Contents

1.0 Introduction

Masood and Sonntag (2020) have extensively documented the potential benefits and challenges of Industry 4.0 for small businesses. This report presents a risk assessment for the proposed digital transformation of "Pampered Pets," a small suburban business that primarily sells pet food and other items through face-to-face interactions and email orders.

Section 1.1 justifies the chosen methodologies, while section 1.2 analyses the current business state using appropriate methodologies. Section 1.3 proposes a model of the business, which is further analysed in section 2 using the same methodologies and mitigations. A summary of the findings is presented in section 3.

1.1 Methodology

To provide a thorough assessment of risks, the team will use a hybrid approach to mitigate the weaknesses of any one individual technique (Krishnan, 2017) by leveraging complementary asset-centric (DREAD) and developer-centric (STRIDE) methodologies. Threats will be identified using STRIDE and then rated qualitatively using DREAD (Kim et al., 2022). STRIDE and DREAD results will subsequently be used to produce attack trees to identify possible mitigations of the highest-rated threats (Salter et al., 1998; Shostack, 2014).

1.2 Current Digital Landscape

The digital topology of the current system is shown below, figure 1, it is an unsecured network with multiple endpoints:

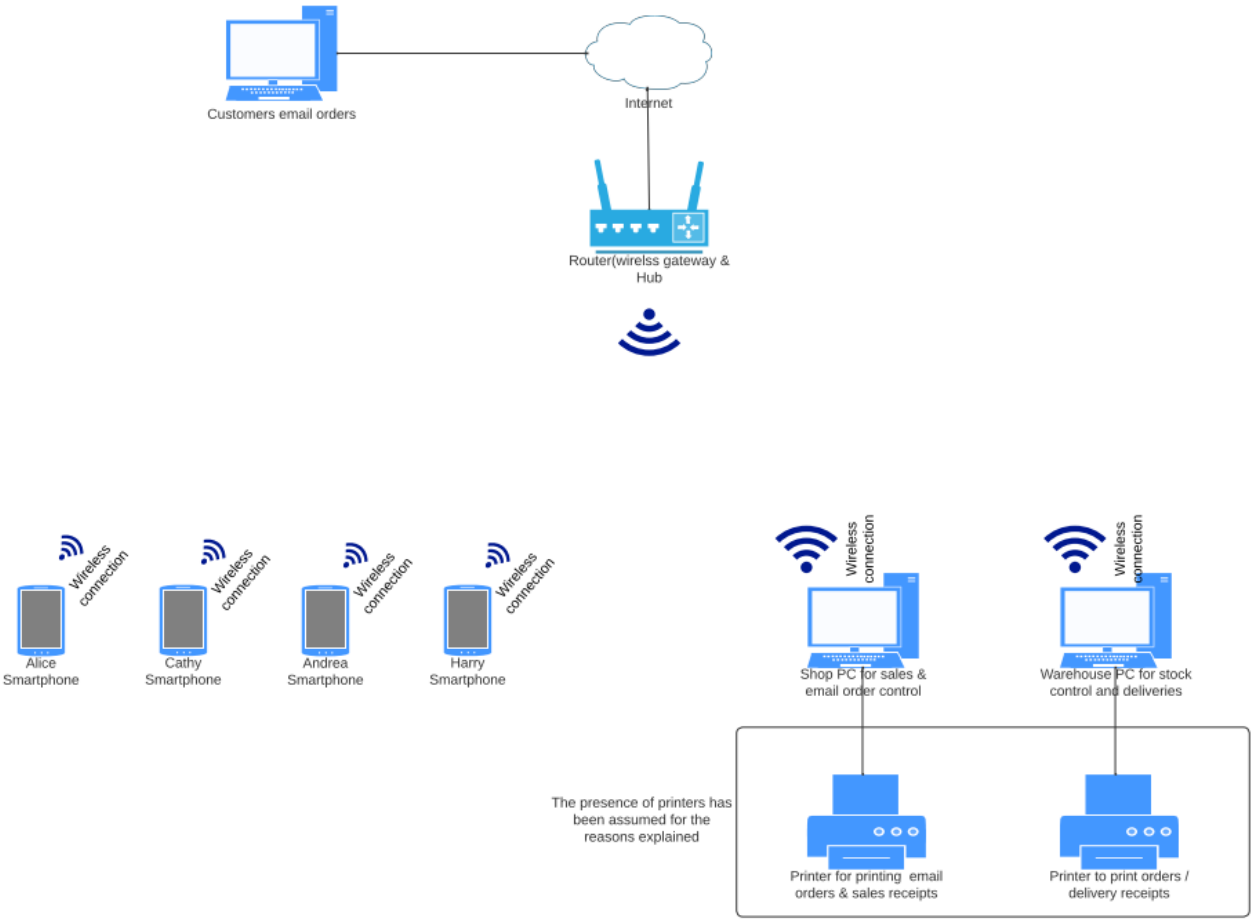

Figure 1 Current digital topology

1.3 DREAD, STRIDE & Attack Trees

The STRIDE and DREAD threat models are used to evaluate Pampered Pets' vulnerability threats. Both models provide qualitative risk analysis based on personal perceptions. The STRIDE model identifies potential mitigations by assessing likelihood and impact, while the DREAD model provides a risk rating assessment. See Table 1 for identified threats using the STRIDE model.

