University of York

Department of Computer Science

A Risk Assessment for RoboDoc - an organisation using Autonomous Robotic Surgery

With a description of legal, regulatory and technical issues for consideration

Word Count: 2998

26th June 2023

Abstract

This document constitutes a risk assessment for RoboDoc which uses Autonomous Robotic Surgery (ARS)[1]. It also describes legal, regulatory and technical issues that RoboDoc should consider.

Contents

1 Risk Management Plan

This cyber-security risk management plan conforms to standard BS EN ISO/IEC27001[2]. Standard BS7799-3[3] has also been used as a guide. ISO/IEC27001 has been selected because it is the UK implementation of the international information security standard EN ISO/IEC27001:2017 [2] and RoboDoc will be based in the UK.

1.1 Organisation and context

Clause 4 in standard ISO/IEC27001 refers to ISO31000:2009 which stipulates that objectives, external and internal parameters should be explained[4]. This section therefore deals with clause 4 of ISO/IEC27001 as well as clause 6 of BS7799-3 - specifically the context of RoboDoc and its interested parties[2][3]. It also describes potential consequences of not securing internal and external parameters as required by section 6.1.2 d) in ISO/ISEC27001[2].

The objective for RoboDoc is to use technology based on the Autonomous Robotic Surgery (ARS) project[1] to conduct surgeries on patients. It will adhere to UK laws and regulations, consult with patients and discuss their medical needs before surgery.

Data that will need to be stored and/or processed:

External:

1. Patient credentials.
2. Medical records.
3. Records of consultations.
4. Payments for procedures.

Internal:

1. Employee credentials.
2. Payroll information.
3. General company data e.g. software for surgery; financial data; policies and reports.

Interested parties would be patients, employees and RoboDoc's shareholders.

Crucially, if the ARS system was compromised, very serious consequences would result with the potential for great harm to patients and the reputation of RoboDoc.

1.2 Risk Assessment

This section deals with ISO/ISEC27001 6.1.2 a) - establishing the risk acceptance criteria; 6.1.2 c) - Identifying security risks; and 6.1.2 d) - analysis to determine level of risk[2].

Standard Fusion describe typical threats to an organisation[5]. These are shown here along with associated vulnerabilities[6]:

1. Adversarial from outsiders:
    - Attacks against browsers.
    - Attacks against and from web-sites.
    - Attacks through email.
    - Threats in networks.
    - Threats in Wireless networks.
    - Denial of service and distributed denial of service.
    - A false positive authentication via off-site services.
2. Adversarial from insiders:
    - Machines left logged in and unattended.
    - False positive authentication.
3. Erroneous actions performed by users (including doctors):

- Succumbing to fraudulent emails.
- Incorrect data entry.
- Accidental deletion.
- Unsafe browsing.

4. Erroneous actions performed by system administrators: As above with the addition of incorrect privilege assigned to users.
5. Equipment failure.
6. Software errors. This would include errors in software for the ARS system.
7. Natural disasters and other situations resulting in the loss of all hardware.

The OWASP risk rating methodology has been used to evaluate risk[7]. This methodology starts with the standard risk model:

$$\text{Risk} = \text{Likelihood x Impact}$$

However, for risk levels, it takes a more fluid approach arriving at descriptions of risk that are note; low; medium; high; and critical[7]. This will also be the approach taken here.

Using the OWASP groupings for likelihood and impact scenarios, each vulnerability is considered[7]. Under technical implications, the key cyber-security issues of Confidentiality, Integrity and Availability are introduced. These issues, as Pfleeger et al. explain, have been the fundamental principles of computer security even as far back as 1972[6]. However, the

OWASP methodology states that business impact should take precedence over technical impact[7]. Therefore, business impact has been used to evaluate risk.

Risk levels for each vulnerability have been summarised in table 1.1. Detailed calculations can be found in appendix A and definitions for scores in appendix B. The OWASP model states that precision is not a requirement in determining values so figures in appendix A are estimates[7]. These estimates are used to determine the level of risk using the phrases previously described[7].

