Assignment Guidance and Front Sheet

This sheet is to be populated by the Module Tutor, checked by the Programme Team, and uploaded toMoodle for students to fill in their ID and submit with their assessment.

2039563, 2143557, 2153487, 2136249	**Student fill in own ID and attach document for submission**

Module Title & Code	*WM142 – Information Risk Management*
Module Owner	*Peter Norris*
Module Tutor	*Alexandra Samantha Driscoll*
Module Marker	*Alexandra Samantha Driscoll*
Assessment type	*Essay*
Date Set	*Wednesday 2nd March 2022*
Submission Date (excluding extensions)	*Friday 13th May 2022*
Marks return date (excluding extensions)	*Tuesday 14th June 2022*
Weighting of mark	*70%.*

Assessment Detail	*Please see below*
Additional details	*The wordcount is 3,000 words.*
Module learning outcomes (numbered)	*– Apply a relevant risk management approach to agiven organisation or scenario*
Learning outcomes assessed in this assessment(numbered)	*– Apply a relevant risk management approach to a given organisation or scenario*
Marking guidelines	

Task	**Mark**
1: Choose an appropriate methodology for performing information risk assessment and briefly explain and justify how you applied your chosen methodology. You should include examples of what you did in the appendix.	10
2: Identify the most relevant information risks and complete a risk register.	20
3: Select and explain the top four risks from your risk register (discuss the threat actors, threat, vulnerability, impact, and likelihood) and recommend ways to treat them.	40
4: Create a presentation for the owner and managers of Sherbourne House. explaining the top four risks and the recommended treatments.	20
5: Provide a variety of references from a variety of sources, including academic sources to support the key arguments within the report.	5
6: The assignment is formatted appropriately. Marks will also be awarded for presentation, including spelling and grammar	5
TOTAL:	100

	Please see below for a more detailed marking scheme
Submission guidance	*All work must be submitted to Tabula, please see below for more details.*
Academic Guidance	*Academic guidance to be provide throughout the module.*
Resubmission details	The University policy is that students should be given the opportunity to remedy any failure at the earliest opportunity. What that "earliest opportunity" means in terms of timing and other arrangements is different depending on Programme(i.e. Undergraduate, Full Time Masters, Part Time Postgraduate, or Overseas). Students are advised toconsult your Programme Team or intranet for clarity.
Late submission details	If work is submitted late, penalties will be applied at the rate of **5 marks per University working day** afterthe due date, up to a **maximum of 10 working days** late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). "Late"means **after the submission deadline time as well as the date** – work submitted after the given time even on the same day is counted as 1 day late.

Assessment

Introduction

During this module you have been learning how to identify information risks and treat them. Usually, information risk management is conducted within teams. To replicate this you will be asked to work in groups. This will give you an opportunity to gain experience with working in groups, which is a vital skill for both information risk management and cyber security.

Information risk management will involve consultation with members of the organisation, many of which may have little knowledge of information security. Information risk management practitioners do not decide which risk controls to implement, but make recommendations to senior management, who will make the final decision. Those in senior management are often busy, with little spare time and may not have a full understanding of information security. Because of this it is vital that as information risk management practitioners we can communicate effectively with others.

In this assignment you will be asked to conduct an information risk assessment at a hotel and conference centre. Once you have completed the risk assessment process, you will write a report outlining the top four risks along with recommended treatments aimed at the owner. No risks may be ignored or accepted.

Finally, you will create a presentation explaining the top four risks, along with recommended treatments for the owner of Sherbourne House and its managers. This presentation will be ten minutes and you will be expected to present it and answer questions at a viva.

The case study for this assignment can be found at the end of this document. The case study is large and contains a significant number of information assets and potential risks. Information risk practitioners will never be able to identify every single risk.

You are not expected to identify every possible risk from the case study. Focus on identifying the most relevant risks. You should aim to identify at least twenty risks.

Tasks

You must complete the following tasks.