STRIDE Model (Shostack,2014; Shevchenko et al., 2018)

Attack Type	Likelihood	Impact	Mitigations
SPOOFING	High	Very high	1. Use authentication and authorisation methods. 2. Make employees Cyber aware and provide security training
TAMPERING	High	Very high	1. Apply encryption policy such as MDA 5 or SHA256. 2. Implement strong security policies (strong passwords, MFA) and security procedure in regular basis.
REPUDIATION	Very High	High	1.Use tracking methods such as secure logs to track malicious events.
INFORMATION DISCLOSURE	High	Low	1. Use access control lists (ACL). 2. Use strong encryption policies (MDA 5 or SHA256).
DENIAL OF SERVICE	High	Medium	1. Use web application firewalls at the application layer. 2. Use reliable antivirus on all the corporate devices
ELEVATION OF PRIVILEGE	High	Medium	1. Use Access control lists. 2. Apply least privilege principles.

Table 1 STRIDE Summary.

Table 1 summarises potential vulnerabilities and threats to the current business landscape, a full table can be found in Appendix 1. Currently, there is a high likelihood of cyber-attacks.

DREAD (Meier et al.,2003; EC Council, no date)

The DREAD threat model (see table 2) provides a current risk rating assessment, the full table is shown in Appendix 2.

Threat attack	Risk	Mitigations
DAMAGE	Risk =7.5	1. Create back up procedure in a secure cloud space. 2. Use WAF at application layer
REPRODUCIBILITY	Risk =7.5	1. Keep software up to date. 2. Apply recommended security batches
EXPLOITABILITY	Risk =9	1. Implement strong password policies. 2. Use MFA. 3. Use segmented wireless access points to reduce unauthorised access.
AFFECTED USERS	Risk =10	1. Apply access control lists (ACL). 2. Apply security procedures in a regular basis. 3. Make users cyber-aware and provide training. 4. Apply proxy settings. 5. Be GDPR Compliant
DISCOVERABILITY	Risk =10	1. Install secure logs to track events and malicious activities.

Table 2 DREAD threat model.

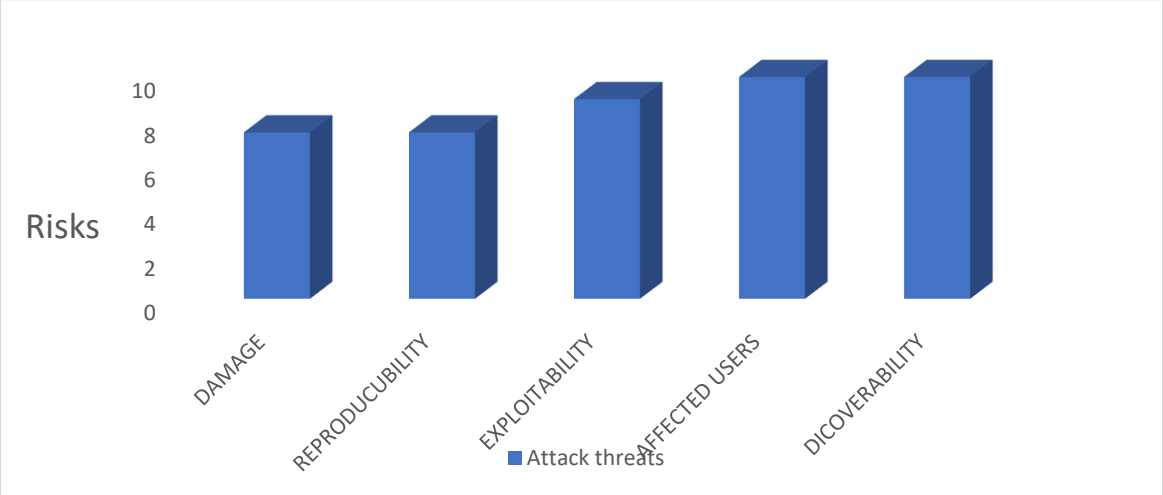

Figure 2 DREAD column chart displaying the risk level.

The Overall Threat rating calculated by the DREAD formula currently is calculated as:

D+R+E+A+D=7.5+7.5+9+10+10= 44

The DREAD ratings can be seen in Appendix 6.

Vulnerability risk for the Papered Pet as it currently stands is critical. Critical vulnerabilities must be addressed immediately.

Attack Defence Trees (ADT)

ADT diagrams suggest defences to mitigate possible attacks with a "Probability of Success" domain to quantify risk (Kordy et al., 2014). CVSS (Common Vulnerability Scoring System) V3 algorithm assesses the probability of attack success and mitigation success. The CVSS calculator and probability of success equations can be found in Appendix 5. The ADT is complex and has subsystems, including the physical store subsystem for face-to-face commerce. Figures 3-6 show success probabilities for various subsystems and Table 3 provides vulnerability scores. Implementing mitigations and addressing vulnerabilities will guide Pampered Pet's future.

