regards to the strategies adopted by social engineers and the threat a phishing email may pose to their devices/personal information.

Security Incident / Attack: An active attacker gains the trust and co-operation of the user through social engineering manipulation. The lack of education of the identifiers of malicious behaviour on the users behalf allows the attacker to gain any confidential information they require directly from the user. In the context of a phishing email, this could range anywhere from wireless access to their entire device, to specific account credentials. The severity of the attack would depend largely on the competency of the user and their education on identifying phishing attacks.

III. Physical threats to mobile devices

Title: Is the Samsung Galaxy S24 (Ultra) Waterproof? Does it have an IP Rating?

Author: Haneet Singh

Reference:

Singh, H. (17 Jan 2024) Is the Samsung Galaxy S24 (Ultra) Waterproof? Does it have an IP Rating?. *Ytechb*, Retrieved from: https://www.ytechb.com/is-the-samsung-galaxy-s24-ultra-waterproof/ on 24 April, 2024.

Brief Summary: The article examines the water-resistant capabilities of the Samsung Galaxy S24 series. The International Electrotechnical Commission (IEC) has given these goods an IP68 rating, which means they may be submerged in up to 1.5 metres of freshwater for a maximum of 30 minutes. This certification ensures that consumers' phones can resist accidental dips into water or light rain. However, it is crucial to remember that the IP68 water resistance certification does not imply that the devices are completely waterproof, and they should not be purposely immersed or exposed to harmful liquids such as salt water or ionised water. The efficiency of water resistance may decline over time owing to regular wear and tear; also, water damage is often not covered by warranty.

Information Asset: Information assets saved locally on the Samsung Galaxy S24, such as contacts, local photos, videos, and app data, are susceptible to loss or corruption if not backed up to cloud storage. These assets are stored within the device's memory when it is vulnerable.

Threat: Exposure to environments with high-volume water beyond 1.5 metres deep for more than 30 minutes, or harmful liquids like saline and chlorinated water. Such conditions would compromise the availability and/or integrity of these assets.

Vulnerability: The S24 is designed to be water resistant rather than fully waterproof, making it susceptible to liquid damage.

Security Incident / Attack: Chlorination is an important phase in the water treatment process that involves adding chlorine to water to kill unwanted microbes such as viruses, bacteria, and cysts (WaterProfessionals, n.d.). As a Commercial Delivery Manager of Waterworks, the user will frequently visit the water treatment plant to meet with stakeholders and clients, providing tours and explanations of the company's water purification methods. Due to the frequent closeness to chlorinated water basins during these demonstrations, there is an increased risk of accidents, such as the manager's phone falling into chlorinated water. Such a security incident could cause the phone's internal components to be destroyed by the corrosive nature of chlorine, perhaps resulting in loss of functionality and data.

Privacy impact analysis

An application commonly used for personal use by the Waterworks manager is Facebook by Meta. The relevant privacy policy for Facebook is the Meta Privacy Policy available at its website (Meta, 2022a). Using the Meta Privacy Policy, we can analyse a sample of privacy risks that may arise from a popular application's (Facebook's) personal use. Meta collects information that can be generalised into four categories (Meta, 2022b):

- User activity and user-provided information. Meta products, such as Facebook, collect user 'activity', defined non-exhaustively as sent messages, photos and videos, buying and selling things. This includes content the user creates, shares, or provides (through activity), metadata on content and messages, content viewed or interacted with and how it's interacted with applications and features used as well as actions taken in them, purchases or other transactions (including credit card information), hashtags used, and the time, frequency, and duration of activities on Meta products. Sensitive information (e.g. religious beliefs) however, may have special protection under laws of the user's jurisdiction.

- Friends, followers and connections. Meta collects contact information (name, email, phone, etc.) and contacts connected to the device. Information may still be collected for people who do not use Meta Products, or use them without an account. Meta also collects inferential information based on other's activity, where they may suggest friends based on whether they both appear on the same uploaded contact list.

- App, browser, and device information. Meta collects and receives information from devices and how they are used. This pertains to the device's software and characteristics (such as hardware information), what the user is doing on their device, device identifiers, device signals, application-shared information (GPS location, camera access, photos, and related metadata), network information (such as IP addresses), location-related information (e.g. location estimates using IP address), Meta product performance on device, and cookies.

- Information from partners, vendors and third parties. This information regards device information, websites visited and cookie data, apps used, games played, purchases made on Meta products, user demographics (e.g. education level), advertisements shown and/or interacted with, and information collected from partners' products and services.

Meta has a plethora of avenues to collect data on the user. Firstly, Meta collects information directly from users when they provide information. This collection is exemplified by Meta's definition of 'activities'. This information also includes how users interact with the platform and associated metadata. Device information is also collected. Meta also uses tracking technologies (such as cookies and pixel tags) to collect data for personalisation. They also share information with and receive information from partners, vendors, and third-party sources for other personalised services. All of this information, apart from third-party data mining, is requested by Meta and subsequently consented to, subject to Facebook's Terms of Service. Meta is of the view that all this information is required to maintain the 'quality of user experience' for the services they provide on their platform.

Shockingly, even if you don't have an account, Meta will collect information on that individual if they interact with Meta Products. Browser and application logs of visits to public content on Meta products will be collected, alongside the device model and operating system. Information is also collected from partners using 'Meta Business Tools'. These 'tools' are technologies offered by Meta to application developers, and business partners (including advertisers) that measure products and services with a priority of targeting or personalisation. These tools include (1) Meta pixel, used in websites to track the effectiveness of advertising and actions taken on the site (Meta, 2023). (2) Conversions API, connects an advertiser's marketing data with Meta to optimise advertisement targeting, cost, and outcomes. (3) App Events API, enables applications or web pages to track user events through the Facebook Software Development Kit's automatic data logging (Meta, n.d.-a.). (4) Meta Ads Manager, provides set up and management of advertisement campaigns (Meta Blueprint, 2022). (5) Facebook Social Plugins, provide applications the functionality to like, share, comment, etc. (Meta, n.d.-c). (6) Facebook Login, allows Facebook users to log into connected applications or websites (Meta, n.d.-b). Meta outsources their data to measurement and marketing vendors to analyse and optimise advertisement interactions. Meta may also sell de-identified user data to other third parties.

Facebook tracks some information at all times through the use of cookies. This is different to when Facebook is currently running and tracking information such as whether it is in the foreground, the mouse cursor is moving, and location information. With cookies, Meta can compile more information about the user, such as information about the use of other websites and applications as well as device information, whether or not the user is registered or logged in. This means not only does Facebook gather data on logged-off users, but also gathers data on unregistered individuals who may have interacted with a Meta product.

Meta justifies their extensive user information collection with arguments of content and targeted advertising personalisation, security, and safety.

Detailed Phone Applications Description and Analysis systems are used against cyber attacks or terms of service violations (e.g. scraping from bots), user safety from harmful content, and performance of their products. Through the sharing of user information with 'external researchers', Meta claims that their business or mission, social good (crisis response through research support), technological advancement, public interest, and health and well-being. The privacy policy briefly states that they may also sell de-identified user data to other third parties. Overall, only the personalisation and integrity that Meta offers are directly related to the user's purpose for use. Whilst sharing data for social good and other seemingly altruistic reasons is beneficial to a lot, the individual user's purpose is not for this. The collected information is primarily focused towards the benefit of Meta and the user's experience of their products appears to be secondary.

Meta retains information on a case-by-case basis and for as long as it is required. This includes information necessary for the operation or provision of products (e.g. information to maintain account), features that require the information, retaining information to comply with legal obligations, and other 'legitimate' purposes "such as to prevent harm; investigate possible violations of our terms or policies; promote safety, security and integrity; or protect ourselves, including our

rights, property or products". In addition, Meta's privacy policy preserves information from accounts that have been disabled or have violated their terms and policies. Data will be kept until the user's account is deleted or Facebook no longer requires the data to provide their product and services.

Facebook transfers and stores user information in data centres globally. Utilising standard contractual clauses (for global information transfer) approved by the European Commission to ensure data has adequate levels of data protection. They also use equivalent mechanisms under applicable laws that apply to data transfers out of other regions. Currently, Facebook offers encryption on information in transit over public networks and for information in storage.

Information can be shared with other users depending on the privacy setting of the user's profile, where minimal information is shared if their account is private. If the profile is public, others may be able to view a larger amount of personal information and also have access to their posts and interactions. Regarding the sharing of information with third parties, information may be expansively used. In the context of researchers, they can use the information for previously mentioned altruistic motives. For partners and vendors, they can use the information as a tool to process for their businesses or practices. Other third parties (such as advertising vendors) may buy de-identified data from Facebook for targeted advertising.

A Facebook user can access their information through the application or also by downloading their data. The user is required to log in before they can access this data. As the user can access the extensive data collected by Facebook, the risks associated with data breaches become more critical as threat actors may determine Facebook as a viable target. Unauthorised access would be detrimental to the individual user given the excessive access to their personal and other information.

Facebook, for the most part, meets the requirements of Australian privacy legislation. It does not meet Australian Privacy Principle (APP) 2 'anonymity and pseudonymity' and has historically had breaches of APP 6 and 11. While not an issue with the APP's, Facebook tends to have an issue with minimising the user information collected.

- APP 2 - individuals cannot use applications anonymously. It is possible to use Facebook pseudonymously, but is technically a breach of their terms of service. Meta believes the 'real name' policy helps keep users safe. In practicality, Facebook should be able to provide at least pseudonymity or even anonymity, depending on the user's use purpose for the application.

- APP 6 & 11 - Facebook had previously been in breach of APP 6 when they disclosed personal information to the 'This Is Your Digital Life' application. Personal information was disclosed via their friend's use of the application. This also meant a breach of APP 11, as Facebook did not take reasonable steps to protect its users' personal information from unauthorised disclosure; they were not permitted to access that information (OAIC, 2023). Facebook does de-identify personal information for personalisation (such as targeted advertising).