1. Choose an appropriate methodology for performing information risk assessment and briefly explain and justify how you applied your chosen methodology. You should discuss examples of how you used this methodology. Any examples should be placed in the appendix.
2. Identify the most relevant information risks and complete a risk register.
   - You should aim to identify at least twenty risks.
3. Create a report aimed at the owner. You should discuss the top four information risks (discuss the threat actors, threat, vulnerability, impact, and likelihood) and recommend ways to treat them
   - If your group only has three members, then pick the top three risks
4. Create a presentation to explain the top four risks and their treatments to the owner and managers of Sherbourne House.
   - The top risks and treatments should be the same as the ones in task 3
   - The presentation should be around ten minutes
   - The presentation should be appropriate for the owner and managers, who may have little knowledge about information security
   - You will be expected to present your presentation at a viva
   - During the viva you will be expected to answer questions
   - Attendance at the viva is mandatory for all group members
   - Once you have submitted your assignment you are not allowed to modify your presentation

Deliverables

Your final submission will consist of a report of up to 3,000 words (excluding references, tables, and appendices). The risk register and presentation does not count towards the word count. Any submissions beyond 3,300 words will attract a penalty of 10%. The report should contain:

1. A table of contents
2. An introduction
3. A section explaining your chosen methodology
4. A section containing the report aimed at the owner discussing of the top four risks and any recommended risk treatments.
   a. The report should be an appropriate document aimed at management, for example a board paper
5. A conclusion
6. A reference section
7. Any appendices

As well as the report you should also submit the following:

1. A copy of your risk register
2. A copy of your presentation slides
3. A folder containing any other files you may have created

Submission

You should submit the following to Tabula:

1. Your report, which should be called IRM_Assignment2_Report_Group[X].pdf
2. Your risk register which should be called IRM_Assignment2_RiskRegister_Group[x].xlxs
3. Your presentation which should be called IRM_Assignment2_Presentation[X].pptx
4. A folder containing any additional files called IRM_Assignment2_AdditionalFiles_Group[x]

Replace [X] with your group number. For example: IRM_Assignment2_Report_Group[1].pdf

All students must upload an identical copy of the assignment

Important Notes

1. No identified risks can be ignored or accepted
2. You must use the Harvard referencing system.
3. The report must be submitted as a pdf
4. Your risk register should be a spreadsheet
5. Your presentation slides should be submitted as a PowerPoint file.
6. All work should be done and saved in your assignment group on Microsoft Teams
7. Late submission penalties will apply
8. This is a group assignment
    - All members are expected to submit identical copies of the assignment
9. Group members are responsible for ensuring all members participate
    - If there are issues that cannot be resolved, then Alexandra will deal with them. However, students will have been expected to make reasonable attempts to resolve any issues
    - Any student not sufficiently participating will have their assignment mark capped at 40%
    - Any students who do not contribute to the assignment may not pass.
    - Any student who does not allow others to contribute may also be penalised
10. The assignment is due Friday 13th May 2022
11. All group members must attend a viva in the third semester
12. The dates and times will be announced nearer the
13. Contact Alexandra Driscoll if you have any questions: alexandra.s.driscoll@warwick.ac.uk
14. Your group may be required to attend a viva in the third semester

Marking Scheme

The following marking scheme will be used. The assignment has a total of 100 marks.

Task	Criteria	Mark
1: Choose an appropriate methodology for performing information risk assessment and briefly explain and justify how you applied your chosen methodology. You should include examples of what you did in the appendix.	1a: An appropriate methodology was chosen	5
	1b: Explanation and justification for chosen methodology, which included a discussion of examples	5
2: Identify the most relevant information risks and complete a risk register.	2a: Appropriate information risks identified	10
	2b: An appropriate risk register is created	10
3: Select and explain the top four risks from your risk register (discuss the threat actors, threat, vulnerability, impact, and likelihood) and recommend ways to treat them.	3a: Top four risks identified	4
	3b: Components of top four risks discussed	16
	3c: Potential risk treatments for each risk identified	4
	3d: Potential risk treatments discussed and compared	16
4: Create a presentation for the owner and managers of Sherbourne House. explaining the top four risks and the recommended treatments.	4a: Presentation explains the top four risks and their treatments	8
	4b: Presentation slides are appropriately formatted, and the presentation is appropriate for the owner and managers of Sherbourne house.	12
5: Provide a variety of references from a variety of sources, including academic sources to support the key arguments within the report.	5a: Sources included	1
	5b: Academic sources included	1
	5c: Sources referenced correctly using the Harvard referencing system	3
6: The assignment is formatted appropriately. Marks will also be awarded for presentation, including spelling and grammar	6a: Report in an appropriate style and correct file formats used	1
	6b: Spelling and grammar	2
	6c: Appropriate formatting, including tables and figures appropriately labelled and cited within the document text	2