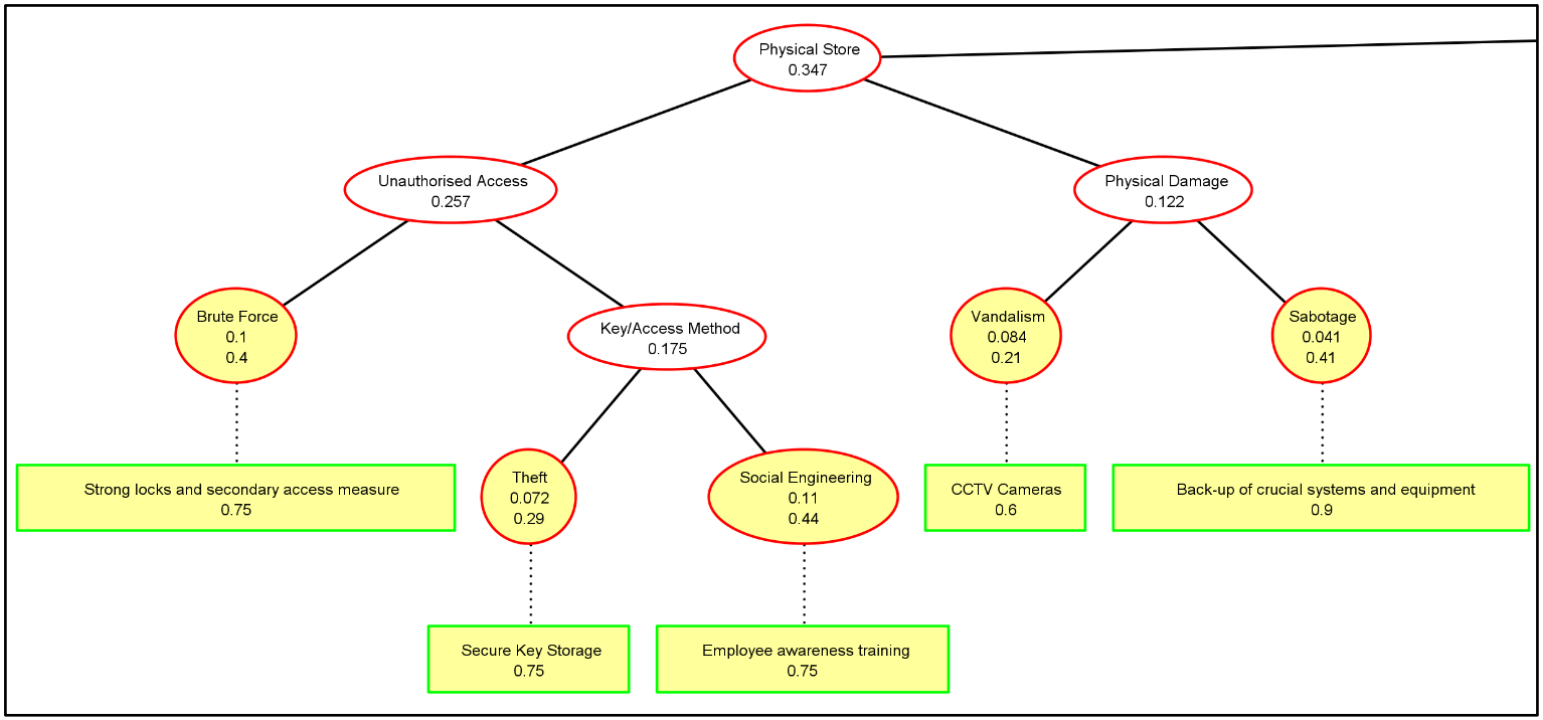

Figure 3 Physical Store

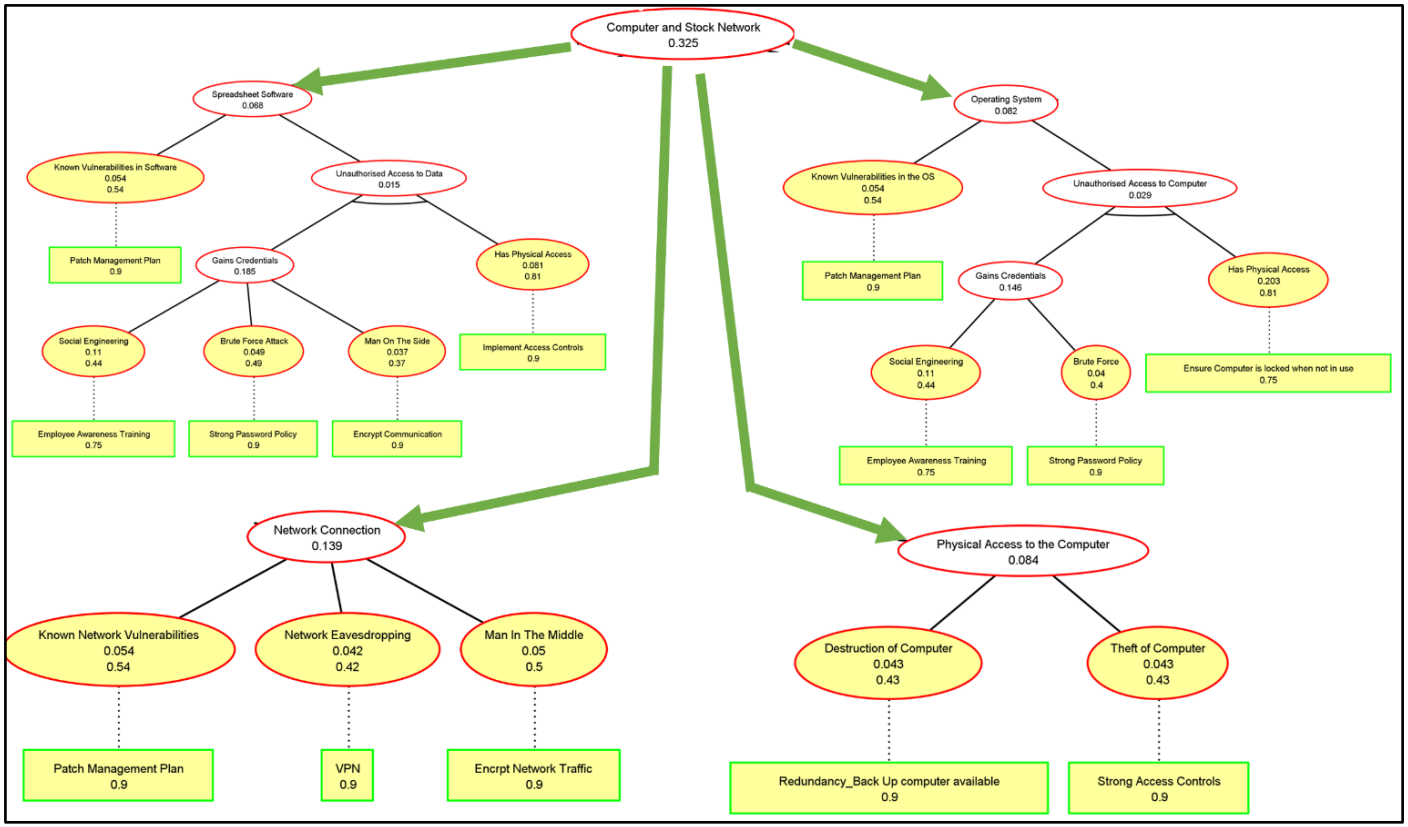

Figure 4 Collage of the computer and stock store subsection of the ADT.