Vulnerability	**Risk rating**
Attacks Against Browsers (including through un-safe browsing)	LOW
Attacks against and from web-sites	LOW
Attacks through email	LOW
Threats in networks	MEDIUM
Threats in Wireless networks	MEDIUM
Denial of service and distributed denial of service	MEDIUM
A false positive authentication (On-site or off-site)	HIGH
Machines left logged in and unattended	HIGH
Incorrect Data Entry	LOW
Accidental deletion	LOW
Incorrect privilige levels	LOW
Equipment failure	LOW
Software errors including from ARS	LOW
Loss of all hardware	MEDIUM

Table 1.1 Results from risk analysis

1.3 Risk Treatment

ISO/ISEC27001 6.1.3 a) requires the proposal of security risk treatment options[2]. This section will explain the proposed treatments and as required in ISO/ISEC27001 section 6.1.2e),

results from the risk assessment will be compared with the risk criteria to ascertain which risks require treatment and to establish priorities[2].

ISO/ISEC27001 6.1.2c) requires that owners of risks be established [2]. The responsibility for cyber-security would ultimately lie with the Chief Executive Officer (CEO), but it is expected that they would delegate responsibility to the cyber-security manager. Other individuals within RoboDoc will also have responsibilities and these are noted where relevant.

Risks with a result of 'low' or less are acceptable risks resulting in a reactive approach to dealing with them. This is a simplistic approach though and, as suggested in BS7799-3 6.4.5, other vulnerabilities will be considered under certain circumstances[3].

Low risk vulnerabilities where a reactive approach will be taken are:

1. Browser attacks
2. Email attacks
3. Attacks against and from websites
4. Incorrect data entry
5. Accidental deletion
6. Inaccurate privilege levels assigned by administrator
7. Equipment failure

Some treatments below would also help treat the above vulnerabilities anyway. For example, creating backups would help protect against loss by accidental deletion. Treatments are presented in order of priority:

1. Software errors including in the ARS System

This category has been not been identified as needing treatment from its risk assessment. Indeed, the minor disruption caused by software glitches in administrative areas can be dealt with reactively. However, the ARS system is critical to RoboDoc's operation and any problems could cause a genuine threat to life. Therefore, preventative measures are required.

It is proposed that the robots are stand-alone and should never be connected to any networks with installation of updates performed by the cyber-security manager.

If this is not possible, alternative security measures described below would help to prevent issues if the robots were on the network. However, it is much safer if they are not as a threat agent would need direct, physical access to the robots if they were not on the network. Therefore, aside from authentication, physical premises security staff would have responsibility for ensuring no access was granted.

2. False positive authentication

This was identified as high risk and is also a top priority for implementing. Pfleeger et al. describe authentication as the process of an individual proving their identity[6]. The National Cyber Security Centre outlines different authentication methods and their appropriateness to

different scenarios[8]. RoboDoc's requirements lean towards higher security over user experience. As cyber-security is critical to individual's safety in healthcare[9], FIDO2 authentication is the most appropriate choice here[8]. Users (including doctors) would be provided with an authenticator app to use on their mobile phones[8]. An alternative to this would be multi-factor authentication, but some users may not want to have additional contact information associated with their accounts[8]. The responsibility of downloading the FIDO2 app and setting up authentication will lie with users. Support from the IT team will be provided if required.

3. Machines left logged in

Although this resulted in a high value in the risk assessment, it is free and easy to implement preventative measures. Setting computers to lock automatically after one minute of inactivity will decrease the amount of time available to insiders to gain access. The best strategy though is to train staff to take responsibility and lock their machines when they are leaving them.

4. Threats in Networks

Techniques used by attackers could be wiretapping, packet sniffing, and radiation from cables themselves as well as cable splicing[6].

Encryption is a key aspect of cyber-security[6]. All sensitive data should be encrypted where it is stored, but also encryption on the network needs to be used to ensure data is protected in transit[10]. The two key modes of encryption in networks are end-to-end and link[6]. Each

mode has its merits. Link encryption is considered faster and easier to use whilst end-to-end encryption is more versatile and does not need hardware to operate[6].

