REPORT FOR SHERBOURNE HOUSE

IRM Coursework

Group 4

Table of Contents

1. Our Methodology

To conduct this information risk assessment, we used the ISO 27005:2011 framework. This framework steps through the process of a risk assessment starting with establishing a context. To do this we adapted the framework to include several additional spreadsheets that we thought both helpful and important for conducting the risk assessment while also making it easier for your company to follow the exact steps used to find the information about to be presented to you. These include an information asset profile, a threats sheet and a vulnerabilities sheet. The ISO framework describes the context establishment process as setting the expectations for which the assessment will be conducted. We believe by adding these processes to the context establishment portion of the framework, the risk assessment portion is more thorough. Another important part of context establishment is determining the scales by which impact is measured. For example, the annual profit (turnover minus expenses) of Sherbourne House is £1,000,000. Therefore, it was decided that a very high risk would be one which costed upwards of £1,000,000 as this would exceed what you would be able to pay out if necessary.

After completing these context establishing sheets, the next step in the framework is identifying risks. This involved using a risk register and the information previously gathered to create a list of risks. These can be found on the Threats and Vulnerabilities section of the risk register. It is important to be careful and methodical here, the more risks that are identified. This level of detail ensures that no threat is overlooked and that responsibility & accountability is made clear. When looking through this list you may find many risks that appear repeated. This is because it is quite common to have many assets be affected by the same threats and vulnerabilities but you must separate them into different risks. This is because while the likelihood might be the same for if they will be targeted, the impact for if they will change from asset to asset.

The next step in ISO 27005 is risk analysis, a process that combines quantitative scales & values and qualitative attributes to finish with a determination for how important a risk's treatment is. To do this, more sheets of the risk register were completed. These include assessing the impact and likelihood of each risk. Having both metrics calculated will significantly benefit the next step of the framework, risk evaluation, as each can be assigned a risk level determined via the enhanced risk matrix. A risk matrix helps to assign an easy-to-understand value to each risk, where the higher the number the greater the severity (Sutton, 2014).

Finally, risk evaluation is completed. This uses all the information previously gathered to assign both a treatment method and recommended controls to each risk. Within ISO 27005 there are four types of risk treatment, they are (BSI Standards Publication, 2011):

- Risk modification
- Risk retention
- Risk avoidance
- Risk sharing

For the purposes of this report, no risks will be retained. This means that the treatments we recommend will be either to implement a control that reduces the impact and/or the likelihood, sharing the risk in some way with a third-party or by withdrawing the process which creates the risk thus eliminating it. After this the residual risk is calculated, showing how much the risk has been mitigated via the implemented controls.

2. Top 4 Information Risks

2.1 Risk 1 – RFID Cards

The current system used by the hotel for room access, including authentication, is an access control system provided by Salto, backed up by a computer in the front desk. Although Salto is an industry recognised and reputable brand, the cards currently employed by them use MiFare Classic 1k, which is outdated compared to the most recent protocols implemented – talks were made concerning its security in as early as 2014 (Almeida, 2014). Although it can be argued that the cards discussed here are in fact information containers, they can also be referred to as an asset in their own right – whilst they contain data in the form of bytes that allows for access to be communicated, it's the package of this data with the ability to transmit it via a 13.56 MHz frequency (NXP, 2018). The vulnerabilities available through the age of this system, as well as the assumed improper training given to the staff regarding the security of the cards, means that what should be a simple outsourced access control system turns into very large attack vector for threat actors wishing to gain access to rooms all over the hotel.

If an attacker were to exploit a vulnerability that would allow to clone a staff card, this would enable them to do the most amount of damage in terms of levels of access to parts of the hotel; it can be assumed that staff cards give access to every guest room at a minimum. A likely threat actor here could be a common thief, wanting to steal from a guest – instead of having to interact with their target in any way, all they would have to do is interact with a staff key card for as little as 5 seconds (EXC3L, 2019). By taking a snapshot of the card in this way, they would be able to break its outdated encryption at their leisure, before having an almost identical copy to the staff card.