Privacy Risk Identification

Due to the superabundance of information collection, there are quite a few significant security risks for the data associated with Facebook due to its privacy policy. The risk of data breaches will always remain critically important because of the amount of users and personal information that Facebook collects. Meta claims their products meet information security standards, meaning that they do have processes in place to minimise consequences and prevent and detect threats. There are also risks directly toward the users, such as social engineering attacks (like phishing or impersonation) which may allow subsequent attacks to occur. The greatest risk stems from Meta's privacy policy, where there is a noticeable trend of data mining for user information. As the collected information is not minimised, the user risk becomes far greater. Facebook also has a history of sharing and selling personal information, breaching user privacy. Users also do not have the option for anonymity or pseudonymity if using Facebook legitimately, meaning that users are limited in how their information is available to others. Meta also collects inferential information about users from third parties, increasing the amount of information that they have. Due to the user risks associated with Facebook use, there is also a substantial risk for Waterworks. If data breaches occur, threat actors will have an easy time launching further malicious attacks. Identity theft or credential theft would be a major concern in the context of Waterworks, where the attacker would be able to access Waterworks systems and potentially compromise the availability, integrity, and further confidentiality through subsequent attacks depending on their intent. This concern is not contained solely in data breaches, as the manager of Waterworks is also susceptible to direct social engineering attacks on Facebook. Malicious actors may target the manager of Waterworks for his elevated position in an integral utility company. This information may even be publicly available on their Facebook profile given Meta's privacy policy. Meta's privacy policy allows alternative entry to breach Waterworks through attacks on the manager.

The Waterworks assets at risk are expensive. Some information assets may be in the form of contractual information that could be exposed or altered for reputational and financial damage, resulting in the termination of current or future contracts. The threat of unauthorised access is most likely to occur through vulnerabilities associated with employees of Waterworks. This does not necessarily mean insider attacks but includes exploitation of vulnerabilities towards the individual. The threats are primarily focused towards social engineering, but other cyber attacks would yield the same results but with more difficulty. Through Facebook, phishing is possible via messaging and may include impersonation or identity theft. Another threat would be identity theft of the user, possibly from inferential data mining, but would more likely be due to the inability to be anonymous or pseudonymous on Facebook. Data breaches may occur, exacerbated by the number of entities that Facebook shares user information with. Not only is the threat directed towards Facebook, but also the third parties or partners that have received shared information. The Waterworks manager may not only ruin their reputation but also the company's if they were the vulnerability that was exploited. The manager may lose their job, causing detrimental emotional damage from failing responsibility. Waterworks could also have infrastructure, planning, or strategies foiled through the alteration of developmental data. If the data tampering is not detected, then there may be adverse

legal consequences for the business in the future. If the system is compromised, then the confidentiality of employees personal and sensitive information is also at risk.

Risk Evaluation and Prioritization for Treatment

Risk 1 - Android lock screen bug

There is a risk that while driving mode on Google Maps application is activated on the Samsung S24, an attacker can bypass the security of the device, exposing the user's personal and professional data at risk. Their Google account will then be compromised, leading to potential unauthorised sharing, editing, and exposure of their media. As a result, the confidentiality, integrity and availability of the user's personal and work related media is at risk. Following these events the user's employment may be subject to termination, and personal relationships may be impacted severely. The organisation could suffer minor effects on annual profit, data breaches, and reputational damage.

Given the complexity of human factors and the difficulty of assigning precise numerical values to potential losses, we use a qualitative risk analysis - OWASP Risk Rating Methodology - to assess the severity of impact and likelihood of the event. This is done by determining the level of the likelihood and impact on a scale from 0 to 9, with scores less than 3 indicating "Low" risk, 3 to less 6 is "Medium" and 6 to 9 is "High" (Williams, n.d.). As shown in the *Appendix 5,* the methodology provides a structured approach to assess the likelihood (threat and vulnerability factors) and the impact (through technical and business lenses) of the security risks, along with a detailed scaling system for these factors. After several considerations, the values are assigned to each risk factor (see *Appendix 6*), leading to the classification of both likelihood and impact as "Medium", therefore, the overall risk of severity is "Medium" as well. In light of the assessed medium-level risk, a Risk Modification strategy will be implemented. This approach includes strengthening technical defences with regular software and operating system patches, enforcing policy guidelines for device usage, especially in public or insecure areas, and performing tailored training sessions to raise employee awareness of the unique hazards.

Risk 2 - Phishing Attacks

There is a risk that an active social engineering attacker will gain the trust of the user, gaining access to the user's personal information and account details. In turn the users' work-related and personal accounts on applications such as Commbank and Geo SCADA may be compromised in the hands of an attacker. This therefore endangers the confidentiality, integrity and availability of the user's compromised information as an attacker would have authentication that meets the level of the user. This may impact the user's company significantly depending on the user's access level as well as the users financial safety.

Due to the article containing quantitative data regarding the frequency of a user engaging with a phishing attack, it is possible to determine a value for likelihood of attack when considering the data. According to (refer source) phishing attacks generated by social engineers had an interaction rate of 14% for this particular investigation. This suggests that the majority user's will not interact, however

it largely depends on the education of the user. For the sake of determining the overall risk severity qualitative and quantitative scales were used for likelihood and impact respectively. 14% interaction rate suggests a low likelihood for interactions with social engineering attacks, while the impacts (see *Appendix 7*) appear to be “High”. Following the risk severity matrix this suggests a “High” risk severity. Therefore, it is crucial to mitigate the potential for this attack occurring, through in-depth education for users to identify possible phishing or manipulation tactics and a report system to prevent multiple attacks.

Risk 3 - Water Damage

There is a risk that while providing tours and explanations of the company's water purification methods, the user accidentally drops the phone into chlorinated water basins, leading to the loss of functionality and data due to internal destruction, and potentially having a negative impact on the business operation. Because of the lack of statistical data regarding the severity and frequency of dropping a phone into chlorinated water, particularly, a single quantitative analysis is not the most appropriate approach; it can be variable and unpredictable. Therefore, a qualitative analysis will be utilised.

As stated by Duk Gear (2021), 28% of consumers will drop their phones into liquid, considered a low likelihood. This probability declines for particular scenarios like falling it in chlorinated water, resulting in the conclusion that the overall likelihood of such an incident is “Low”. The impact is also categorised as “Low” (see *Appendix 8*) since only personal data on the device could be lost (work-related data secured in cloud storage). Any minor disruptions to business services can be swiftly addressed by providing the manager a new phone (minimal repair costs and influences). Given the assessment using the risk severity matrix, the overall risk of a phone being damaged by chlorinated water is “Low”. To reduce the likelihood of this incident, it would be prudent to inform the manager about the risk’s existence. Moreover, equipping the manager with a waterproof case during the demonstrations of the water treatment process can serve as an extra safeguard.

Risk 4 - Privacy

Two risks identified during the analysis of Facebook’s privacy policy are identity theft and phishing. Identity theft can occur through a multitude of ways due to the privacy policy of the application. Due to the extensive user information collection and inability to legitimately use the application anonymously or pseudonymously. Through the exploitation of those vulnerabilities, other users (legitimate or illegitimate) can view the user’s profile and gather an abundance of information (somewhat lessened if privacy settings are configured). In combination with inferential data from other sources, it becomes a very simple avenue for a malicious actor to gain enough information on the victim and assume their identity. The social aspect of the Facebook application enables the risk of phishing through the platform. Messages and posts are able to include links for the delivery of malware. Threat actors can impersonate others in order to phish for the user’s information assets (may be in the form of personal or sensitive information). Although Facebook’s privacy policy does not allow impersonation or the illegitimate use of their application, it is not prevented from occurring. Facebook relies on the detection of these accounts through user reporting and does not provide insight on whether other detective measures are or how effective user reporting is as a sole

detector. The aftermath would most likely be directed towards an attack on the Waterworks manager in this context, as an attack on Waterworks would be more complex and risky, aiming to embezzle a sum from them. Attacks directed towards Waterworks, using the manager as a vulnerability to exploit, are possible whereby the attacker could gain authentication and elevated access in Waterworks systems through identity theft (and/or credential theft). Consequences would not only be catastrophic for the company, but also to society due to its critical infrastructure and development.

The likelihood of phishing for personal information occurring is high, accounting for the vulnerabilities arising from Facebook's privacy policy. To phish, anonymous internet users do not require any specific technical skills. Depending on their intent, their skill level may vary accordingly. Exploiting an individual using phishing is completely dependent on the target's competency, so the exploit was rated as 'hard' with 'possible reward'. There would exist automated tools to aid attackers in the discovery of public profiles, but specific targeting based on employment (Waterworks manager) would be obvious and not hidden (due to assumed public profile). Considering both personal and business contexts (Waterworks), only extensive non-sensitive data would be breached with a minimal secondary service becoming unavailable (Facebook). Based on the Meta privacy policy, Facebook does not collect or store sensitive information. However, this sensitive information becomes public information if a user discloses this through a public medium on their platform. In this case, Waterworks is not impacted due to the intent of the attacker. As per Appendix 9, the risk is calculated to be 'medium'. Although the impact is low (in the context of Waterworks), the likelihood is quite high given the ease of personal information access.

In another case, identity theft could occur from the same vulnerabilities stemming from Facebook's privacy policy. The potential impact would be devastating for both the Waterworks manager and the company. The risk factors in this scenario are vastly more unlikely due to high skill requirements and use of resources. The attack would be much more complicated with standardised data security systems and processes in place. Although the attack may seem unlikely or deterring, the reward and damage would be 'high'. Through identity theft, a knowledgeable threat actor could gain elevated authentication and access into the system and breach confidentiality, integrity, and availability completely. This would cause utter financial and reputational among compliance and privacy violations. Pessimistically exploiting the vulnerabilities from both Facebook's privacy policy and the manager, an attacker could enact an elaborate attack to gain full access to both the manager and Waterworks systems and hold the essential service and information at ransom. As per Appendix 10, this risk is calculated to be 'high' and is recommended to be treated as a priority due to the impact severity.

Risk Treatment and Countermeasures

I. Control measure for Risk 1 - Android lock screen bug

Overview of security issue from Part A: Android lock screen bug

A serious security flaw has been identified in Android 13 and 14, allowing attackers with physical access to a smartphone to bypass the lock screen and get access to personal information such as photos, contacts, and browser history. This vulnerability, identified by security researcher Jose Rodriguez, exploits a feature in Google Maps and has yet to be patched, despite being notified to Google. It jeopardises the security, integrity, and availability of sensitive user information.

Treating the risk

Suggested control measure and explanation:

Implementing multi-factor authentication (MFA) on the device's Google account improves security by demanding various kinds of verification before providing account access. This guarantees that even if the lock screen is overcome, the attacker must provide other authentication factors to access sensitive data and services associated with the Google account.

Type of control measure:

Multi-factor authentication (MFA) is a preventative control method that adds an extra layer of protection, requiring more than one factor to get access. This approach is technologically based since it uses authentication technologies including one-time passwords (OTPs), authenticator applications, biometric checks, and security tokens (ACSC, 2023b). MFA greatly improves security by complicating unauthorised access attempts, even if they avoid the initial security procedures. Furthermore, the Australian Cyber Security Centre (ACSC) advises in its guideline for IoT device makers that any related online accounts use WebAuthn or multi-factor authentication (2023a).