With an entirely wired internal network, end-to-end encryption might be the preferred option. However, it is likely that a wireless network would be chosen. With fewer network cables in place, the transmission line is more vulnerable[11]. Protecting against vulnerabilities in the transmission line is one of the strengths of link encrytion[6]. Therefore, link encryption would be the preferred mode here.

Beyond encryption, further measures to implement are:

- Backup systems.
- Weekly port scans to check for vulnerabilities[12]. Results of these scans will be acted upon with vulnerabilities addressed.
- A firewall to filter traffic between inside and outside networks[6]. An application proxy is recommended here to ensure that applications receive only genuine requests[6].
- Network address translation to prevent intruders learning internal addresses.[6].
- A data loss prevention system to help guard against data being sent to unauthorised locations[6].
- An intrusion detection system to notify of intrusions. This should be tuneable and combine signature-based and heuristic systems to gain the advantages of both[6].

To compliment these, the option of using an Infrastructure as a Service (IaaS) cloud based system is recommended because certain security responsibilities would be passed to the cloud provider. For example, using Microsoft Azure, responsibilities for servers, networking and storage would be with Microsoft - including their security.[13].

5. Threats in Wireless Networks

The additional threat faced in wireless networks is interception of the signal by anyone within range[6]. Modern wireless networks are encrypted using WPA encryption[6]. A long and random enough key to protect against guessing attacks must be created[6].

6. Denial of service and distributed denial of service.

These attacks attempt to defeat availability[6]. Another benefit of using Azure's IaaS would be the inclusion of DDoS protection which would pass much of the responsibility for protection to Microsoft[14].

Alternatively, without this, these threats can be tackled using methods such as tuning, load balancing, shunning and blacklisting as described by Pfleeger et al.[6].

7. Loss of all hardware

This could happen due to fire, natural disaster or theft. Using IaaS, as well as benefitting other areas would also mitigate against the loss of computer hardware. It would also further

mitigate against theft as thieves would only have access to locally stored copies of data which would be encrypted as previously described.

8. Additional measures

As well as the above treatments, it is essential to keep virus protection and operating systems up to date[15].

1.4 Verification

ISO/ISEC27001 6.1.3 c) requires that controls established in the risk assessment be checked against Annex A to ensure none have been ommitted[2]. This will include listing controls and justifying their inclusion or exclusion (see ISO/ISEC27001 6.1.3 d)[2]). Figure 2 from clause 9 of BS7799-3 will be used to assist in this process[3]. The CEO will have overall responsibility for this and help to ensure that heads of other departments complete all tasks required of them under Annex A[2].

1.5 Approval

Responsibility for this will lie with the CEO. As stipulated in ISO/ISEC27001 6.1.3 f) though, approval should be sought from all risk owners[2]. BS7799-3 7.1 states that risk owners must be able to understand the results of the risk assessment[3] which will be checked by the cyber-security manager.

1.6 Operation

ISO/ISEC27001 8.2 requires that security risk assessments are carried out at planned intervals[2]. It is envisaged that these be carried out annually by the cyber-security manager. The risk assessment will also be repeated after any changes as required by ISO/ISEC27001 8.2[2].

Figures used in the risk assessment calculations are estimates. They can be improved upon over time as more information is gathered. This is a requirement of clause 10 of ISO/ISEC27001[2]. Crucially, these are starting values and, as ISO/ISEC27001 6.1.2 b) stipulates, the risk assessment must be repeatable to produce consistent results[2]. Therefore, these values can be used in each subsequent assessment and only adjusted if deemed necessary.

In accordance with ISO/ISEC27001 8.3, a physical copy of the latest risk assessment will be kept in RoboDoc's offices[2].

2 Legal and regulatory issues

Pfleeger et al. identify key legal and regulatory issues pertaining to cyber-security[6]. The issues relevant to this scenario are discussed here.