WM142 – Information Risk Management

Sherbourne House Hotel and Conference Centre

Information Risk Assessment

Table of Contents

1.0 Introduction 4

1.1 Purpose of this Report 4

1.2 Framework 4

1.3 Top Four Risks 5

2.0 Fraudulent Emails 5

2.1 Identification of the Risk 5

2.2 Protection and Prevention 6

2.3 Detection 6

2.4 Response 6

2.5 Recovery 6

3.0 Poor Password Management 7

3.1 Identification of the Risk 7

3.2 Protection and Prevention 7

3.3 Detection 8

3.4 Response 8

3.5 Recovery 8

4.0 RFID Cloning 8

4.1 Identification of Risk 8

4.2 Protection and Prevention 9

4.3 Detection 9

4.4 Response 9

4.5 Recovery 10

5.0 Guests Directly Connecting to Internal Network via Ethernet 10

5.1 Identification of the Risk 10

5.2 Protection and Prevention 11

5.3 Detection 11

5.4 Response 11

5.5 Recovery 12

6.0 Conclusion 12

7.0 Bibliography 12

Table of Figures

Table 1 *- Top Four Risks*........ 5

Figure 1 *- Risk Assessment within the Risk Management Process (NIST, 2012)*........ 4

1.0 Introduction

1.1 Purpose of this Report

The purpose of this report is to highlight the top four information risks associated with Sherbourne House Hotel and Conference Centre. After careful evaluation of the organisation and its infrastructure, we have compiled a report that examines each risk, the steps that should be taken to prevent them, and what should be done to recover from any financial, social or environmental consequences if a threat occurs.

1.2 Framework

We have chosen to incorporate the NIST Cybersecurity framework into the risk assessment for Sherbourne House. There are five key functions that form the NIST methodology lifecycle: Identify, Protect, Detect, Respond and Recover. Since many of the potential risks involve the hotel's IT systems, an approach that focuses on mitigating information security risks would protect the business' interests. Data is collected from individuals in the organisation, which is then used to analyse future risks. This is very useful as it ensures threats can be prevented before they occur. (NIST, 2012)

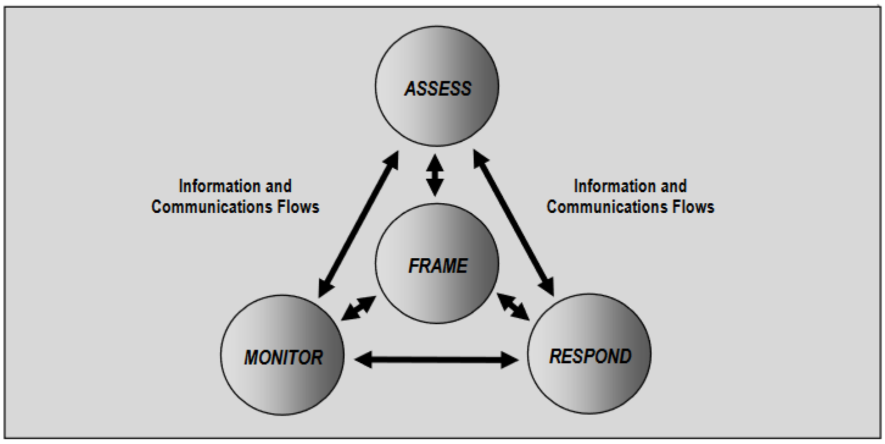
ASSESS
Information and Communications Flows
Information and Communications Flows
FRAME
MONITOR
RESPOND

Figure 1 *- Risk Assessment within the Risk Management Process (NIST, 2012)*

1.3 Top Four Risks

Reference	Brief Description of Risk	Inherent Risk		
		Impact	Likelihood	Risk Level
7	A staff member unintentionally gives away their credentials due to phishing	High	Possible	18
17	The same password being used on all E-Mail accounts could lead to a breach.	High	Likely	20
14	Malicious threat actor figures out RFID technology and access to other rooms	High	Possible	18
19	Guests connecting directly to the internal network via the Ethernet port in their room could lead to exposure of sensitive information	High	Possible	18

Table 1 *- Top Four Risks*

2.0 Fraudulent Emails

2.1 Identification of the Risk

A common risk that affects every organisation is the threat of phishing emails. Over three billion are sent every day and account for 90% of data breaches. Often, these scams will be sent in mass quantities and can install malicious software (Wise, 2022). Sherbourne House should expect to receive a considerable amount of phishing emails, most of which will be filtered as ‘spam’.