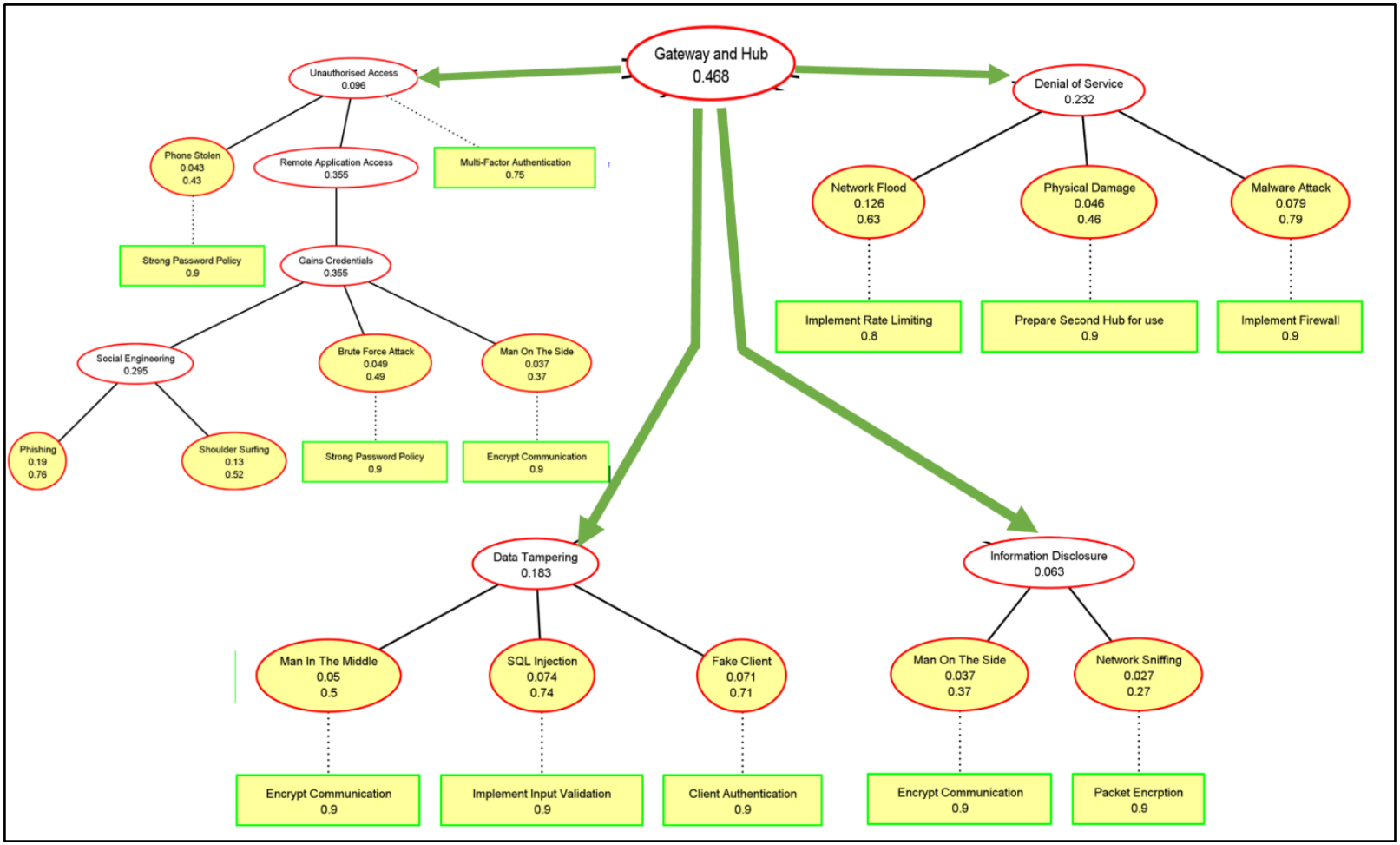

Figure 5 Gateway/Hub Section

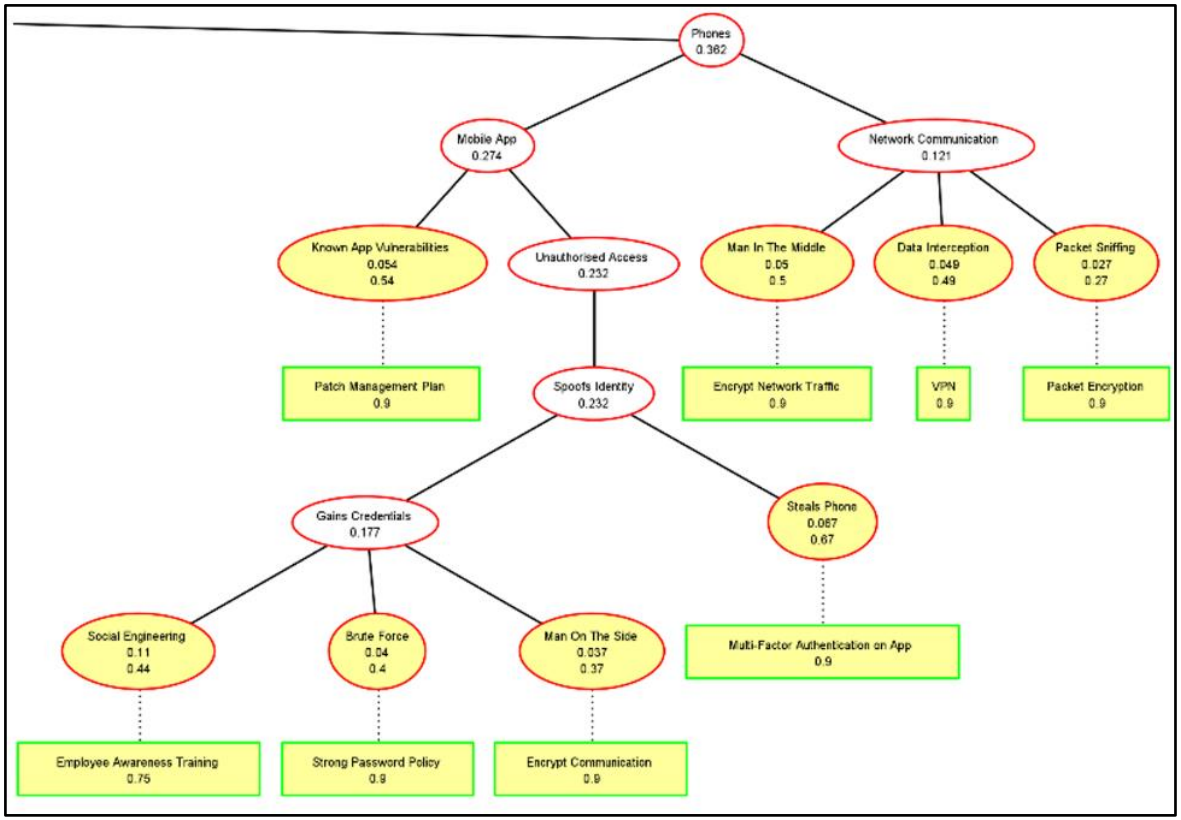

Figure 6 Phone Section

Attack	Attack Vector	Attack Complexity	Privileges r	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact	CVSS Score	CVSS Score(0-1)
Brute Force Access	Physical	Low	None	None	Unchanged	Low	Low	None	4	0.4
Brute Force Attack	Local	High	None	None	Unchanged	Low	Low	Low	4.9	0.49
Data Interception	Network	Low	High	None	Unchanged	High	None	None	4.9	0.49
Destruction of Computer	Physical	Low	Low	None	Unchanged	None	None	High	4.3	0.43
Exploit of Known Vulnerabilities	Network	Low	Low	None	Unchanged	Low	Low	None	5.4	0.54
Fake Client	Network	Low	Low	None	Unchanged	None	High	Low	7.1	0.71
Malicious Insider	Network	Low	High	None	Unchanged	Low	Low	Low	4.7	0.47
Malware Attack	Adjacent Network	High	Low	None	Changed	Low	High	High	7.9	0.79
Malware Infection	Local	High	High	Required	Changed	Low	Low	Low	4.7	0.47
Man in the Middle	Local	High	Low	Required	Unchanged	High	Low	None	5	0.5
Man on the Side	Adjacent Network	High	None	Required	Unchanged	Low	Low	None	3.7	0.37
Network Eavesdropping	Network	High	High	Required	Unchanged	High	None	None	4.2	0.42
Network Flood	Network	High	Low	None	Changed	None	None	High	6.3	0.63
Opportunistic Attack	Network	Low	High	None	Unchanged	High	Low	None	5.5	0.55