Copyright, patents and trade secrets

The ARS project is a framework for implementation[1]. The realisation of that framework in software and hardware will be carried out by RoboDoc. The software, assuming it to be original, automatically qualifies for copyright protection in the UK[16]. This copyright protection would extend to the 176 countries covered by the Berne convention[16] [17] [18]. RoboDoc will need to consider whether it wishes to have additional proof its software was created first in the event it is stolen and claimed as being written by someone else. A service such as that provided by CopyRight.co.uk would provide the facility to register the copyright[16]. However, this is not essential. RoboDoc may prefer that its software is kept as a trade secret, in which case, registering it would not be the preferred choice.

Patents for the physical autonomous robots may be required since they are physical objects and would not be protected by copyright[6]. Without a patent another organisation could

claim the design as their own leaving RoboDoc liable for costs to use their own creations!

Unlike copyright, originality does not automatically qualify a physical object for a patent[6]. As such, keeping the design of the hardware as a trade secret may not be secure enough. If the software was stolen, steps could be taken to legally defend the work[19]. If the hardware was stolen, it could be reverse engineered and there might be no legal recompense if a patent did not exist[6]. Just protecting the hardware as a trade secret would require proof of ownership which could be difficult[6].

Since the autonomous robots require software to work correctly, having a patent for the hardware would not compromise keeping the software as a trade secret. Therefore, it is recommended that the software is a trade secret and that a patent is applied for the hardware through the UK Government[20]. Legal advice on this complex process should also be sought[6].

Privacy and the General Data Protection Regulations (GDPR)

RoboDoc will need to comply with the UK Data Protection Act (2018)[21] which is the UK implementation of GDPR[22]. Key aspects of the legislation for RoboDoc to note are:

- Only personnel that need to will have access to an individual's data.
- Data processing activities must be legally justifiable and should be explained to concerned parties.
- Individuals have a right to access their personal information.
- Individuals have a right to have their data erased upon request.

RoboDoc is obliged to check that the person requesting either of the final two points above is the individual concerned in the data, and they have to comply without delay (typically one month is allowed)[23].

Without compliance to GDPR, RoboDoc could face hefty fines. Depending on the infringement, fines range from €10 million (or 2% of annual revenue) to €20 million (or 4% of annual revenue) with the larger of the two figures taken in each case[24]. Therefore, it is imperative that compliance is established.

3 Techincal issues

According to Mijwil et al.[15], the top five evolving threats in cyber-security are:

- Ransomware attacks
- Internet of Things (IoT) attacks
- Cloud attacks
- Phishing attacks
- Cryptocurrency and Blockchain Attacks

The last of these is not relevant to this scenario but the others are. With instances of Cybercrime expected to grow rapidly in the coming years[25], it is imperative that RoboDoc does all it can to guard against these attacks. It is interesting to note that, as reported by Forbes, Gartner predicts that by as early as 2025, humans will be the main line of defense against Cybercrime rather than technology[26]. RoboDoc will need to ensure it has enough personel to deal with cyber-attacks. Lessons should be learned from the ransomware attack on Newfoundland and Labrador's healthcare system in Autumn 2021[27]. A key reason the

attack was successful was the small number of IT security staff[27]. A further human factor to consider is training. All staff need to be trained to use secure passwords and not fall for phishing scams[15]. This will help the prevention of ransomware attacks and phishing attacks.

Any potential implementation of IoT devices should be considered carefully. For example, an IoT physical premises security system could be infiltrated to observe comings and goings, or even to control the system[15]. IoT devices are the most vulnerable[15] and so these types of device should only be used if essential and with caution - does the device encrypt its signals for example?

If RoboDoc were to use an IaaS cloud service, it would need to ensure the security aspects were set up correctly[15]. Specifically:

- Access levels
- Monitoring systems
- Encryption
- Detection systems

According to Mijwil et al[28], healthcare professionals are exploring the use of Aritificial intelligenence (AI) to help with diagnosis and personalisation of treatment. Similarly, cyber-criminals are experimenting with using AI for sophisticated attacks. Devoteam describe how AI has already been used in the following types of attack as far back as 2019[29]:

- Deepfake

- Phishing
- Denial of Service
- Ransomware
- Persistent threats
- Data processing

Whilst these tpyes of attack are not new (Deepfake is ultimately a form of impersonation), the level of sophistication is greatly improved with AI. As explained previously though, it is humans and not technology that will help RoboDoc defend against this[26]. Good practices in cybersecurity, shared with all staff through training, is the key to defending against attacks[29].