Typically, these emails will be sent indiscriminately to many addresses, rather than targeting a specific organisation, in the hopes that a few unaware individuals might give up sensitive information.

Most of the time these attacks will be random, however there is a very low chance that a spear-phishing attack might occur - an email might be fabricated to specifically target a known organisation. An example of this attack notoriously occurred in March 2017, where two large, unknown companies based in the USA lost £100 million due to a fraudulent email (DOJ, 2017).

2.2 Protection and Prevention

Training employee awareness of this threat is essential to ensure no private information, or any details relating to Sherbourne House, is given away. Regular meetings should be held to educate staff on spotting fake emails and how to respond if they do. By default, many of these emails will be sent straight to the 'Spam' folder. However, should any emails make it past this filter, they should be reported to the IT Manager. If an employee believes that the email is an example of 'spear-phishing', they must make the IT Manager aware of this since it implies that a threat actor is targeting Sherbourne House specifically.

Phishing tests are another great way to find out how many employees might fall for a fraudulent email. This should be performed after the appropriate training has taken place and the names of employees who did fall for one should not be disclosed. Senior staff should not be exempt from these tests, especially since their login credentials could allow an attacker to access more privileged information (Dashlane, 2020). Regular tests should be performed ensure employees know what to do if they receive a spear-phishing email, since these could cause far more devastating consequences to the Hotel than the regular spam emails.

2.3 Detection

Driscoll Webhosting should ensure that the appropriate spam filters are in place on Sherbourne House's mail server. While this is not always 100% effective, the vast majority of phishing emails will be blocked.

A targeted email might prompt the recipient to send over login information. For example, the threat actor might pretend to be a member of management requesting a staff member to 'remind' them of the password. This is especially dangerous as the employee is more likely to believe the email is genuine. Staff should be informed that they will never be asked to give login information over email and if they receive an email asking them to do so, they should report it immediately.

2.4 Response

In the event that an employee has given away their login details, it is vital that all members of staff, management included, immediately change their passwords. The IT manager should also keep track of recent logins and check to make sure no unauthorised devices are accessing the Hotel's local network. If it seems that someone is attempting to login using stolen credentials, that IP address should be blocked from the network immediately.

2.5 Recovery

If an unauthorised user has gained access to Sherbourne House's network, and therefore the database, the personal information of all guests and staff members would be compromised. In this case, the GDPR requires that all guests be notified within 72 hours after the data breach is found (GDPR, 2017). This notification should warn guests and staff to change their bank details as well as any consequences as a result of the breach.

3.0 Poor Password Management

3.1 Identification of the Risk

As detailed in the report, staff in the company have their own unique user credentials. These credentials consist of their staff ID, and a password picked by the member of staff themselves. There are no enforced password rules in the report, despite passwords (or credentials) being one of the primary targets of cyber-attacks, especially for those in which threat actors intend to maintain persistence on the systems.

As outlined above, Sherbourne House will receive a landslide amount of phishing e-mails across all its staff. These are generally sent with the goal of harvesting user credentials, as stated in Microsoft's 2020 Digital Defense report.

Sherbourne House does not enforce password rules and treats WiFi passwords, conference room credentials and even the company's website credentials with little to no importance. Because of this, they are highly susceptible to persistent attacks, where attackers can 'live off the land' and be immensely difficult to track down as they are using valid credentials to pivot and traverse the network. (Spitzner, 2021)

3.2 Protection and Prevention

Employees should follow, at a bare minimum, a verifiably robust password policy, which should include a minimum length of at least 10 characters (it has been proven that password length beats complexity (Spitzner, 2021)), a mix of alphanumeric characters in both upper- and lowercase, and at least one number.

Moreover, the company should emphasise and train the importance of every single account (work and personal) having a unique password for that account. Therefore, if one account is compromised, all other accounts are still secure. Password managers are a fantastic solution to this problem, as one password is equivalent to a large number of unique passwords kept under lock in a password manager.

Finally, the company should introduce MFA (Multi-Factor Authentication) to whatever services are possible; most importantly the crucial services that the company requires, like logging into the admin account on the website. (Spitzner, 2021)

WiFi passwords and the conference room credentials should be changed regularly to keep these systems secure from threat actors logging on with old credentials.