Packet Sniffing	Network	Low	High	None	Unchanged	Low	None	None	2.7	0.27
Phishing	Network	Low	None	Required	Unchanged	Low	High	Low	7.6	0.76
Phone Stolen	Physical	Low	Low	None	Unchanged	None	None	High	4.3	0.43
Phone Theft	Physical	Low	None	None	Changed	High	Low	Low	6.7	0.67
Physical Access	Network	Low	Low	None	Unchanged	High	High	Low	8.1	0.81
Physical Damage	Physical	Low	None	None	Unchanged	None	None	High	4.6	0.46
Poor Security Connection	Local	High	Low	Required	Unchanged	Low	None	Low	3.9	0.39
Sabotage	Physical	Low	Low	None	Unchanged	Low	Low	Low	4.1	0.41
Server Breach	Local	High	High	None	Changed	None	None	Low	5.3	0.53
Shoulder Surfing	Physical	Low	None	None	Unchanged	High	Low	None	5.2	0.52
Social Engineering	Local/Physical	Low	None	Required	Unchanged	Low	Low	None	4.4	0.44
SQL Injection	Network	High	None	None	Unchanged	High	High	None	7.4	0.74
Theft of Computer	Physical	Low	Low	None	Unchanged	None	None	High	4.3	0.43
Theft of Key	Physical	High	None	Required	Unchanged	Low	Low	None	2.9	0.29
Vandalism	Physical	Low	Low	None	Unchanged	None	None	Low	2.1	0.21

Table 3 CVSS Scores for Current Digital Landscap

2.0 Digitalisation Process

According to Dovgal et al. (2021), global Ecommerce sales continue to grow year on year (see Figure 7) In the UK, the % of total sales represented by Ecommerce sales is 25% as of February 2023 (Office for National Statistics, 2023).