One final area for discussion is the use of security ratings. The use of security ratings, like those proposed by Heng and Lopez in 2019[30], was on the rise even as far back as 2018[31]. It is a way of organisations determining their strength in cyber-security using a continuous, data driven process[32]. The higher the cyber-security rating score, the better the security posture[33]. Security ratings are also useful in improving an organisation's own security processes[32]. Whilst security ratings are not currently a requirement, RoboDoc may wish to establish their security rating through an organisation such as Bitsight[34]. With a good security rating, RoboDoc would be able to use this to demonstrate its strength in this area as a potential third party provider[32]. It could also use security ratings to help in choosing any third party organisations it might wish to work with[32].

Appendix A

These tables show the calculations for each vulnerabilities' risk.

Table B1: Browser, web and email vulnerabilities			Vulnerabilities		
			Attacks Against Browsers (including through un-safe browsing)	Attacks against and from web-sites	Attacks through email
Liklelihood	Threat Agent Factors	Skill level	5	5	6
		Motive	4	5	4
		Opportunity	7	4	4
		Size	2	2	2
	Vulnerability Factors	Ease of Discovery	3	3	3
		Ease of Exploit	3	3	5
		Awareness	1	1	7
		Intrusion Detection	3	3	3
		Averages:	3.5	3.25	4.25
		Likelihood level:	MEDIUM	MEDIUM	MEDIUM
Impact	Technical Impact Factors	Loss of confidentiality	2	2	7
		Loss of integrity	1	2	1
		Loss of Availability	1	1	1
		Loss of accountability	7	9	9
		Averages:	2.75	3.5	4.5
		Technical Impact Level:	LOW	MEDIUM	MEDIUM
	Business Impact Factors	Financial damage	1	2	1
		Reputation damage	1	2	2
		Non-compliance	2	2	2
		Privacy violation	1	4	2
		Averages:	1.25	2.5	1.75
		Business Impact Level:	LOW	LOW	LOW
		Risk:	LOW	LOW	LOW

Table B2: Network and service vulnerabilities			Vulnerabilities		
			Threats in networks	Threats in Wireless networks	Denial of service and distributed denial of service
Liklelihood	Threat Agent Factors	Skill level	9	9	9
		Motive	5	5	4
		Opportunity	4	4	4
		Size	2	2	2
	Vulnerability Factors	Ease of Discovery	3	3	3
		Ease of Exploit	3	3	3
		Awareness	3	3	9
		Intrusion Detection	1	1	1
		Averages:	3.75	3.75	4.375
		Likelihood level:	MEDIUM	MEDIUM	MEDIUM
Impact	Technical Impact Factors	Loss of confidentiality	7	7	1
		Loss of integrity	7	7	1
		Loss of Availability	5	5	5
		Loss of accountability	7	7	7
		Averages:	6.5	6.5	3.5
		Technical Impact Level:	HIGH	HIGH	MEDIUM
	Business Impact Factors	Financial damage	3	3	3
		Reputation damage	7	7	7
		Non-compliance	5	5	7
		Privacy violation	5	5	1
		Averages:	5	5	4.5
		Business Impact Level:	MEDIUM	MEDIUM	MEDIUM
		Risk:	MEDIUM	MEDIUM	MEDIUM

Table B3: Authentication vulnerabilities			Vulnerabilities	
			A false positive authentication (On-site or off-site)	Machines left logged in and unattended
Liklelihood	Threat Agent Factors	Skill level	3	7
		Motive	4	4
		Opportunity	4	1
		Size	2	2
	Vulnerability Factors	Ease of Discovery	3	1
		Ease of Exploit	3	1
		Awareness	7	9
		Intrusion Detection	1	9
		Averages:	3.375	4.25
		Likelihood level:	MEDIUM	MEDIUM
Impact	Technical Impact Factors	Loss of confidentiality	7	7
		Loss of integrity	7	7
		Loss of Availability	7	7
		Loss of accountability	7	7
		Averages:	7	7
		Technical Impact Level:	HIGH	HIGH
	Business Impact Factors	Financial damage	7	7
		Reputation damage	9	9
		Non-compliance	7	7
		Privacy violation	5	5
		Averages:	7	7
		Business Impact Level:	HIGH	HIGH
		Risk:	HIGH	HIGH