Degree of protection provided:

MFA provides an additional layer of security beyond just the device lock screen, which significantly reduces the likelihood of an unauthorised access to a Google account. By requiring multiple verification methods, MFA ensures security even if one factor is compromised. The effectiveness of MFA is supported by research, which indicates that it can lower the risk of compromise by 99.22% (Meyer et al., 2023).

Limitations of this control measure:

Users may find the additional login steps inconvenient, especially when accessing accounts frequently. Moreover, the effectiveness of MFA depends on the strength and security of the authentication factors used. Finally, deploying MFA may incur additional expenditures for enterprises, such as acquiring hardware tokens or integrating biometric systems.

Reference details:

ACSC (2023a) IoT Secure-by-Design Guidance for Manufacturers. Retrieved from IoT Secure-by-Design Guidance for Manufacturers | Cyber.gov.au Date accessed: 21 May 2024.

ACSC (2023b) Protect Yourself: Multi-Factor Authentication. Retrieved from Protect Yourself: Multi-Factor Authentication | Cyber.gov.au Date accessed: 21 May 2024.

Meyer, L. A., Romero, S., Bertoli, G., Burt, T., Weinert, A., & Ferres, J. L. (2023) How effective is multifactor authentication at deterring cyberattacks?. Retrieved from How effective is multifactor authentication at deterring cyberattacks? Date accessed: 21 May 2024.

II. Control measure for Risk 2 - Phishing attack

Overview of security issue from Part A: Phishing attack

By way of social engineering it is possible for malicious actors to gain the trust of the user through impersonation, this is referred to as phishing, the objective of which is to have the user hand over sensitive information such as login credentials and personal information. A successful phishing scam performed on the case device has a "High" severity rating on the Severity Matrix, due to it compromising all three security goals (Confidentiality, Integrity, Availability).

Treating the risk

Suggested control measure and explanation:

Implementing a consistent and regimented cyber security training program, that all employees are to partake in, helps ensure workers are educated and aware of vulnerabilities. This allows employees to identify potential phishing scams by recognizing common tactics and strategies employed by malicious actors, and to develop habits that allow them distinguish inconsistencies in the phishing scams.

Type of control measure:

Cyber security training is a preventative type of control method, implemented to help reduce multiple risk vectors such as, phishing scams, password management, ransomware, portable media and network connections. The objective of the training is to educate employees on the types of information that attackers are attempting to obtain, what platforms they will use to trick users and what methods they will employ to obtain the information.

Degree of protection provided:

Educated users are less likely to fall victim to phishing, mitigating the likelihood of successful attacks. A report of ProofPoint in 2021 revealed a significant impact - 80% of organisations reported reduced employee's susceptibility to phishing attempts after implementing security awareness training. Moreover, consistent training programs have been shown to considerably curb the risk, declining from 60% to just 10% within the first 12 months (Daily, n.d.).

Limitations of this control measure:

The effectiveness of this control measure depends on employees' engagement and adherence to training programs. It requires time and money to follow and maintain effective training services. Human error remains a problem, and even well-trained individuals can occasionally fall for sophisticated phishing techniques.

Reference details:

Daly, J. (n.d.) How often should employees really receive security awareness training?. Retrieved from How often should employees really receive security awareness training Date accessed: 21 May 2024.

ProofPoint (2021). 2021 State of the Phish: An In-Depth Look at User Awareness, Vulnerability and Resilience. Retrieved from An In-Depth Look at User Awareness, Vulnerability and Resilience. Date accessed: 21 May 2024.

III. Control measure for Risk 3 - Water damage

Overview of security issue from Part A: Water damage

Due to the nature of the Water utility company, it has been identified that during the course of their duties the user will be exposed to additional levels of risk from water to their phone. If exposed to the chlorinated water of the plant facilities, the phone could experience a short circuit resulting in stored data becoming corrupted, additionally the availability to work related functions would be compromised as the phone would be in an unusable state. However, after assessment via a risk matrix, the likelihood and consequence was assigned “low”, due to the use of cloud storage of critical data and the ease of replacement.

Treating the risk

Suggested control measure and explanation:

The user's phone model, a Samsung s24, is a relatively popular model, as such a number of cases are available for purchase, among these are many which are designed to be waterproof, designated with the IP68 rating. Ingress Protection (IP) 68 is a part of the IEC 60529 international standard, and refers to an electrical enclosure that is considered both dust-tight and “Protected against the effects of continuous immersion in water” (IEC, 2024).

Type of control measure:

This measure is preventive because it aims to stop water from entering the phone by providing physical protection to the device. It is technologically based as it relies on materials and design features that provide water resistance.

Degree of protection provided:

Significantly decreases the chance of water damage by providing physical protection to the device. Protects the phone’s functionality and data integrity, mitigating potential operational disruptions and data loss. However, they do not provide absolute protection. For example, OverBoard’s IP68 waterproof cases are meant to protect devices at depths of up to 6 metres for 60 minutes (2024). Beyond these limits, the protection may not be effective.

Limitations of this control measure:

Waterproof cases may add bulk to the device, affecting its ease of use. It is possible to incur additional costs when purchasing high-quality waterproof cases. At all times, the case must remain intact and properly sealed. Wear and tear may diminish the effectiveness of the waterproof seal over time, necessitating frequent examination and potential replacement. Furthermore total water protection cases such as waterproof sleeves may limit accessibility of the device in exchange for added protection. Finally, features such as less sensitive touch screen, camera quality & audio input/output may be hindered or inaccessible due to the added protection.

Reference details:

IEC (2024) IP ratings. Retrieved from IP ratings | IEC Date accessed: 21 May 2024.
OverBoard (2024). IP68 Waterproof Rated Products. Retrieved from IP68 Waterproof Rated Products Date accessed: 21 May 2024.

IV. Control measure for Risk 4 - Privacy policy

Overview of security issue from Part A: Facebook privacy policy

One of the two vulnerabilities arising from Meta's privacy policy was phishing. There are many ways that phishing attacks can occur on the Facebook application to steal user information, such as malicious links to deliver malware presented via direct messages, posts, or even text-editable fields on user profiles. The most effective way that phishing is enacted through Facebook would be through spear-phishing (likely through impersonation). As the privacy policy does not allow legitimate anonymity or pseudonymity, limited personal information is readily available for targeted impersonation of users. Phishing attempts can more commonly occur (but less effectively) through bot accounts, directly messaging users with suspicious links. These phishing attacks attempt to directly violate the confidentiality of the user's login credentials, financial information, and other personal information. The availability and integrity of personal information (on Facebook) can be subsequently breached, depending on the actor's intent. Other applications are also at risk for confidentiality, integrity, and availability if the user reuses the same login credentials.

Treating the risk

Suggested control measure and explanation:

Enabling phishing-resistant two-factor authentication (2FA) on Facebook with a security key is an effective method to reduce the impact of successful phishing attacks. 2FA is an option for Facebook users offered upon account creation (Facebook, n.d.); however, it is not mandatory and is likely overlooked by many users due to decreased usability. The only phishing-resistant 2FA option Facebook provides is a physical security key.

Type of control measure:

The use of phishing-resistant 2FA is a preventive control measure, aiming to prevent the majority of phishing attacks through the additional authentication factor. The type of authentication used in this case is a physical security key, providing more protection than other 2FA options but less usability. In this context, attackers will need to have access to the physical security key, which would require enacting another attack (e.g., theft) to gain access to the user's Facebook account. This narrows the threat pool to extremely sophisticated, targeted, and localised attacks, which is equally unlikely if the goal is Facebook account compromise.

Degree of protection provided:

There is a substantial reduction in the consequences of phishing attempts through the large prevention of successful attacks. As security tokens are phishing-resistant, subsequent attacks on the additional authentication measure are required to compromise user data. It is considered phishing-resistant as it is possible for a phishing attack to convince the target to send their security token (e.g., through the impersonation of the token provider claiming that the device is faulty and

requires repair). A great asset of phishing-resistant authentication is its subversion (risk avoidance) of widely used MFA vulnerabilities such as push bombing, SS7, and SIM swap attacks (CISA, 2022).

Limitations of this control measure:
Phishing-resistant 2FA on Facebook offers a great increase in protection against phishing but trades off user usability and convenience. Whenever a user wants to login to Facebook, they would now require their physical security key that is easily lost or forgotten; the user's access entirely depends on their remembrance to possess the security key.

Another limitation is introducing the risk of theft. Theft of the security token immediately compromises the availability of Facebook, and depending on the threat actor, has the potential for subsequent attacks to compromise the confidentiality and integrity of user data. Although introducing a new vulnerability, the overall risk is greatly reduced and therefore at a much more acceptable level.

Reference details:
CISA (2022) Implementing Phishing-Resistant MFA. Retrieved from Implementing Phishing-Resistant MFA Date accessed: 21 May 2024.
Facebook (n.d.) How two-factor authentication works on Facebook. Retrieved from How two-factor authentication works on Facebook Date accessed: 21 May 2024.

Overview of security issue from Part A: Facebook privacy policy
Identity theft is the second risk resulting from the Meta privacy policy. By collecting a vast amount of personal (and sensitive) information through Facebook, data breaches pose significant and severe consequences. Other attacks to target user information, such as inferential attacks, could ultimately lead to a major risk for the organisation: identity theft. Assuming the identity of the Waterworks manager, they would have practically all the information required to compromise their work account and potentially cause catastrophic damage to the water utility provider (due to the manager's already elevated access). Ransomware is a likely attack that would ultimately be effective in succeeding due to the critical infrastructure of the water provider. The main vulnerability and risk for all these attacks is the venue in which they can cause this damage: identity theft through the use of a third-party application with a poor privacy policy (Facebook).

Treating the risk
Suggested control measure and explanation:
The most effective control measures to mitigate this vulnerability and reduce risk pertain to the Meta privacy policy. Compliance with APP 2 (anonymity and pseudonymity) would allow users to considerably reduce the amount of information compromised in a successful attack. Although not in Australian privacy legislation, good practice would be adherence to the EU GDPR (General Data Protection Regulation) for data minimisation (Intersoft Consulting, 2016).

As requesting a change to Meta's privacy policy is extraordinarily unlikely, a more fitting control measure would be human training. Training would include awareness education on common attempts and recovery from such attacks. As numerous attacks can result in identity theft, traditional

measures such as using stronger passwords and limiting online personal information would be included in training.