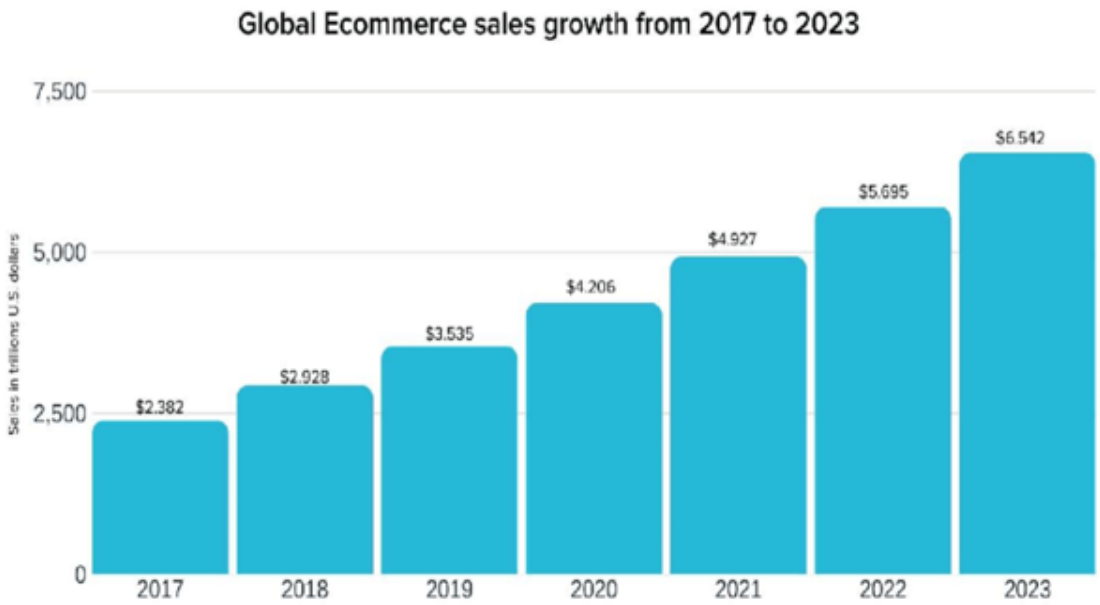

Figure 7 Global E-commerce Sales

Small businesses benefit from an online presence (Haines, 2022), some evidence supporting these benefits are:

- Online sales are crucial for 81% of small businesses, with 43% reporting a significant impact on revenue (Insureon, 2018).
- In the UK, 81% of shoppers conduct online research before making a purchase (Anderson, 2022).
- Without an online presence, businesses risk losing customers to competitors who offer better customer service through digital transformation (Haines, 2022).

2.1 Timeline Proposed

Assuming the goal is to create a secure digitised network for Pampered Pets over 6 months, the following timeline is proposed. See Appendix 3 for more details.

Figure 8 Timeline

2.2 Proposed Changes to Network Topology

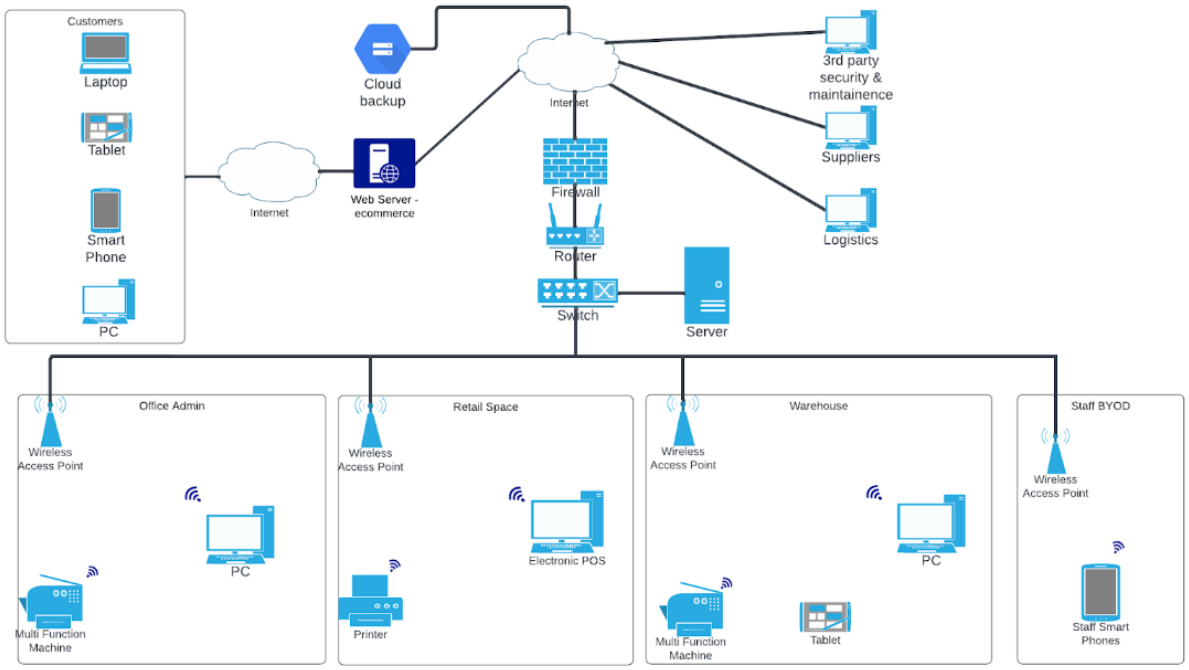

Figure 11 Digital topology for digitalisation.

Figure 11 shows a network with multiple wireless access points to improve secure Wi-Fi reliability by reducing congestion. This layout serves as the foundation for the subsequent threat analysis.

2.3 Risk & Threat for New System

Digitalisation completed, STRIDE and DREAD are used to re-evaluate the threats:

STRIDE (Van Leeuwen et al.,2018)

THREAT ATTACK	LIKELIHOOD	IMPACT	Mitigations
SPOOFING	Medium	Very high	Monitor log to check user login activities.
TAMPERING	Medium	Very high	Secure logging data.
REPUDIATION	Medium	High	Cloud monitoring and logging.
INFORMATION DISCLOSURE	Medium	Very high	Use authentication and authorisation to limit access.
DENIAL OF SERVICE	High	Very high	Whitelisting and block IP addresses
ELEVATION OF PRIVILEGE	High	Low	Use least privilege service.