Table B4: User and privilige errors			Vulnerabilities		
			Incorrect Data Entry	Accidental deletion	Incorrect privilige levels
Liklelihood	Threat Agent Factors	Skill level	1	1	6
		Motive	1	1	1
		Opportunity	7	7	1
		Size	4	4	2
	Vulnerability Factors	Ease of Discovery	7	7	7
		Ease of Exploit	5	5	5
		Awareness	1	1	1
		Intrusion Detection			
		Averages:	3.71428571	3.71428571	3.28571429
		Likelihood level:	MEDIUM	MEDIUM	MEDIUM
Impact	Technical Impact Factors	Loss of confidentiality	1	1	1
		Loss of integrity	1	1	3
		Loss of Availability	1	1	1
		Loss of accountability	1	1	1
		Averages:	1	1	1.5
		Technical Impact Level:	LOW	LOW	LOW
	Business Impact Factors	Financial damage	1	1	1
		Reputation damage	1	1	1
		Non-compliance	2	2	5
		Privacy violation	1	1	1
		Averages:	1.11111111	1.11111111	1.72222222
		Business Impact Level:	LOW	LOW	LOW
		Risk:	LOW	LOW	LOW

Table B5: Hardware and software errors			Vulnerabilities		
			Equipment failure	Software errors including from ARS	Loss of all hardware
Liklelihood	Threat Agent Factors	Skill level	1	1	1
		Motive	1	1	1
		Opportunity	9	9	9
		Size	1	1	1
	Vulnerability Factors	Ease of Discovery	1	2	1
		Ease of Exploit	1	1	1
		Awareness	1	1	1
		Intrusion Detection	1	3	1
		Averages:	2	2.375	2
		Likelihood level:	LOW	LOW	LOW
Impact	Technical Impact Factors	Loss of confidentiality	1	2	1
		Loss of integrity	1	2	1
		Loss of Availability	9	7	9
		Loss of accountability	1	7	9
		Averages:	3	4.5	5
		Technical Impact Level:	MEDIUM	MEDIUM	MEDIUM
	Business Impact Factors	Financial damage	7	7	9
		Reputation damage	3	9	9
		Non-compliance	5	7	7
		Privacy violation	1	5	5
		Averages:	3.44444444	5.61111111	6.11111111
		Business Impact Level:	MEDIUM	MEDIUM	HIGH
		Risk:	LOW	LOW	MEDIUM

Appendix B

The tables below assign values to likelihood and impact of key features in vulnerabilities and are derived from the OWASP risk rating methodology[7].

Skill level	Score
None	1
Some technical skills	3
Advanced Computer Use	5
Network and Programming Skills	6
Security Penetration Skills	9

Table A1: Threat Agent Skill Level

Opportunity	Score
Full access/expensive resources required	0
Special access/resourcess required	4
Some access/resources required	7
No access/resources required	9

Table A2: Threat Agent Opportunity

Motive	Score
Low/No reward	1
Possible reward	4
High reward	9

Table A3: Threat Agent Motivation

Size of group attacking	Score
Developers	2
System administrators	2
Intranet users	4
Partners	5
Authenticated users	6
Anonymous Internet users	9

Table A4: Threat Agent Group Size

Ease of Discovery	Score
Practically impossible	1
Difficult	3
Easy	7
Automated tools available	9

Table A5: Ease of discovery of vulnerability

Ease of Exploit	Score
Theoretical	1
Difficult	3
Easy	5
Automated tools available	9

Table A6: Ease of exploiting vulnerability

Awareness	Score
Unknown	1
Hidden	3
Obvious	7
Public Knowledge	9

Table A7: Awareness of vulnerability

Intrusion detection	Score
Active detection	1
Logged and reviewed	3
Logged without review	8
Not logged	9