Type of control measure:
Privacy policy improvements would be a preventive measure aiming to reduce the impact of successful attacks. This control measure is unlikely to be implemented; however, human education would be worthwhile and will be focused on.

Human training would be considered to be preventive, detective, and corrective. Through training, users can be made aware of and employ traditional security methods if they haven't already, preventing (or, more correctly, reducing) successful attacks to achieve identity theft. Education is also detective, as identity theft is commonly unnoticed (FTC, 2000) and are only notified once some sort of consequence has occurred (ABS, 2024). It is also corrective, as awareness training covers how to respond to identity theft (e.g., changing passwords, reporting the cybercrime to police, and notifying financial institutions) (Victoria Police, 2024).

Degree of protection provided:
Though there are detective identity theft technologies, the human victim will remain the most vulnerable. Building a strong foundation with cyber safety training (including identity theft awareness) will be one of the most expensive investments for risk reduction. A trained human will be exponentially more risk-averse (through prevention, detection, and correction), thereby limiting the severity of the impact of a successful attack. The protection offered is not localised to Facebook but to all applications a user uses, as well as safety against all social engineering attacks.

Limitations of this control measure:
Human training minimally accounts for vulnerabilities apart from the individual trained human (e.g., data breaches from any vulnerability), as they will only be able to enact recovery from successful attacks. In some instances, identity theft is unavoidable, so all that can be done is to reduce the risk where it is controllable.

Reference details:

ABS (2024) Personal Fraud. Retrieved from Personal Fraud Date accessed: 21 May 2024.
FTC (2000) Prepared Statement of the Federal Trade Commission on Identity Theft. Retrieved from Prepared Statement of the Federal Trade Commission on Identity Theft Date accessed: 21 May 2024.
Intersoft Consulting (2016) Art. 5 GDPR – Principles relating to processing of personal data. Retrieved from Principles relating to processing of personal data Date accessed: 21 May 2024.
Victoria Police (2024) Online identity theft. Retrieved from Online identity theft Date accessed: 21 May 2024.

Recommendations

I. Organisational Controls

Implementation of a well-defined policy that formally meets the requirements for AS/NZS 27002:2022 Control 5.1 ensures Waterworks Utilities management supports the protection of its company's sensitive information from unauthorised access. Control 5.1 should aim to prevent and reduce risk of data loss or theft. Guidelines exist for implementation of control 5.1 which should be followed and considered. Top level managerial approval process for the policy should then take place to ensure the policy meets these standards. The policy for responses in relation to phishing attacks should be shared with internal and external stakeholders (ISMS.ONLINE, n.d.). The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its stability remains applicable for the purpose of information security. Control 5.1 is a preventative measure and the organisation's policy should reflect preventative measures in relation to both phishing attacks and lay out standards for device usage. Advisory organisations have an estimated cost of $5000.00 AUD per year to advise management for policy changes and implementation (Capterra, n.d.). In terms of time of implementation, generally a policy meeting these standards should be considered with changes in cybersecurity industry standards for the prospective future of the organisation .

Waterworks Utilities defining a policy surrounding the use of 'Good Cloud' cloud storage in regards to the storage and access of work-related data. Cloud storage through Google Cloud is aimed at enabling organisations to access, store and maintain data. Removing the cost requirements for implementing and operating a first-party data centre. Google Cloud's data storage network is maintainable and can be adjusted according to an organisation's needs. There are multiple modes of google cloud storage being, private, public and hybrid storage networks (Google Cloud, n.d.). This may be considered in terms of the sensitivity of data and its accessibility for employees. Furthermore google cloud requires multi-factored authentication for access. Policy for cloud storage should consider the security, sustainability, control and compliance with industry standards. Therefore the implementation of Google Cloud storage may potentially reduce required costs as there is no need for an on-site data centre. Alternatively reduces the time and resources required to erect a functional and secure data storage network for the organisation.

II. People Controls

Education

Organised training programs for cyber security ensures employees are provided with the necessary knowledge and combative techniques that may not come naturally to their positions, by providing them with this base knowledge Waterworks would be empowering employees to develop good security habits and logical deduction skills to alert themselves and others to ever changing attack methods and vectors of malicious actors.

Waterworks would begin with identifying and grouping employees with similar access to specific technologies, this will allow them to establish which employees will require more extensive training

and which employees require a minimum standard. Following this employees will be organised to attend seminars in staggered waves to prevent undue interruption to regular work schedules, during the training sessions all employees will be educated on subjects such as: techniques for creating secure passwords and appropriate means of storage, using internet browsers safely and viewing work appropriate content, securing data correctly using cloud services and, identification and recognition of phishing attacks.

The second major portion of the training will then shift focus to incident response, that being what employees are expected to do in critical cyber security events. Many cyber security incidents are time sensitive and require employees to execute specific actions as soon as possible, in order for the most favourable outcome to be achieved, so the focus of the training will be placed on quick response times and effective decision making.

Upon compilation of the training session it is important to ensure that the information was appropriately conveyed, this should be completed through 3 different avenues. The first is an online quiz, the objective of which is simply to assess if employees retained the information during the training session. When designing questions for the quiz, the writer should aim to make the questions clear and reasonably straightforward; this will ensure the data derived from the quiz will directly relate to employee comprehension. Secondly as a means to test employees are implementing demonstrated techniques to recognize and verify phishing scams, it is imperative that Waterworks establish regular phishing simulations, this can be done using services such as Knowbe4 where employees are sent emails posing as legitimate services, and should the employee respond to the email incorrectly i.e. opening attached links, Waterworks is notified. Workers that are found to be responding incorrectly to these should then be assigned repeat train sessions. As final means to assure the validity of the training sessions implementing a simple feedback survey, will allow employee to give both a self assessment and to provide feedback on the effectiveness of the training, allowing the training to further adapt become more effective.Finally by regimenting the training employees can be updated on any new or developing forms of attack, as well refreshing their current understanding of known vectors.

By Implementing the suggested training structure Waterworks will not only be able to reduce an estimated 60% susceptibility rate of phishing scams down to 10% (Daly, n.d.), they will also be moving themselves more in line with industry standard as, as reported by Commonwealth Cyber Security Posture in 2023 report, found 82% of survey entities have an incident response plan (ASD, 2023). If run within the company, financial costing for this training structure could be made low by utilising the free services such as KnowBe4, with the predominant cost coming mostly from employee salaries. The estimated time for the creation of the training structure would be about 1-2 weeks, and then a further month would be required to perform training sessions, as they would be required to be staggered out, to avoid interruption to workflow.

Identity Theft Awareness Training (in the context of Facebook)

Identity theft is a critical attack that Waterworks should prioritise the prevention of. Meta's privacy policy does not comply with APP 2 (anonymity and pseudonymity) so there is no way to legitimately use Facebook without publicly providing vital personal information. Facebook also data mines to

share and sell such information for their business purpose. This behaviour is a vulnerability as it is a singularly rich source of personal information and poses a substantial risk for Waterworks.

Stealing the identity of a Waterworks manager, in this context, catastrophic damage can occur to the infrastructure, business, and reputation of the utility company. Threat actors would have all the necessary information to gain access to Waterworks systems and wreak havoc with elevated access. The introduction of ransomware is a foreseeable attack for which Waterworks would most likely pay; Waterworks as a business relies on its upkeep - reputational damage and financial losses would be minimised if ransomware is paid. Another dilapidating threat is data integrity compromise. Infrastructure plans and financial information can be altered to suit the attacker's intent, causing crippling reputational damage and a lack of faith in the company.

It is recommended to formally request Meta comply with Australian Privacy legislation to yield the most effective results. As this request is foreseeably unlikely, Waterworks should allocate resources to provide awareness education to employees. The employees are the factors at risk for identity theft and therefore should also be the frontline for protection. Education on all prevention, detection, and correction of this risk will yield the most cost-effective and efficient solution to combat this critical attack. New employees should have identity theft awareness training as part of their role induction, whilst all remaining employees should have time allocated to complete this training. Training should also be renewed annually to ensure employees remain competent.

III. Technological Controls

Enable MFA

Implementing multi-factor authentication (MFA) for Google accounts connected with the device is an important step towards improving security. MFA requires numerous forms of verification before providing account access, so even if the lock screen is overcome, attackers must provide extra authentication factors to access sensitive data stored in Google services. This restriction is consistent with AS/NZS 27002:2002, Section 8.5 on secure authentication (ISMS.ONLINE, n.d.). MFA is crucial for the water utility firm since it offers a strong layer of protection against unauthorised access, especially for key workers like the manager of commercial and delivery, who is using a Samsung S24. Enabling MFA should be completed within the next 7 days and should be prioritised for all key Google accounts used by workers, particularly those containing extremely sensitive information.

Enable Phishing-Resistant 2FA (Security Key) on Facebook

To treat the increased risk of phishing on Facebook, arising from their privacy policy and platform, it is recommended to enable two-factor authentication choosing a physical security key as the added factor. With the use of this phishing-resistant 2FA, the occurrence of a successful attack is vastly lessened which subsequently reduces the overall risk. This 2FA method is only a preventive measure but can also be secondarily regarded as detective as threat actors would attempt to gain access to the security token through (the new risk of) theft or additional phishing attempts. These are very forward methods to gain possession of the security key, which most untrained victims could reasonably identify. This control measure is practical and cost-effective, only marginally affecting the

user's (not Waterworks) time and convenience for Facebook use. Effectively preventing common phishing attacks minimises risk for Waterworks. Phishing can lead to the delivery of malware and the use of compromised information in further attacks. These attacks are of a wide variety (e.g. financial information compromise and identity theft), which is where the risk for Waterworks arises.

Implement Regular Data Backups

It is vital for Waterworks to ensure all work-related data on workers' devices are regularly backed up to Google cloud service, preventing critical information loss due to device damage or other incidents. This aligns with AS/NZS 27002:2002, Section 8.13 on information backup (ISMS.ONLINE, n.d.). In the event of security incidents or attacks, the water utility company can facilitate quick recovery to maintain the business operation. This measure should be implemented immediately and regularly. The setup cost for Google Cloud Storage is moderate, depending on the selected backup option. For instance, Google One offers 2TB of cloud storage for $12.49 per month, which is sufficient for substantial data backup needs. For Waterworks, this cost scales with the number of users and the amount of data being backed up.