An impact of this would be the complete loss of trust in the security of the hotel by the guests, especially since the access logs used in combination with the current locks would only have recognised that a member of staff accessed the room at a particular time; this can then be disproven by camera footage, but the damage to the reputation will already have been done. As well as reimbursing the guest for the original damage of the theft, a PR team may be necessary to navigate the issues that would arise.

In terms of likelihood of this occurring, it would not be a daily risk, however as soon as a dedicated enough threat actor with slightly above average technical skills finds the issue, there will be a large risk of constant issues regarding cards being cloned or modified. This is down to this risk having larger initial difficulty to exploit due to its technical complexity. Fortunately, this problem can be remedied with relative ease and slight cost by reaching out to Salto, the current provider, or another provider if they are not willing to co-operate. The provider will be able to upgrade your current system to a modern day one, with card specifications to match; instead of an outdated MiFare classic system, a MiFare Plus system could be used - this way the original locks could be retained, but with far better card security, and peace of mind for customers.

2.2 Risk 2 – The passwords for the database being chosen by members of staff leading to a threat actor gaining access to sensitive information.

An information asset container is described as some kind of physical or digital technology that stores, transports or processes information assets (Stevens, 2005). These can range from paper and USB sticks to web servers and networks. An important container to protect is the web server which itself holds an important database containing all the booking information used from the custom-built software alongside data about running the hotel and the conference centre. This database itself is a container, storing many information assets that are critical to be kept safe and can be accessed via a web browser with the staff's ID and a password they choose themselves. This is the vulnerability that can be exploited in this risk. Without proper training or guidance, allowing people choose their own passwords will often lead to security vulnerabilities. As mentioned, every staff member has a unique set of credentials that can access the database meaning that there are 78 different passwords that can grant access (this come from the 78 staff members that work at the Sherbourne House), and as staff IDs are shown on staff cards this makes the likelihood for this risk high.

If an attacker were to exploit this vulnerability, they could access a whole range of information assets contained within the database but the asset that causes the impact to be so high is that customer's financial information. If Sherbourne House had a data breach / data leak containing financial data then there would be serious financial and reputational damage which could easily exceed both your annual profit and current savings (IT Governance, 2022). There are many types of threat actors who could exploit this threat, like criminals wanting to cause damage or steal money or a member of staff accidentally allowing the information to be accessed by the public.

The treatment for this issue is to reduce the likelihood, the easiest way is to enforce a password policy. The National Cyber Security Centre (NCSC) currently recommends selecting three random words and using that as your password. The reasoning is that the length of this passphrase will make it harder to crack over an enforced system where attackers will know that a capital letter, two symbols and a number will appear. It is also easier to remember three random words than it is to remember a password with enforced complexity (Kate R, 2021).

Another option for how to make your database more secure is to employ two-factor authentication (2FA) to access it. This is a process of confirming someone is who they say they are via what they know, what they have and what they are. The best way for Sherbourne House to implement this would be to enforce the password policy referenced before and then with it have an authentication code be sent to the staff members phone whenever they want to access the database. This can easily be done through the staff members phone and its increasingly likely that they will have come across 2FA before as more social media platforms are making it mandatory to have enabled.

Solving this risk for accessing the database will likely also help to reduce the risk level of other risks, this is because there are other risks that have different vulnerabilities but with the same threat of accessing the database. Employing these treatment methods will mean that even if the other vulnerabilities are exploited, there is another layer of defence stopping the sensitive data in the database being accessed.

2.3 Risk 3 – Physical Accessibility to networks for guests and conference room

With the inclusion of guest accessible ethernet ports that allow network access for personal devices, such as laptops, threats from inside the physical and digital network increase in probability. As the network itself isn't correctly configured to allow for different permission levels, it can cause unauthorised users to be able to access and alter material they shouldn't. Furthermore, if the staff network and guest networks aren't properly separated, there could be some cases where threat actors could hop between the two and plant malware on the staff network. Other potential problems could include physical devices implanted into the ethernet sockets that could be used to install malware onto other guest laptops.