Table A8: Awareness of vulnerability

Loss of Confidentiality	Score
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

Table A9: Technical impact due to loss of confidentiality

Loss of Integrity	Score
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

Table A10: Technical impact due to loss of integrity

Loss of Availability	Score
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

Table A11: Technical impact due to loss of availability

Loss of Accountability	Score
Fully traceable	1
Possibly traceable	7
Completely anonymous	9

Table A12: Technical impact due to loss of Accountability

Financial damage	Score
Less than cost to fix vulnerability	1
Minor effect on annual profit	3
Significant effect on annual profit	7
Bankruptcy	9

Table A13: Business impact due to financial damage

Reputation damage	Score
Minimal damage	1
Loss of major accounts	3
Loss of goodwill	7
Brand damage	9

Table A14: Business impact due to reputation damage

Non-compliance	Score
Minor violation	2
Clear violation	5
High profile violation	7

Table A15: Business impact due to non-compliance

Privacy violation	Score
One individual	3
Hundreds of people	5
Thoudands of people	7
Millions of people	9

Table A16: Business impact due to privacy violation

References

[1] Autonomous Robotic Surgery, *ARS - AUTONOMOUS ROBOTIC SURGERY*, Accessed = 2023-06-08. [Online]. Available: https://www.ars-project.eu/.

[2] 'Information technology - security techniques - information security management systems - requirements (iso/iec 27001:2013),' BSI, Tech. Rep., Mar. 2017.

[3] 'Information security management systems - part 3: Guidelines for information security risk management (revision of bs iso/iec 27005:2011),' BSI, Tech. Rep., Oct. 2017.

[4] 'Risk management— principles and guidelines,' BSI, Tech. Rep., Nov. 2009.

[5] StandardFusion, *4-step guide to performing an iso 27001 risk analysis*, Accessed = 2023-06-09, 2023. [Online]. Available: https://www.standardfusion.com/blog/4-step-guide-performing-iso-27001-risk-analysis/.

[6] C. P. Pfleeger, S. L. Pfleeger and J. Margulies, *Security in Computing, 5th Edition*. Pearson, 2015.

[7] OWASP Foundation, *Owasp risk rating methodology*, Accessed = 2023-06-08. [Online]. Available: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology.

[8] National Security Centre, *Authentication methods: Choosing the right type*, Accessed 2023-06-15. [Online]. Available: https://www.ncsc.gov.uk/guidance/authentication-methods-choosing-the-right-type.

[9] Department of Health and Social Care, *Policy paper: A cyber resilient health and adult social care system in england: Cyber security strategy to 2030*, Accessed 2023-06-23. [Online]. Available: https://www.gov.uk/government/publications/cyber-security-strategy-for-health-and-social-care-2023-to-2030/a-cyber-resilient-health-and-adult-social-care-system-in-england-cyber-security-strategy-to-2030.

[10] T. Radichel, *Encryption on the wired and wireless who's listening to your communications and how?* Accessed 2023-06-16. [Online]. Available: https://medium.com/cloud-security/encryption-on-the-wired-and-wireless-c5425ec4ae98.

[11] Y. Chung, S. Choi, Y. Lee, N. Park and D. Won, 'An enhanced lightweight anonymous authentication scheme for a scalable localization roaming service in wireless sensor networks,' *National Library of Medicine*, vol. 16, no. 10, 2016. DOI: 10.3390/s16101653.

[12] Fortinet, *What is a port scan? how to prevent port scan attacks?* Accessed 2023-06-16. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/what-is-port-scan.

[13] Microsoft, *Get started for azure it operators*, Accessed = 2023-06-08, 2023. [Online]. Available: https://learn.microsoft.com/en-us/azure/guides/operations/azure-operations-guide.

[14] Microsoft, *What is azure ddos protection?* Accessed 2023-06-15. [Online]. Available: https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview.

[15] M. Mijwil, O. J. Unogwu, Y. Filali, I. Bala and H. Al-Shahwani, 'Exploring the top five evolving threats in cybersecurity: An in-depth overview,' *Mesopotamian Journal of CyberSecurity*, vol. 2023, pp. 57–63, Mar. 2023. DOI: 10.58496/MJCS/2023/

010. [Online]. Available: https://mesopotamian.press/journals/index.php/CyberSecurity/article/view/44.