Regular Software Updates and Patches

Ensuring all devices are regularly updated with the most recent software updates addresses known operating system vulnerabilities. Regular updates dramatically minimise security flaws, reducing the risk of successful exploitation. This control is consistent with Section 8.8 of AS/NZS 27002:2002 on management of technical vulnerabilities (ISMS.ONLINE, n.d.). For Waterworks, establishing a process for regular software patches is critical to maintain the security integrity of staff's devices, which should be implemented immediately. The costs are modest, with the majority of the time spent by IT staff on monitoring and occasional manual updates.

Use Waterproof Cases

Employees of Waterworks are frequently exposed to environments with high water risk, such as water treatment plants. These cases create a physical barrier that protects devices from accidental water damage, ensuring that devices remain functional and data remains accessible. The organisation is recommended to purchase and distribute waterproof covers for all relevant devices within the following month. The initial cost is reasonable, estimated around $50 per case (OverBoard, 2024), depending on the number of employees and devices that need protection. Replacement costs will range from low to moderate, depending on wear and tear.

Removal of Facebook

The absolute most practical way to entirely remove the risks associated with using Facebook due to its privacy policy would be the deletion of the user account and the removal of the application. In the context of this report, this is the decision of the Waterworks manager and not the company, as it is their personal device. This measure simply requires a small briefing on the risks associated with the applications privacy policy, consuming minimal time, money, and personnel. It is recommended to communicate with employees regarding the potential removal of Facebook for the safety of the company; however, this is unlikely.

References

ABS. (2024). *Personal Fraud*. Www.abs.gov.au. https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/latest-release#:~:text=Key%20statistics

ACSC. (2023a). *IoT Secure-by-Design Guidance for Manufacturers | Cyber.gov.au*. Cyber.gov.au. https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/iot-secure-design-guidance-manufacturers

ACSC. (2023b). *Protect Yourself: Multi-Factor Authentication | Cyber.gov.au*. Cyber.gov.au. https://www.cyber.gov.au/protect-yourself/resources-protect-yourself/personal-security-guides/protect-yourself-multi-factor-authentication

ASD. (2023). *The Commonwealth Cyber Security Posture in 2023 | Cyber.gov.au*. Cyber.gov.au. https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/commonwealth-cyber-security-posture-2023

Capterra. (n.d.). *Hicomply.* Capterra. https://www.capterra.com.au/software/1033067/hicomply

CISA. (2022). *Implementing Phishing-Resistant MFA.* https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

Daly, J. (n.d.). *How often should employees really receive security awareness training?* Blog.usecure.io. https://blog.usecure.io/how-often-should-employees-really-receive-security-awareness-training

Dropbox. (2023). *Dropbox - Privacy Policy.* Dropbox. https://www.dropbox.com/privacy

Duk Gear. (2021). *5 Shocking Cell Phone Statistics That Are Sure to Blow Your Mind.* DukGear. https://www.dukgear.com/post/5-shocking-cell-phone-statistics-that-are-sure-to-blow-your-mind

Esri. (2019). *What is arcgis online?*—arcgis online help | arcgis. Arcgis. https://doc.arcgis.com/en/arcgis-online/get-started/what-is-agol.htm

Facebook. (n.d.). *How two-factor authentication works on Facebook*. Facebook.com. https://www.facebook.com/help/148233965247823

FTC. (2000). *Prepared Statement of the Federal Trade Commission on Identity Theft.* https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-identity-theft/idthefttest.pdf

Google. (n.d.-a). *Dropbox: Secure Cloud Storage - Apps on Google Play.* Play.google.com. https://play.google.com/store/apps/datasafety?id=com.dropbox.android&hl=en&gl=US

Google. (n.d.-b). *Facebook - Apps on Google Play.* Play.google.com. https://play.google.com/store/apps/datasafety?id=com.facebook.katana&hl=en&gl=US

Google. (n.d.-c). *Fruit Ninja® - Apps on Google Play.* Play.google.com. https://play.google.com/store/apps/datasafety?id=com.halfbrick.fruitninjafree

Google. (n.d.-d). *Geo SCADA Mobile - Apps on Google Play.* Play.google.com. https://play.google.com/store/apps/datasafety?id=com.schneidertcc.android.apps.mobilescada&hl=en&gl=US

Google. (n.d.-e). *Google Photos - Apps on Google Play*. Play.google.com. https://play.google.com/store/apps/datasafety?id=com.google.android.apps.photos&hl=en&gl=US

Google. (n.d.-f). *Microsoft Authenticator - Apps on Google Play.* Play.google.com. https://play.google.com/store/apps/datasafety?id=com.azure.authenticator&hl=en&gl=US

Google. (n.d.-g). *Microsoft Teams - Apps on Google Play*. Play.google.com. https://play.google.com/store/apps/datasafety?id=com.microsoft.teams

Google. (2009). *Privacy Policy – Privacy & Terms – Google.* Google. https://policies.google.com/privacy

Google. (2024). *Get More Storage, More AI capabilities, and More Features.* Google One. https://one.google.com/about/

Google Cloud. (n.d.). *What is Cloud Storage & How Does it Work?* Google Cloud. https://cloud.google.com/learn/what-is-cloud-storage#:~:text=Cloud%20Storage%20enables%20organizations%20to

GSMArena. (2024). *Samsung Galaxy S24.* GSMArena. https://www.google.com/url?q=https://www.gsmarena.com/samsung_galaxy_s24-12773.php&sa=D&source=docs&ust=1713422618269030&usg=AOvVaw05rzCDJvHPES0mrs_dTt4d

IEC. (2024). I*P ratings | IEC.* Www.iec.ch. https://www.iec.ch/ip-ratings

Intersoft Consulting. (2016). *Art. 5 GDPR – Principles relating to processing of personal data.* General Data Protection Regulation. https://gdpr-info.eu/art-5-gdpr/

ISMS.ONLINE. (2020). *ISO 27002:2022 – Control 5.1 – Policies for Information Security.* ISMS.online. https://www.isms.online/iso-27002/control-5-1-policies-for-information-security/

Meta. (n.d.-a). *App Events API. Meta for Developers.* https://developers.facebook.com/docs/marketing-api/app-event-api/

Meta. (n.d.-b). *Facebook Login.* Meta for Developers. https://developers.facebook.com/products/facebook-login/

Meta. (n.d.-c). *Social Plugins.* Meta for Developers. https://developers.facebook.com/docs/plugins

Meta. (2022a). *Facebook.* Facebook. https://www.facebook.com/about/privacy/update/printable

Meta. (2022b). *Meta Privacy Policy - How Meta collects and uses user data.* Facebook. https://www.facebook.com/privacy/policy/

Meta. (2023). *Meta Pixel: Measure, Optimize & Retarget Ads on Facebook & Instagram.* Facebook. https://www.facebook.com/business/tools/meta-pixel

Meta Blueprint. (2022). *Get Started With Meta Ads Manager.* Meta. https://www.facebookblueprint.com/student/activity/212724?ref=cms_redirect#/page/5fc6e1a34a46d349e9dfecb1

Meyer, L. A., Romero, S., Bertoli, G., Burt, T., Weinert, A., & Ferres, J. L. (2023). *How effective is multifactor authentication at deterring cyberattacks?* ArXiv.org. https://doi.org/10.48550/arXiv.2305.00945

MSTonySmith, aditisrivastava07, tonysmit, Kimpossibletoo, SerdarSoysal, hyoshioka0128, donnah007, & v-dihans. (2024). *Data and Privacy Information - Microsoft Teams.* Learn.microsoft.com. https://learn.microsoft.com/en-us/microsoftteams/rooms/data-and-privacy-info

OAIC. (2023). *High Court clears way for OAIC case against Facebook to proceed.* OAIC. https://www.oaic.gov.au/newsroom/high-court-clears-way-for-oaic-case-against-facebook-to-proceed

OverBoard. (2024). *IP68 Waterproof Rated Products.* OverBoard Australia. https://www.over-board.com.au/collections/class-5-ip68-waterproof-rated-products

ProofPoint. (2021). *2021 State of the Phish: An In-Depth Look at User Awareness, Vulnerability and Resilience.* https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2021.pdf

Samsung. (2024). *Samsung Galaxy S24 Series Is Now Available Worldwide.* Samsung. https://news.samsung.com/global/samsung-galaxy-s24-series-is-now-available-worldwide#:~:text=From%20January%2031%2C%20the%20Galaxy

Sbeadle1. (2021). *Mobile Privacy Policy.* Community.se.com. https://community.se.com/t5/Geo-SCADA-Knowledge-Base/Mobile-Privacy-Policy/ba-p/278510

SCADA. (n.d.). *What is SCADA?* SCADA International. https://scada-international.com/what-is-scada/#:~:text=What%20does%20SCADA%20stand%20for

Sevilla, G., & Mcallister, N. (2024). *The Best CRM Software for 2024.* PCMag Australia. https://au.pcmag.com/cloud-services-1/36284/the-best-crm-software

Singh, H. (2024, January 17). *Is the Samsung Galaxy S24 (Ultra) Waterproof?* Answered! Ytechb. https://www.ytechb.com/is-the-samsung-galaxy-s24-ultra-waterproof/

Spadafora, A. (2023, December 11). *Massive Android lock screen bug lets attackers access your photos and other personal data — how to stay safe.* Tom's Guide. https://www.google.com/url?q=https://www.tomsguide.com/news/massive-android-lock-screen-bug-lets-attackers-access-your-photos-and-other-personal-data-how-to-stay-safe&sa=D&source=docs&ust=1714266271513206&usg=AOvVaw2iKZdC7he5pmK5oJ0QYgiG

Townsend, K. (2023, October 24). *The $64k Question: How Does AI Phishing Stack Up Against Human Social Engineers?* SecurityWeek. https://www.securityweek.com/the-64k-question-how-does-ai-phishing-stack-up-against-human-social-engineers/

Unitywater. (n.d.). *Position descriptions for current vacancies.* Unitywater. https://www.unitywater.com/about-us/careers/position-descriptions-for-current-vacancies

Victoria Police. (2024). *Online identity theft.* Www.police.vic.gov.au. https://www.police.vic.gov.au/online-identity-theft

WaterProfessionals. (n.d.). *Process Water Treatment.* WaterProfessionals. https://www.waterprofessionals.com/process-water/

Williams, J. (n.d.). *OWASP Risk Rating Methodology.* Owasp. https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

Appendices

Appendix 1

Article 1: Massive Android lock screen bug lets attackers access your photos and other personal data — how to stay safe

Your locked Android phone may not be as safe as you think

Even though we mainly worry about hackers compromising our devices through malware or malicious apps, a newly discovered bug could allow an attacker with physical access to one of the best Android phones to look at photos, contacts, browsing history and other personal data stored on a device.