3.3 Detection

Granular logging of all activity on accounts on the system will make IT staff aware of rogue accounts on the network, which is an obvious symptom of a password breach.

On top of this, encouraging employees to test their passwords against website such as haveibeenpwned.com (which shows you if your password has been found in any password breaches) can keep them informed of how secure their password is.

If employees fall victim to a phishing attack or become aware their password has been breached, they should be strongly encouraged to come forward so that the IT staff can review the logs of their company account and detect any malicious activity on the network.

3.4 Response

If an employee's password has been found in a breach, the account should be immediately flagged for log review. Provided there has been no malicious activity on the account since the breach, the password should be immediately changed.

If malicious activity has been found on the account, other measures should be taken into consideration, dependant on what the threat actor has done on the account. The password should always be immediately changed, and any alternative forms of persistence should be surveyed for before responsive actions are taken on the activity.

3.5 Recovery

Once the response has finished, the account has been secured and activity on the account logged and responded to as necessary, an audit should be carried out into how the password was breached, whether by phishing scam or a simple brute-force attack.

How the account was breached can infer a lot of information about potential vulnerabilities on the system, and if an audit is not carried out it is very likely to re-occur on either the same or another account.

4.0 RFID Cloning

4.1 Identification of Risk

Both guests and staff members are assigned with key cards that use 'MiFare Classic 1K' RFID technology to lock and unlock rooms. While these cards are programmed to only allow access to particular rooms, depending on the user, they can easily be cloned or reprogrammed by a malicious threat actor to gain access to a room. The most likely threat is the committing of theft, however in less likely but far more serious cases, the safety and lives of the guests and staff themselves might be at risk.

The threat actor could potentially be a member of staff or a former guest who cloned their card during their stay. By using widely available software, the actor could reprogram the RFID chip and modify the details stored on it, such as the staff name and ID number (staff card) or the room number that the card accesses (guest card).

4.2 Protection and Prevention

The cards are extremely vulnerable to this exploit, and it is possible that this might be a regular occurrence, since RFID cloning devices are very easy and inexpensive to obtain. The most effective protection method would be to use encoding software for the access control system. This would allow the creation of encryption keys to encode the credentials stored on the RFID chip, which would prevent the cards from being read by unauthorised readers while still being read by the hotel's door locks **Invalid source specified.**.

However, if the threat actor was working with an employee, or is an employee themself, they could have insider knowledge about the encoding software being used. To counter this, the encoding software should be strictly inaccessible to any employee besides the IT manager. The password to use the software should be updated regularly and two-factor authentication methods should be in place for added security.

It is also recommended that 24/7 security guards are employed. If the threat actor enters the premise with a cloned key card, they pose a very serious threat to guests and staff. While this does not prevent an individual from cloning a card, it will certainly reduce the likelihood of a crime being committed as a result.

4.3 Detection

When a door is locked or unlocked, a log is kept and stored on the hotel's database. It is recommended that these logs are checked for unusual patterns, such as a door being unlocked at considerably late hours, as this could imply a break-in. Although some guests perhaps might be out late at night, it is much more likely that a crime would be committed during these hours.

Cameras should be installed on the door itself and connected to the hotel's network, as this will allow a clear image of the threat actor if they attempt to access a room, which regular CCTV cameras might not accomplish.

4.4 Response

If it is believed that a room has been accessed using a cloned key card, the door cameras should be able to get a clear image of the individual attempting to get in. This footage can then be relayed to the authorities so they can identify the suspect. This might not always work, since the threat actor could be aware of the camera and obscure their face. However, the on-site security guards will be wary of anyone attempting to hide their identity from cameras.

When the door lock detects a card that does not have the correct permissions to unlock or lock it, the hotel manager should be notified. This way, they can inspect the relevant CCTV footage and discover whether the individual is a malicious actor or perhaps just a guest or staff member who accidently tried an incorrect door.

4.5 Recovery

In the unlikely event that an individual has gained access to a guest's room, it is very likely that property belonging to the guest, such as laptops or money, would be stolen. According to the travel insurance of the guest victim, Sherbourne Hotel's liability insurance and its terms and conditions, the appropriate amount of compensation should be issued to the guest or their next of kin. It is very likely that there will be a significant amount of negative publicity in this event, so the hotel must be prepared to make amends.