Table 4 STRIDE analysis post digitalisation.

We observe cyber-attacks have a high impact and require skilled programming and expert tools; more details are shown in Appendix 4.

DREAD (Meier et al.,2003; EC Council, no date)

THREAT ATTACK	RISK	Mitigations
DAMAGE	Risk = 8	Add encryption methods, SHA256 or MDA5.
REPRODUCIBILITY	Risk = 5	1. Keep software up to date 2. Apply recommended security batches
EXPLOITABILITY	Risk = 5	1. Use strong password policies. 2. Use MFA.
AFFECTED USERS	Risk = 6	1. Apply access control lists (ACL) 2. Apply security procedures on a regular basis.
DISCOVERABILITY	Risk = 5	Use secure logs to track events and malicious activities

Table 5 DREAD Post Digitalisation

The Overall Threat rating calculated by the DREAD formula after the digitisation is calculated as

D+R+E+A+D=8+5+5+6+5 = 29

Digitising Pampered Pets reduced vulnerability risk from 44, but it still exists. Mitigation solutions outlined in the section should be implemented to address these vulnerabilities.

Attack Defence Trees

Figure 12 shows the digitalised ADT of Pampered Pets as a single system, reducing the attack surface and resulting in a lower probability of success score of 0.542, indicating increased security. In contrast, the current business has a high score of 0.922, indicating a high likelihood of a successful attack. These scores support the idea that digitalisation would enhance the business's security, score breakdown is found in Appendix 5.

The CVSS scores for the digitalised business are shown below (see Table 6).

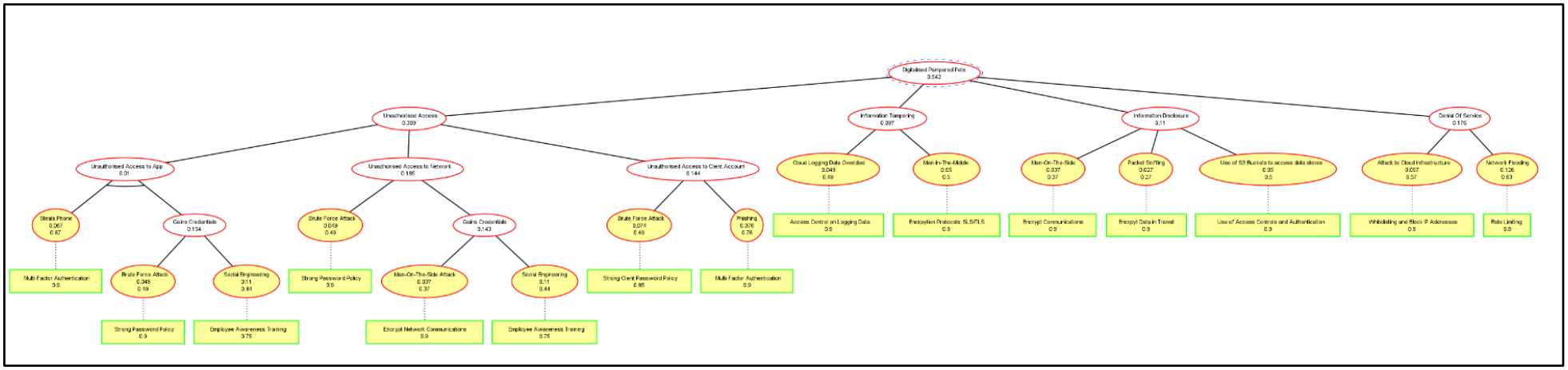

Figure 12 ADT for digitalised business

Attack	Attack Vector	Attack Complexity	Privileges required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact	CVSS Score	CVSS Score(0-1)
Brute Force Attack	Local	High	None	None	Unchanged	Low	Low	Low	4.9	0.49
Cloud Infrastrucutre Attack	Adjacent Network	Low	Low	None	Unchanged	None	None	High	5.7	0.57
Cloud Logging Data Overided	Network	Low	High	None	Unchanged	None	High	None	4.9	0.49
Man-In-The-Middle	Local	High	Low	Required	Unchanged	High	Low	None	5	0.5
Man-On-The-Side Attack	Adjacent Network	High	None	Required	Unchanged	Low	Low	None	3.7	0.37
Network Flooding	Network	High	Low	None	Changed	None	None	High	6.3	0.63
Packet Sniffing	Network	Low	High	None	Unchanged	Low	None	None	2.7	0.27
Phishing	Network	Low	None	Required	Unchanged	Low	High	Low	7.6	0.76
Phone Theft	Physical	Low	None	None	Changed	High	Low	Low	6.7	0.67
Social Engineering	Local/Physical	Low	None	Required	Unchanged	Low	Low	None	4.4	0.44
Use of S3 Buckets	Network	High	High	None	Unchanged	High	Low	None	5	0.5

Table 6 CVSS Scores for post-digitalisation

3.0 Mitigations and Summary

Threats to Pampered Pets were identified using STRIDE and DREAD threat models, and cloud computing is recommended to mitigate them (Van Leeuwen et al.,2018). Digitising features can also help with GDPR and PCI DSS compliance. Specific recommendations include:

- Implementing an e-commerce system handled by a third party for cybersecurity and compliance with GDPR and PCI DSS (Abdulkader et al.,2013).
- Investing in advanced ERP logistic systems for improved reporting, customer service, supply chain management, and cost savings (Costelo,2021).
- Using online marketing campaigns to create brand awareness and customer engagement (Abdulrazak et al.,2022).
- Implementing regular training for staff and appointing a data protection officer for GDPR and PCI DSS compliance.
- Using online marketing campaigns to ensure proper handling of customer data and obtain their consent.