As reported by Security Affairs, a security researcher by the name of Jose Rodriguez has found a new lock screen bypass vulnerability that affects smartphones running Android 13 or Android 14.

After asking on social media whether or not it was possible to open a Google Maps link from his phone's lock screen, Rodriguez found that he was able to do so by exploiting a vulnerability.

To make matters worse, Rodriguez claims that he reported the issue to Google back in May of this year and now six months later, it has yet to be patched. Hopefully the search giant addresses this bug soon, but in the meantime here's everything you need to know about this lock screen bypass bug along with what you can do right now to minimize its impact.

Using Google Maps to access your data

The way in which an attacker can exploit this vulnerability to access the data stored on your smartphone depends on how you have Google Maps configured.

For those that do not have Driving mode activated, an attacker can access your recent and favorite locations (like home and work) as well as your contacts. From here, they can also share the location of your phone in real time with any of your contacts or via an email that they need to enter manually.

If you do have Driving mode activated though, an attacker can chain together this exploit with another one to access photos stored on your device, and they can also publish them or add them as a profile image to your Google Account. At the same time, the attacker can also access extensive information about your account and how it's configured. However, there is also the possibility that they can gain full access to your Google Account from a second device — Rodriguez is still looking into that part.

While uninstalling Google Maps from your phone would prevent an attacker from using this lock screen bypass bug to their advantage, since it's a system app, it can't be uninstalled.

In an email to Tom's Guide, a Google spokesperson revealed that "we are aware of this reported issue, and we are working on a fix." However, we still don't have a timeline for when it could roll out to affect Android smartphone users.

How to keep your Android smartphone safe from attacks

Based on what we know so far about this lock screen bypass bug, those who are really concerned about an attacker gaining access to their Android smartphone should consider disabling Driving mode in Google Maps for the time being. While we don't have our own guide on this process, this support document from Google lays out exactly what you need to do to enable or disable Driving mode.

It's worth noting though that an attacker still needs physical access to your smartphone to exploit this bug. For that reason, if you don't let your phone out of your sight, you should be okay until a patch to fix this issue rolls out. This means that you want to avoid leaving your phone on the table when out to eat as an attacker could take it right off the table. Likewise, when using your phone in public, you want to be aware of your surroundings as someone could come along and snatch it out of your hands.

When it comes to cyber attacks and other ways hackers can break into your phone online, the best Android antivirus apps can help keep you safe from malware, malicious apps and other threats. If you're on a tight budget though, you want to make sure that Google Play Protect is enabled on your device as it can also scan all of your existing apps and any new ones you download for malware.

This lock screen bypass bug is quite serious and as it even applies to the latest version of Android, Google is already working on a fix that could be rolled out soon.

Appendix 2

Article 2: The $64k Question: How Does AI Phishing Stack Up Against Human Social Engineers?

Future AI-generated phishing emails are likely to be more effective and damaging than the email-based attacks we are seeing today.

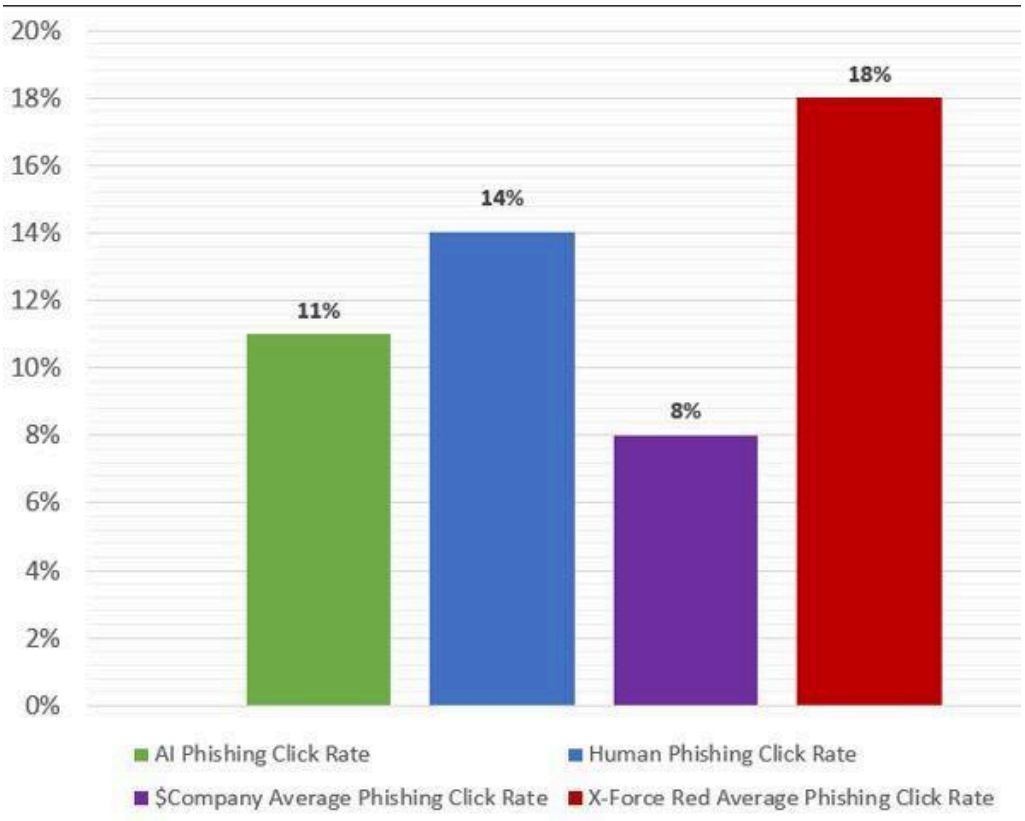
Since the arrival of ChatGPT, the media and security pundits have warned that phishing is now on steroids: more compelling and a vastly increased tempo. IBM's X-Force Red wanted an objective assessment on this subjective assumption.

The method chosen was to test an AI-generated phishing email and a human generated email against employees working for a healthcare firm. Sixteen hundred staff members were selected: 800 received the AI phish, while the other 800 received the human phish.

The outcome of the investigation is that AI can produce a phish considerably faster than humans (five minutes from five simple prompts compared to 16 hours for the IBM human social engineers); but that human social engineering is currently more effective than AI phishing.

Stephanie Carruthers, IBM's Chief People Hacker at X-Force Red, puts human success down to three major factors: emotional intelligence, personalization, and a more succinct and effective headline. "Humans," notes IBM's report on the test, "understand emotions in ways that AI can only dream of.

We can weave narratives that tug at the heartstrings and sound more realistic, making recipients more likely to click on a malicious link."



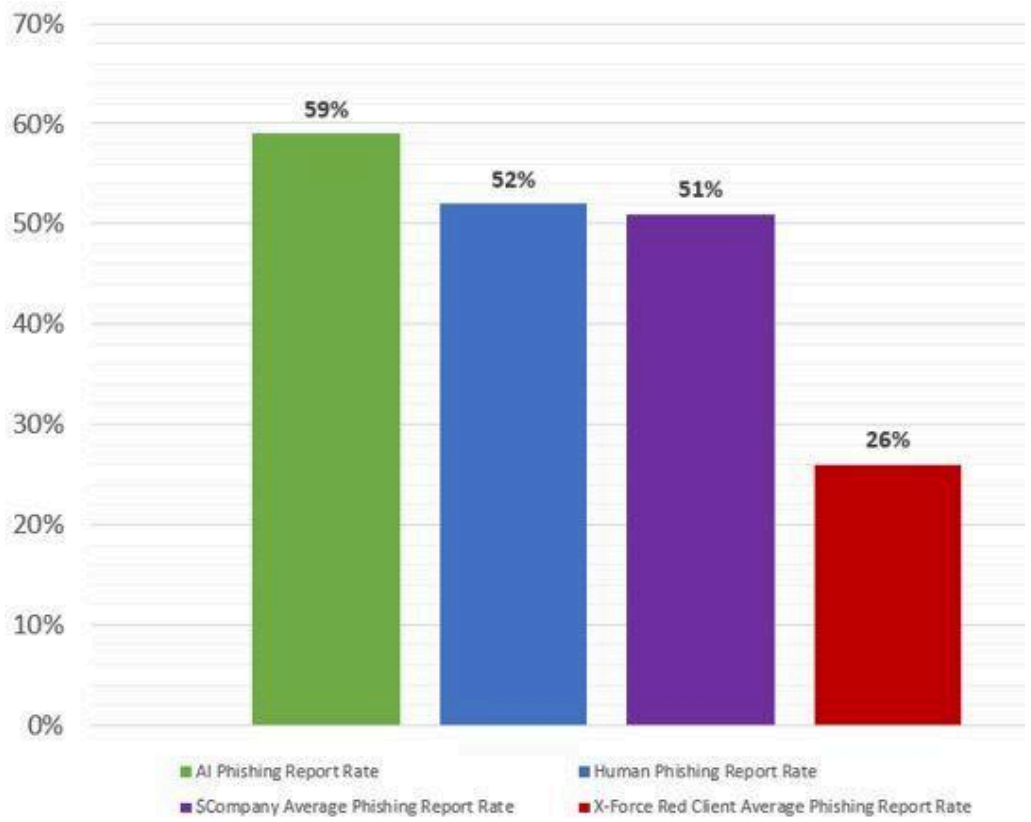
In short, the current algorithmic recompilation of stored knowledge is not as compelling as an OSINT-driven human narrative.

But this is only half the story.

Firstly, the results were close. The human phish achieved a 14% click rate against 11% from the AI phish. Fifty-two percent of the human emails were reported as suspicious, against 59% of the AI emails.

Secondly, AI is in its infancy while human social engineering has been honed over decades of experience. Two questions: could the AI have been used more efficiently (for example with different prompts; that is, better prompt engineering), and how much will AI improve over the next few years?

Carruthers is aware of these issues. "I spent hours creating the prompt engineering and figuring out which ones worked – and I can tell you the first ones I produced were garbage. A lot with AI is garbage in garbage out," she told SecurityWeek. She is confident that these were the best prompts that could be achieved today. "I think I have very solid principles and techniques with what I was asking it to do… I am very happy with the results."



One example explains her efforts. ChatGPT can be prompted to answer in different styles. Given the apparent lack of 'emotional intelligence', could the AI be instructed to respond with greater emotion? "The first responses I got were good, but felt just a bit robotic, a bit cold," said Carruthers. She tried to inject warmth. "But the more I played with it the more like it just started to break – it just doubled down on the coldness, or it got really wacky. It was hard to find that balance."