If this were to happen, and a threat actor did exploit such a vulnerability, the network's integrity would be affected, and could cause multiple devices connected to be affected too. Any guest connected to the guest network could have their device compromised and could consequently lead to the network going down. This would be the main asset affected in such an attack. Subsequent other assets involved could be the staff network, staff machines and potentially all other devices within the hotel. A major attack sourced from one of these ethernet ports could potentially take down the whole system.

Should the Sherbourne House Hotel IT Manager decide to keep these ethernet ports available for use by hotel guests, there needs to be changes in order to reduce the risks posed by them. For example, there should be some form of privileges on the network to disallow connections from guest rooms to be able to upload files. There could also be an anti-virus installed onto the network to scan for any potential threats. Physical anti-malware boxes could be installed onto the network in order to scan all ports for suspicious activity. These boxes would be able to mitigate a lot of the threats involved when considering how threat actors could use these ethernet ports to their advantage. Potential places to acquire these boxes include network-box.com. Network-box.com remotely manages these boxes, including the repair and replacement of said boxes, (Network Box Corporation, 2021).

In terms of an easier and quicker solution, the IT Manager could decide to remove ethernet port functionality within the guest rooms, completely removing this as a potential risk. This would affect the overall guest experience but would be best in terms of risk reduction.

Looking at the conference room laptop access available to guests, this risk can be mitigated in a similar way to the ethernet ports. You could have an employee scan the chosen USB device or have an anti-virus installed on the machine. Furthermore, you could include restrictions upon the guest machine so that any requests coming from it that are not considered normal are blocked. Similar controls should be in place comparable to mitigating the threats posed by the ethernet ports.

Overall, when considering the effects of mitigating the risks these assets pose, it is important also to think about the knock-on effect securing physical guest access points will have on other potential risks. There is a lot of risk involved with implementing such functionality, especially when no controls are in place to stop any unintended guest activity.

2.4 Risk 4 – Wi-Fi being encrypted with WPA

The hotel has two Wi-Fi networks in use, the "Hotel Guest WiFi" and the "Conference WiFi". Both wireless access points are directly connected to the wired network, and they are encrypted with WPA. WPA stands for "Wi-Fi Protected Access" which is a wireless security protocol released in 2003. Currently in 2022, WPA is greatly deprecated and since its release it has been superseded by WPA2 in 2004 and more recently by WPA3 in 2018. Using such an old security protocol poses many a risk to the hotel's network as attacks on Wi-Fi networks have gotten more sophisticated over the years since 2003.

A major attack on the WPA security protocol is KRACK, or the "Key Reinstallation Attack". This attack was discovered in 2016 and it affects WPA and WPA2 Wi-Fi connections. The vulnerability stands in the WPA keys which ensure encrypted connectivity between the client and the access point. The hotel uses Windows Server 2012 R12, which is an out-of-date operating system that is vulnerable to such an attack. (IEEE Computer Society, 2004; Vanhoef & Piessens, 2017)

The staff might use Linux, Android, iOS or macOS which are the most vulnerable as they have the largest attack surface. If these operating systems are out of date and they are connected to the hotel's access point, they have from four to six points of access for this vulnerability. For Windows machines, version 10, or Server, they have a smaller attack surface, with only one point of attack, but they are just as vulnerable. A threat actor would be more inclined to attack the server with one attack point, which hosts crucial information, rather than a staff's smartphone with five attack points, which may not hold any data of value.