[16] H. C. I. P. M. Software? *Authentication methods: Choosing the right type*, Accessed 2023-06-19. [Online]. Available: https://copyright.co.uk/how-can-i-protect-my-software.html.

[17] WIPO, *Summary of the berne convention for the protection of literary and artistic works (1886)*, Accessed 2023-06-19. [Online]. Available: https://www.wipo.int/treaties/en/ip/berne/summary_berne.html.

[18] copyright-australia.com, *The berne convention : List of countries*, Accessed 2023-06-19. [Online]. Available: https://copyright-australia.com/176-Countries-Berne-Convention.html.

[19] GOV.UK, *Defend your intellectual property*, Accessed 2023-06-19. [Online]. Available: https://www.gov.uk/patent-your-invention/prepare-your-application.

[20] GOV.UK, *Apply for a patent*, Accessed 2023-06-19. [Online]. Available: https://www.gov.uk/defend-your-intellectual-property.

[21] 'Data protection act 2018 2018 chapter 12,' Crown and database right, Tech. Rep., May 2018.

[22] 'Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation),' THE EUROPEAN PARLIAMENT and COUNCIL, Tech. Rep., Apr. 2016.

[23] Proton AG, *Everything you need to know about the "right to be forgotten"*, Accessed 2023-06-19. [Online]. Available: https://gdpr.eu/right-to-be-forgotten/.

[24] Proton AG, *What are the gdpr fines?* Accessed 2023-06-19. [Online]. Available: https://gdpr.eu/fines/.

[25] A. Fleck, *Cybercrime expected to skyrocket in coming years*, Accessed 2023-06-20. [Online]. Available: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/.

[26] M. Koo, *Technology won't protect your data—humans must come first*, Accessed 2023-06-20. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2023/03/30/technology-wont-protect-your-data-humans-must-come-first/.

[27] R. Antle, *The inside story of how n.l. health officials failed to act before a ransomware gang struck*, Accessed 2023-06-20. [Online]. Available: https://www.cbc.ca/news/canada/newfoundland-labrador/nl-ransonmare-attack-report-in-depth-1.6860899.

[28] M. Mijwil, M. Aljanabi and A. H. Ali, 'Chatgpt: Exploring the role of cybersecurity in the protection of medical information,' *Mesopotamian Journal of CyberSecurity*, vol. 2023, pp. 18–21, Feb. 2023. DOI: 10.58496/MJCS/2023/004. [Online]. Available: https://mesopotamian.press/journals/index.php/CyberSecurity/article/view/29.

[29] DEVOTEAM, *Dangers and challenges of ai in cybersecurity. are you prepared?* Accessed 2023-06-20. [Online]. Available: https://www.devoteam.com/expert-view/dangers-and-challenges-of-ai-in-cybersecurity/.

[30] S.-H. Heng and J. Lopez, 'Defining a new composite cybersecurity rating scheme for smes in the u.k,' eng, in *INFORMATION SECURITY PRACTICE AND EXPERIENCE, ISPEC 2019*, ser. Lecture Notes in Computer Science, vol. 11879, Switzerland: Springer International Publishing AG, 2019, pp. 362–380, ISBN: 9783030343385.

[31] Help Net Security, *Adoption of security ratings platforms is on the rise*, Accessed 2023-06-20. [Online]. Available: `https://www.helpnetsecurity.com/2018/04/27/security-ratings-platforms/`.

[32] MediaSonar, *Security ratings: Do they matter?* Accessed 2023-06-21. [Online]. Available: `https://mediasonar.com/2023/02/14/security-ratings/`.

[33] BITSIGHT, *What are security ratings? a complete and authoritative guide*, Accessed 2023-06-21. [Online]. Available: `https://www.bitsight.com/blog/what-is-a-security-rating`.

[34] BITSIGHT, *Manage cyber risk. outdo expectations.* Accessed 2023-06-21. [Online]. Available: `https://www.bitsight.com`.