The second question is the big unknown – how much will AI improve over the next few years? This itself has two parts: how much will publicly available AI improve, and how much will criminal AI improve?

Gen-AI obtains its information from what it ingests. Public gen-AI must be wary in this. It must avoid absorbing dangerous personal information that can then resurface in its responses. Criminal AI has no such concerns. So, while the primary source for public AI will be the surface web (with compliance guardrails), there are no such restrictions for criminal AI – which will most likely combine both the surface and the dark web as its data source, with no guardrails.

The potential for criminal AI to include and combine stolen personal data could lead to highly personalised spear-phishing. If this is combined with improved emotional intelligence, the result is likely to be very different to today's IBM test.

This is subjective conjecture and is exactly what IBM was trying to avoid in its study. But given that ChatGPT can already achieve an 11% success rate in its phishing, it is not something we should completely ignore.

Carruthers own primary takeaway from her study admits such. “If you had asked me before I started who I think would win, I would say humans, hands down. But the more I started prompt engineering, I started getting a little nervous and… these emails are getting better and better,” she told SecurityWeek.

“So, I think my biggest takeaway is to question what the future is going to look like. If we continue to improve gen-AI and make it sound more human, these phishing emails are going to be possibly devastating.”

Appendix 3

***Article 3**:* Is the Samsung Galaxy S24 (Ultra) Waterproof? Does it have an IP Rating?

Samsung has finally unveiled the new Galaxy S24 series, adding three new premium phones to its portfolio. The S-series phones are renowned for delivering the best experience in terms of software, camera, performance, or build. However, these premium features often come with a higher cost.

Following the footsteps of Apple, Samsung introduced the titanium design to its premium Galaxy S24 Ultra. The company says the Galaxy S24 Ultra is our most durable smartphone ever, thanks to the design changes.

Talking about the Galaxy S24 and Galaxy S24 Plus, then these phones come with an Armor Aluminum frame.

If you’re curious about whether the Galaxy S24 is waterproof or water-resistant, you’ve come to the right place. In this guide, I’ll address all your queries regarding the Galaxy S24 series’ durability.

Whether it’s the Galaxy S24, the Galaxy S24 Plus, or the Galaxy S24 Ultra, these phones come with several improvements and upgrades

Let’s shed light on how well the Galaxy S24 and Galaxy S24 Ultra will withstand daily wear and tear.

Are Samsung Galaxy S24 or Galaxy S24 Ultra Waterproof?

No, the new Galaxy S24 series phones are not completely waterproof. Instead, the Samsung Galaxy S24 phones are water-resistant and come with an IP68 rating for dust and water resistance.

The “IP68” rating by the International Electrotechnical Commission (IEC) signifies protection from both solid dust particles and water immersion. The first digit in the Ingress Protection rating, indicates protection against solid dust particles, while, the second digit denotes their ability to withstand water immersion.

Samsung says the new Galaxy S24, S24 Plus, and S24 Ultra can endure submersion in fresh water to a maximum depth of 1.5 meters for up to 30 minutes and are protected from dust – all without the need for extra cases or covers.

In practical terms, the Galaxy S24 series phones are designed to withstand accidental splashes, spills, or light exposure to water.

Another thing to keep in mind is, that water resistance is not permanent it may diminish over time due to normal wear and tear, also, be aware that water damage is typically not covered under warranty.

Samsung advises users to avoid taking the phone to the beach or swimming pool as salt water or ionized water can damage the water and dust resistance feature. Another advice for S24 owners is to promptly rinse, residue, or dry the phone immediately if wet.

What kind of water exposure can the Galaxy S24 resist?

Samsung Galaxy S24 can withstand submersion in up to 1.5 meters of fresh water for up to 30 minutes. All other liquids, including water with salt and chlorine, can damage the phone internally.

Can I take my Galaxy S24 (Ultra) in the shower?

The Galaxy S24 series phones are designed to handle a quick splash or light rain. You can take it in the shower, however, Samsung says the touch screen and some other features may not work properly while the device is in the water.

Just like any electronic device or smartphone, it's important to treat the Galaxy S24 with care and follow the company's guidelines to enjoy its water-resistant capabilities.

Appendix 4

Detailed Phone Applications Description and Information Analysis

Often Used

Application			Information Analysis	
Application	**Description**	**Associated Information: Accessible, collected, stored and/or shared**	**Criticality - potential consequences**	**Sensitivity - security goals and the potential costs.**
CommBank	Commonwealth Bank interface. Used to access personal bank accounts and finances.	● Personal Information: Name, Email address, User IDs, Address, Phone number ● App activity: App interactions, In-app search history ● Financial info: Account Balance, Account Numbers & BSB , Purchase History ● App info and performance : Crash logs, Diagnostics ● Device IDs	From a purely business related perspective the application has very little criticality on Waterworks operations, as it stores nor has any access to business related accounts or information. However from the users perspective, this application has an extremely high criticality as loss of confidentiality would mean the breach of sensitive personal information, and loss of accessibility will restrict users control of personal funds.	Due to the high levels of personal criticality to the user, and the potential for the compromising of both the confidentiality and availability security goals, compounded with loss of time the user will need to invest in resolving the situation, this application has been designated a HIGH sensitivity level.

Drop-box	A Cloud storage interface. Dropbox is used as a company wide storage solution, in addition to their dedicated work folder, the user has access to other company folders, relevant to their work, such as policy documents and contact records, contract details .	● Personal information: Name, email address, User IDs ● Work Related Schematics / Drawings ● Contract Documentation: Drafts, Finalised ● Financial Analytics ● Water Treatment Analytics ● Operational Analytics ● Device Information: attributes, operation, signal, settings ● App activity: App interactions, In-app search history ● Device ID ● Contact Information: contacts name, contacts email address, contacts phone number (Google, n.d.-a; Dropbox, 2024)	Losing access to the account would constitute a breach of accessibility security goals, and result in a major loss of production to the user. Additionally the loss of confidentiality of contained files would result in the exposure of not only preparatory documents but stakeholder private information as well. Finally, given the variety of information stored in the service, a breach of integrity would mean a major loss of long term work and possibly a loss in trust in work that may have been affected.	Given the high criticality in all 3 security goals (confidentiality, integrity and accessibility) combined with severity of cost for time and money to recover from a breach, this application is designated HIGH sensitivity.

Facebook	A Social media website. Users frequently access the application, both on and off the job. They often use the location features of the application to post about where they currently are and what they are doing. The user uploads periodic selfies, some of which the background shows various restricted access environments normally not viewable by the public, others contain office space in which documents can be seen that contain personal information of employees.	● Personal Photos : Photos/videos of owner's self, children, and family members ● Location: precise and approximate ● Personal information: Name, Email address, User IDs, Address, Phone number, Political or religious beliefs, Sexual orientation ● App activity: App interactions, In-app search history ● In app purchase information: user payment information, purchase history, credit score ● Device Information: attributes, operation, signal, settings ● Device IDs ● Contact Information: contacts name, contacts email address, contacts phone number (Google, n.d.-b)	Facebook collects and stores and stores a large amount of data abouts its users, one such data source is the contacts saved to the phone, some of which are other Waterwork state holders that the user communicates with as part of their duties, a breach of this information would constitute a loss in their personal information which could be used in further attacks such as in personation. Facebook also collects a large amount of personal information of the user, of which would be a breach in confidentiality.	In the event of a breach of confidentiality, a large amount of personal data on not just the user but also other connected stakeholder would be lost, however as this information would not directly lead in it self to a major cost to the water works, as a result this application has been designated MODERATE sensitivity.

Geo SCADA Mobile	Remote control and monitoring of PLC equipment.	• Device ID • App info and performance: Crash logs, Diagnostics • Location: approximate, precise • Personal Information: User ID • PLC device information and status (Google, n.d.-d; Sbeadle1, 2021)	Of the applications installed on the device GEO SCADA has the highest levels of criticality, this is because in the result of a malicious actor taking control of the application, they would be able to potentially harm or even destroy the highly expensive connected equipment used for maintaining the Waterworks plant. In a worse case scenario this may even result in the harm of nearby employees.	The Geo Scada application has been evaluated to be of a HIGH sensitivity level. The reasoning behind this decision is predominantly led by the consequences that would occur in the case of the integrity security goal being breached. A breach would likely result in the damage to mission critical equipment, with a high monetary value and high time investment in replacement .
Google Chrome	Internet Browser. Outside personal use the application is used for occasional research about water treatment topics, such as scientific development, competitor behaviour and customer feedback. Furthermore it is used to login into Waterwork ESP	• PLC device information and status • Saved usernames and passwords • Personal Information: Name, email address, User IDs, Address, Phone number • Download History • Network Information: carrier and phone number • Location : approximate • Financial Information: purchase history, stored account information	Like most other internet browsers google chrome stores data about the websites visited and the files downloaded, in general this information would have little consequence given a breach of confidentiality, however websites which the user has saved passwords with are a different matter entirely, as this would allows the malicious actors to access websites that would normally have authentication checks.	With potential for malicious actors to impersonate users and breach integrity security goals, this application houses a risk for significant potential for damage to Waterworks

Google Maps	Provides detailed information about geographical regions and sites worldwide	● User Location:precise ● Business Location: precise ● Route and Navigation information ● Business Listings and Reviews	Unauthorised access to user location data poses severe privacy and safety risks, potentially leading to legal consequences under strict privacy regulations. While the application is not crucial to the company's core activities, there is still a chance of security breaches. Such a leak might jeopardise the integrity of map data, resulting in misdirected personnel, delayed critical repairs or hampered emergency responses.	User location data is highly sensitive and guarded for confidentiality, which can lead to severe privacy violations and legal consequences if compromised. On the other hand, this application has a LOW sensitivity on business operations.
Microsoft Authenticator	Provides 2 factor authentication and account recovery for linked accounts, including those used for Waterwork.	● Temporary authentication codes ● User IDs ● Location: approximate (Google, n.d.-f)	As the application provides the ability to recover accounts, so it does provide potential for malicious actors to steal the access connected accounts, as such breaches of accessibility to the app or confidentiality to recovery codes they hold would lead to disastrous consequences.	Due to the levels of criticality combined with the high potential cost of down time to accounts and/or the possible destruction they may occur during that time, the application is designated HIGH sensitivity

Microsoft Teams	Communication platform. The Application is solely used for work duties such as to communicate with other stakeholders and host online meetings.	● Device ID ● Contact Information: contacts name, contacts email address, contacts phone number ● Personal Information: Name, Email Address, User ID, Phone number ● Message content and metadata: Colleagues and work partners ● Location: approximate, precise ● App activity: App interactions, In-app search history, other user-generated content ● Calendar: event time, event location, event participants ● App info and performance: Crash logs, Diagnostics (Google, n.d.-g; MSTonySmith et al., 2024)	As the application is used solely for work related conversation, the information stored in the chat records will likely contain sensitive information of work related company operations, which in the case of a confidentiality breach could be used for reconnaissance for further attacks or to steal proprietary information. Additionally, loss of accessibility to this application could leave the user without means to contact other stakeholders. Most concerning of all is the potential for loss of integrity, whereby a malicious attacker pretends to be the user via the account and proceeds to prompt other users for sensitive information.	With criticality steaming from all 3 sections of the cyber security goal (confidentiality, accessibility and integrity), and with a high potential damage and cost, due to an impersonation attack, this application has been designated with a HIGH sensitivity.