5.0 Guests Directly Connecting to Internal Network via Ethernet

5.1 Identification of the Risk

Within every hotel room there is an Ethernet port put in place for the guest to connect to the internet via the internal hotel network. While the IT administrator believes that this this is not a threat due to the presence of the guest WiFi. A threat actor would have direct access to the internal network.

As noted in the case study, this is a massive risk to the organisation's security. If a threat actor had an immediate and uncontrolled connection to the internal network, they would be able to bypass all network perimeter defences and have direct access to all internal resources – notably, the database and booking systems. From here, a wide array of consequences could be presented. Sensitive data could be breached, system downtime could occur, and the safety of guests and staff could be put at risk.

5.2 Protection and Prevention

The hotel should employ a much better network security implementation in order to deal with this risk. To begin with, it is recommended that the organisation deploy a specific switch that would create a wired Virtual Local Area Network (VLAN) to compartmentalize the guest network from the internal network.

Whilst it is a more extreme option than segmenting the wired network, the hotel can take steps to completely remove any Ethernet ports from all guest rooms within the hotel in order to restrict guest access to the internal network and ultimately limit Ethernet connections to the staff only. This would force guests to use the guest WiFi, which can then be monitored/filtered and would not provide access to the internal network.

It is also recommended that the hotel deploy a firewall of their choosing on the network in order to further filter traffic between destinations on the internet and the LAN. This would give the organisation granular control over connections and would allow the IT team to decide what hosts have access to specific resources.

5.3 Detection

Logging of all network and system activity within both the network traffic and internal hosts would make the IT team aware of any malicious or unintended activity within the network.

If a targeted attack by a threat actor was to occur, the IT team could also deploy heaving logging into each specific user's activity on the network. This could be done via an Intrusion Detection System (IDS) and would monitor network traffic for suspicious activity and alert the IT team when such activity is detected.

5.4 Response

If a threat actor has been detected to be exploiting the fact that Ethernet connections connect to the internet via the internal network, the first action taken should be to immediately disconnect the said host from the internet in order to discontinue any connections to internal resources.

If the IT team has sufficient logging, they should be able to see which Ethernet port is being used, and in which specific room. This would allow them to identify the guest responsible for the abuse and remove them from the hotel, followed by a report to the relevant authorities.

5.5 Recovery

If an unauthorised user or threat actor manages to access internal resources, it is very likely that personally identifiable information is in turn breached. This would require the hotel to report a personal data breach to the relevant supervisory authority. The hotel may also want to alert the relevant customers affected by the breach as a courtesy and may have to pay compensation out. Finally, the hotel may want to release a public statement addressing the breach and discuss methods of improving their security in order to improve relations and create transparency.

6.0 Conclusion

From this report, the most significant risks posed towards Sherbourne House Hotel and Conference Centre have been highlighted. Any vulnerabilities found in the hotel's infrastructure have been rectified and the potential threats, which might have occurred had these flaws been left unchecked, mitigated. The possible actors who might exploit these vulnerabilities have been suggested as well as the likelihood of the threat, and the impact it might have on the organisation. For each risk, recommended control strategies have been discussed to minimise these threats and also to reduce, and recover from, the effects of any consequences should the threats still occur.

7.0 Bibliography

Dashlane, 2020. *How to Run an Effective Phishing Test at Work.* [Online] Available at: https://blog.dashlane.com/phishing-test/

DOJ, 2017. *Lithuanian Man Arrested For Theft Of Over $100 Million In Fraudulent Email Compromise Scheme Against Multinational Internet Companies.* [Online] Available at: https://www.justice.gov/usao-sdny/pr/lithuanian-man-arrested-theft-over-100-million-fraudulent-email-compromise-scheme

GDPR, 2017. *Guidelines on Personal data breach notification under Regulation 2016/679.* s.l.:s.n.

NIST, 2012. *Guide for Conducting Risk Assessments.* [Online] Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Spitzner, L., 2021. *Strong, Secure Passwords Are Key to Helping Reduce Risk to Your Organization.* [Online]
Available at: https://www.sans.org/blog/strong-secure-passwords-are-key-to-helping-reduce-risk-to-your-organization/
[Accessed May 2021].

Wise, J., 2022. *How Many Phishing Emails Are Sent Daily in 2022? 11+ Statistics.* [Online] Available at: https://earthweb.com/how-many-phishing-emails-are-sent-daily/