This vulnerability threatens the safety of the hotel's network traffic as a man-in-the-middle can intercept packets passively, just by posing as the wireless access point. Threat actors could be interested in the speakers at the conferences that the hotel is hosting, trying to intercept their packets to see their network traffic - emails, user credentials, bank details, etcetera. Worse, a threat actor could inject malware into the packets or modify their contents to their choosing, as they are unencrypted. This type of threat could be very visible if a threat actor has the right equipment. The equipment is not sophisticated, it is just an Android smartphone. When the Wi-Fi connections are listed, the Android menu displays their method of encryption. A threat actor could see that the Wi-Fi network is encrypted with WPA and be compelled to launch a KRACK attack, so the threat is likely to occur. (Vanhoef & Piessens, 2017)

This threat could, not only prove devastating for other businesses, divulging potential secrets of organisations, but it would hurt the reputation of the hotel, therefore losing its revenue, and potentially having to lay off staff, meaning that its impact is high.

Fortunately, most access points since 2005-2006 have WPA2 as an option, however this method of encryption is vulnerable too. The hotel would need to upgrade its access points to WPA3 compliant ones, but this method may be costly. A more cost-effective method would be to set the points to WPA2, if they have the option, and disable an option in the access point called the "EAPOL-Key". This ensures that that they cannot re-send handshakes, but it comes at the cost of poor connectivity. The most cost-effective method is to update all the machines to their latest version of their respective operating systems. The Windows Server 2012 R12 operating system must be updated, preferably to the latest version, or better yet, upgraded to Windows Server 2022. The staff machines must be updated to the latest version of Windows 10. The hotel must recommend that staff update their operating systems on their devices, be it smartphones or computers, to ensure security of their network traffic. (IEEE Computer Society, 2004; Microsoft, 2017; Vanhoef & Piessens, 2017)

3. Conclusion

By implementing the controls to fix these issues, Sherbourne House will significantly increase the overall physical and technological security of its systems. These treatment methods are not significantly high cost nor do they require hours of maintenance to bring into fruition but they are efficient and effective in reducing the risk level of the identified risks.

4. Bibliography

Almeida, M., 2014. *Hacking Mifare Classic Cards.* San Paulo: black hat.

BSI Standards Publication, 2011. *BS ISO/IEC 27005:2011.* s.l.:s.n.

EXC3L, 2019. *Cracking Mifare Classic cards with Proxmark3 RDV4.* [Online]
Available at: https://medium.com/exc3l/cracking-mifare-classic-cards-with-proxmark3-e42121cd968b
[Accessed 11 5 2022].

IEEE Computer Society, 2004. *802.11i.* [Online]
Available at: https://paginas.fe.up.pt/~jaime/0506/SSR/802.11i-2004.pdf
[Accessed 11 May 2022].

IT Governance, 2022. *GDPR Fines.* [Online]
Available at: https://www.itgovernance.co.uk/dpa-and-gdpr-penalties#:~:text=The%20UK%20GDPR%20and%20DPA,whichever%20is%20greater%20%E2%80%93%20for%20infringements.
[Accessed 06 05 2022].

Kate R, 2021. *The logic behind three random words.* [Online]
Available at: https://www.ncsc.gov.uk/blog-post/the-logic-behind-three-random-words
[Accessed 07 05 2022].

Microsoft, 2017. *Windows Wireless WPA Group Key Reinstallation Vulnerability.* [Online]
Available at: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-13080
[Accessed 11 May 2022].

Network Box Corporation, 2021. *About Us | NETWORK BOX.* [Online]
Available at: http://response.network-box.com/about-us
[Accessed 12 May 2022].

NXP, 2018. *MF1S50YYX_V1 MIFARE Classic EV1 1K - Mainstream contactless smart card.* [Online]
Available at: https://www.nxp.com/docs/en/data-sheet/MF1S50YYX_V1.pdf
[Accessed 11 5 2022].