Rarely Used

Application			Information Analysis	
Application	**Description**	**Associated Information: Accessible ,collected, stored and/or shared**	**Criticality- potential consequences**	**Sensitivity- security goals and the potential costs.**
Google Photos	Stores Photos and Videos. Stored Content is predominantly of a personal nature, depicting the user's self, friends, and family. However intermingled are photos the user has taken as an aspect of their duties and communicating with colleagues, these include Drawings, schematics, Documentation, machinery parts, job sites etc.	● Personal Photos : Photos/videos of owner's self, children, and family members ● Photos of work-related schematics / drawings ● Location: precise and approximate ● Device ID ● App activity: App interactions, In-app search history ● Personal Information: Name, Email address, User IDs, Address, Phone number (Google, n.d.-e)	As the user captures media pertaining to work, said media has a bearing on criticality if a breach of confidentiality were to occur, the extreme of which would be at the loss of technical diagrams pertaining to plants centres as these may contain proprietary operations or be used for further attacks on the plant. Additionally accessibility to the media plays a minor role in the criticality of the application, as users occasionally may need to refer back to the media as referential material, however as the information would likely be able to be reobtained from other sources, it is of minor concern.	In the case of a breach, the loss of availability to this application would be unlikely to result in any economic loss or value loss. Potentially more harmful is the loss of confidentiality of documentation that has been photographed as it may provide information for malicious actors' future attacks. For these reasons this application has a sensitivity rating of moderate.

Fruit ninja	Mobile Game. A free game the user enjoys playing in their free time, although it is possible to purchase additional in-game extras, the user has not done so.	● Device ID ● Personal information: User ID ● Location: approximate ● basic profile information general location of link service: Facebook, Twitter, Game Centre ● Cookies ● App activity: App interactions, duration ● App info and performance : Crash logs, Diagnostics ● Financial history: purchase history (Google, n.d.-c)	The fruit ninja game collects very little information of consequence, outside of some basic personal information and since the user does not make use of the in-app shop, no financial information is collected either.	As the criticality is so low for this application, there is no real way for a breach to result in any cost. For this reason this application is designated LOW sensitivity.

Appendix 5

Scales of OWASP Risk Assessment

	Factors	Components	Scales
Likelihood	Threat Agent Factors	Skill Level	No technical skills (1), some technical skills (3), advanced computer user (5), network and programming skills (6), security penetration skills (9)
		Motive	Low or no reward (1), possible reward (4), high reward (9)
		Opportunity	Full access or expensive resources required (0), special access or resources required (4), some access or resources required (7), no access or resources required (9)
		Size	Developers (2), system administrators (2), intranet users (4), partners (5), authenticated users (6), anonymous Internet users (9)
	Vulnerability Factors	Ease of Discovery	Practically impossible (1), difficult (3), easy (7), automated tools available (9)
		Ease of Exploit	Theoretical (1), difficult (3), easy (5), automated tools available (9)
		Awareness	Unknown (1), hidden (4), obvious (6), public knowledge (9)
		Intrusion Detection	Active detection in application (1), logged and reviewed (3), logged without review (8), not logged (9)
Impact	Technical Impact Factors	Loss of Confidentiality	Minimal non-sensitive data disclosed (2), minimal critical data disclosed (6), extensive non-sensitive data disclosed (6), extensive critical data disclosed (7), all data disclosed (9)
		Loss of Integrity	Minimal slightly corrupt data (1), minimal seriously corrupt data (3), extensive slightly corrupt data (5), extensive seriously corrupt data (7), all data totally corrupt (9)
		Loss of Availability	Minimal secondary services interrupted (1), minimal primary services interrupted (5), extensive secondary services interrupted (5), extensive primary services interrupted (7), all services completely lost (9)
		Loss of Accountability	Fully traceable (1), possibly traceable (7), completely anonymous (9)
	Business Impact Factors	Financial damage	Less than the cost to fix the vulnerability (1), minor effect on annual profit (3), significant effect on annual profit (7), bankruptcy (9)
		Reputation damage	Minimal damage (1), Loss of major accounts (4), loss of goodwill (5), brand damage (9)
		Non-compliance	Minor violation (2), clear violation (5), high profile violation (7)
		Privacy violation	One individual (3), hundreds of people (5), thousands of people (7), millions

			of people (9)

Note. From "OWASP Risk Rating Methodology" by Williams, J., n.d., (https://owasp.org/www-community/OWASP_Risk_Rating_Methodology)

Appendix 6

OWASP Risk Assessment for Risk 1

Likelihood factors

Threat Agent Factors

Skills required	Security penetration skills [1]
Motive	Possible reward [4]
Opportunity	Some access or resources required [7]
Population Size	Partners [5]

Vulnerability Factors

Easy of Discovery	Easy [7]
Ease of Exploit	Theoretical [1]
Awareness	Obvious [6]
Intrusion Detection	Logged without review [8]

Score: O 4.875 (Medium)

Impact factors

Technical Impact Factors

Loss of confidentiality	Extensive critical data disclosed [7]
Loss of Integrity	Extensive seriously corrupt data [7]
Loss of Availability	Extensive primary services interrupted [7
Loss of Accountability	Attack possibly traceable to individual [7]

Business Impact Factors

Financial damage	Minor effect on annual profit [3]
Reputation damage	Minimal damage [1]
Non-Compliance	High profile violation [7]
Privacy violation	One individual [3]

Score: T 7 (High) B 3.5 (Medium) O 5.25 (Medium)

Overall Risk Severity = Likelihood x Impact

	Impact		
Likelihood	Low	***Medium***	High
Low	Low	Low	Medium
Medium	Low	***Medium***	High
High	Medium	High	Critical

Appendix 7

OWASP Risk Assessment for Risk 2 - IMPACT ONLY

Impact factors	
Technical Impact Factors	
Loss of confidentiality	Extensive critical data disclosed [7]
Loss of Integrity	Extensive seriously corrupt data [7]
Loss of Availability	Extensive primary services interrupted [7]
Loss of Accountability	Attack possibly traceable to individual [7]
Business Impact Factors	
Financial damage	Significant effect on annual profit [7]
Reputation damage	Loss of major accounts [4]
Non-Compliance	Clear violation [5]
Privacy violation	Thousands of people [7]
Score: T 7 (High) B 5.75 (Medium) O 6.375 (High)	

Appendix 8

OWASP Risk Assessment for Risk 3 - IMPACT ONLY

Impact factors	
Technical Impact Factors	
Loss of confidentiality	Not Applicable [0]
Loss of Integrity	Not Applicable [0]
Loss of Availability	All services completely lost [9]
Loss of Accountability	Not Applicable [0]
Business Impact Factors	
Financial damage	Damage costs less than to fix the issue [1]
Reputation damage	Minimal damage [1]
Non-Compliance	Not Applicable [0]
Privacy violation	Not Applicable [0]
Score: T 2.25 (Low) B 0.5 (Low) O 1.375 (Low)	

Appendix 9

OWASP Risk Assessment for Risk 4.1

Risk Severity of Phishing - in the context of personal use on Facebook

OWASP Risk Assessment Calculator

Calculate

Likelihood factors		Impact factors	
Threat Agent Factors		**Technical Impact Factors**	
Skills required	No technical skills [9]	Loss of confidentiality	Extensive non-sensitive data disclosed [6]
Motive	Possible reward [4]	Loss of Integrity	Not Applicable [0]
Opportunity	No access or resources required [9]	Loss of Availability	Minimal secondary services interrupted [1]
Population Size	Anonymous Internet users [9]	Loss of Accountability	Attack possibly traceable to individual [7]
Vulnerability Factors		**Business Impact Factors**	
Easy of Discovery	Automated tools available [9]	Financial damage	Not Applicable [0]
Ease of Exploit	Difficult [3]	Reputation damage	Not Applicable [0]
Awareness	Obvious [6]	Non-Compliance	Not Applicable [0]
Intrusion Detection	Not logged [9]	Privacy violation	Not Applicable [0]
Score: O 7.25 (High)		Score: T 3.5 (Medium) B 0 (Low) O 1.75 (Low)	

Overall Risk Severity = Likelihood x Impact

	Impact		
Likelihood	***Low***	Medium	High
Low	Low	Low	Medium
Medium	Low	Medium	High
High	***Medium***	High	Critical

Appendix 10

OWASP Risk Assessment for Risk 4.2

Risk Severity of Identity Theft - in the context of Waterworks

OWASP Risk Assessment Calculator

Calculate

Likelihood factors		Impact factors	
Threat Agent Factors		**Technical Impact Factors**	
Skills required	Security penetration skills [1]	Loss of confidentiality	All data disclosed [9]
Motive	High reward [9]	Loss of Integrity	All data totally corrupt [9]
Opportunity	Special access or resources required [4]	Loss of Availability	All services completely lost [9]
Population Size	Anonymous Internet users [9]	Loss of Accountability	Attack possibly traceable to individual [7]
Vulnerability Factors		**Business Impact Factors**	
Easy of Discovery	Difficult [3]	Financial damage	Backruptcy [9]
Ease of Exploit	Theoretical [1]	Reputation damage	Brand damage [9]
Awareness	Hidden [4]	Non-Compliance	High profile violation [7]
Intrusion Detection	Active detection in application [1]	Privacy violation	Thousands of people [7]
Score: O 4 (Medium)		Score: T 8.5 (High) B 8 (High) O 8.25 (High)	

Overall Risk Severity = Likelihood x Impact

	Impact		
Likelihood	Low	Medium	***High***
Low	Low	Low	Medium
Medium	Low	Medium	***High***
High	Medium	High	Critical