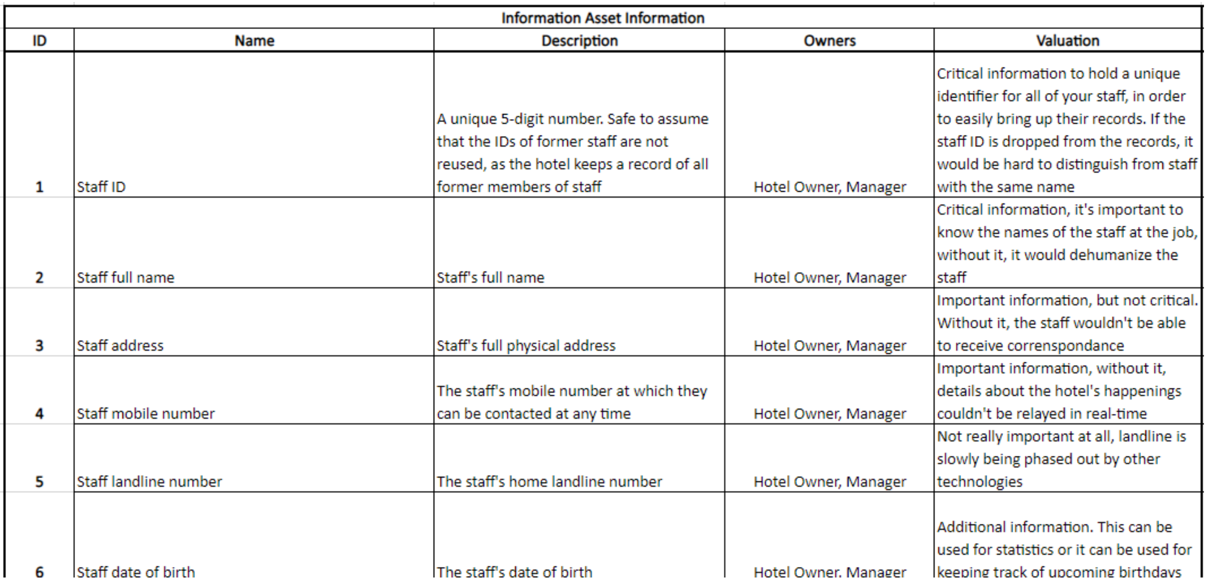
Stevens, J. F., 2005. IAP and Information Security. In: *Information Asset Profiling.* s.l.:s.n., pp. 4-7.

Sutton, D., 2014. Risk Analysis And Risk Evaluation. In: *Information Risk Management: A practicioner's guide.* s.l.:BCS Learning & Development Limited, pp. 71-72.

Vanhoef, M. & Piessens, F., 2017. *Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2.* [Online]
Available at: https://dl.acm.org/doi/pdf/10.1145/3133956.3134027
[Accessed 11 May 2022].

5. Appendix

Appendix A: An excerpt from the Information Asset Profile.



Information Asset Information				
ID	**Name**	**Description**	**Owners**	**Valuation**
1	Staff ID	A unique 5-digit number. Safe to assume that the IDs of former staff are not reused, as the hotel keeps a record of all former members of staff	Hotel Owner, Manager	Critical information to hold a unique identifier for all of your staff, in order to easily bring up their records. If the staff ID is dropped from the records, it would be hard to distinguish from staff with the same name
2	Staff full name	Staff's full name	Hotel Owner, Manager	Critical information, it's important to know the names of the staff at the job, without it, it would dehumanize the staff
3	Staff address	Staff's full physical address	Hotel Owner, Manager	Important information, but not critical. Without it, the staff wouldn't be able to receive cornrespondance
4	Staff mobile number	The staff's mobile number at which they can be contacted at any time	Hotel Owner, Manager	Important information, without it, details about the hotel's happenings couldn't be relayed in real-time
5	Staff landline number	The staff's home landline number	Hotel Owner, Manager	Not really important at all, landline is slowly being phased out by other technologies
6	Staff date of birth	The staff's date of birth	Hotel Owner, Manager	Additional information. This can be used for statistics or it can be used for keeping track of upcoming birthdays

Appendix B: Assumptions

Assumption 1: The "all data is stored in a MySQL 7 Database" is referring to the data used from the custom-built software used for booking and running the hotel. Although the "all data" is vague, coming just after new information about software it made sense to be connected.

Assumption 2: There is no password policy, we have assumed this as it was mentioned in the technical issues section of the case study and because there are many other security flaws that would make having a password policy unlikely.