Cloud computing improves security by managing, accessing, securing, and recovering data during malicious events. Supply chain changes are not recommended, even though reduce costs (Tummala et al., 2006), due to the high risk of ingredient quality, disruptions caused by COVID, and difficulty ensuring the quality of ingredients from overseas producers.

4.0 References

Abdulkader, S. & Abualkishik, J. & Abualkishik, A.M. (2013) Cloud Computing and E-commerce in Small and Medium Enterprises (SME ’s) : the Benefits , Challenges. International Journal of Science and Research (IJSR). ISSN (Online): 2319-7064.

Abdulrazak T.,A(2022) The Effect of Digital Marketing on SMEs. *A case study of Swedish And Nigerian companies. Luleå University of Technology.*

Anderson, D. (2022). 38 Statistics Retail Marketers Need to Know in 2023. Available from: https://www.invoca.com/blog/retail-marketing-statistics [Accessed 9th April 2023].

Costello L. (2021) Benefits of ERP: Advantages, Disadvantages & Selecting an Enterprise Resource Planning System. Available from: https://terillium.com/benefits-of-erp/ [Accessed 4 March 2023].

Dovgal, O., Dovgal, G., Goncharenko, N. & Fomina, Y. (2021). DIGITAL TRANSFORMATION OF THE BUSINESS ENVIRONMENT: PROSPECTS AND PARADOXES. Available from: https://www.researchgate.net/figure/Global-Ecommerce-sales-growth-from-2017-to-2023-Source-Global-Ecommerce-Sales-from-2017_fig5_349624660 [accessed 9 Apr, 2023].

EC Council Cyber security exchange(No date). DREAD Threat Modeling: An Introduction to Qualitative Risk Analysis. Available from: https://eccouncil.org/cybersecurity-exchange/threat-intelligence/dread-threat-modeling-intro/ [Accessed 30 March 2023].

Haines, B. (2022). 9 Reasons Your Business Needs an Online Presence. Available from: https://www.thebalancemoney.com/putting-offline-business-online-2531853 [Accessed 9th April 2023].

Insureon. (2018). Poll: 43% of small businesses experience sizable revenue growth with online sales. Available from: https://www.insureon.com/blog/small-business-online-sales-revenue-poll. Accessed [9th April 2023].

Office for National Statistics. (2023). Internet sales as a percentage of total retail sales (ratio) (%). Available from: https://www.ons.gov.uk/businessindustryandtrade/retailindustry/timeseries/j4mc/drsi [Accessed 9th April 2023].

Tummala, V.R., Phillips, C.L. and Johnson, M., (2006). Assessing supply chain management success factors: a case study. *Supply Chain Management: An International Journal*.

Kim, K.H., Kim, K. and Kim, H.K., (2022). STRIDE-based threat modeling and DREAD evaluation for the distributed control system in the oil refinery. *ETRI Journal*.

Krishnan, S., (2017). A hybrid approach to threat modelling. *URL https://blogs. sans. org/appsecstreetfighter/files/2017/03/A-Hybrid-Approach-to-Threat-Modelling. pdf,[Accessed on 10-Jul-2018]*.

Masood, T. & Sonntag, P., (2020). Industry 4.0: Adoption challenges and benefits for SMEs. *Computers in Industry*, *121*, p.103261.

Meier, J. & Mackman, A., & Dunner, M., & Vasireddy, S., & Escamilla, R. & Murukan, A. (2003) Improving Web Application Security: Threats and Countermeasures*. Microsoft Corporation.*

Nweke, L.O. & Wolthusen, S., (2020). A review of asset-centric threat modelling approaches. *International Journal of Advanced Computer Science and Applications*, *11*(2), pp.1-7.

Salter, C., Saydjari. O., Schneier, B. & Wallner, J. (1998) Toward a secure system engineering methodology. In: Proceedings of the 1998 Workshop on New Security Paradigms (NSPW ’98). Charlottesville, Virginia, United States. 2–10.

Shevchenko, N., Chick, T. A., O'Riordan, P., Scanlon, T. P., & Woody, C. (2018). *Threat modeling: a summary of available methods.* Carnegie Mellon University Software Engineering Institute Pittsburgh United States.

Shostack, A. (2014). *Threat modeling : designing for security*. Chapter 4. Wiley & sons ltd.

Van Leeuwen,B.P.,& Urias, V., & Stout,W.M.S., &Lin,H.W. (2018) Applying a Threat Model to Cloud Computing. *Sandia National Laboratories Albuquerque, New Mexico, USA.*

5.0 Appendix

1. STRIDE table current

Attack Type	Description	POLICY VIOLATED	Likelihood	Impact	Mitigations
SPOOFING	● Spoofing the file ● Spoofing a process ● Spoofing a role ● Spoofing a person	Authentication	High	Very high	1.Use authentication and authorisation methods. 2. Make employees Cyber aware and provide security training
TAMPERING	● Installation of Malicious software might Tamper the spreadsheets and the transaction files. ● Installation of Malicious software might Tamper the network.	Integrity	High	Very high	1.Apply encryption policy such as MDA 5 or SHA256. 2. Implement strong security policies (strong passwords, MFA) and security procedure in regular basis.
REPUDIATION	● Absence of secure logs to track malicious activities. ● 3rd person performs actions on behalf of the customer claiming.	Non - repudiation	Very High	High	1.Use tracking methods such as secure logs to track malicious events.
INFORMATION DISCLOSURE	● Sales shop and warehouse files are unprotected ● Warehouse files and Sales shop files are accessible by other personal and corporate devices.	Confidentiality	High	Low	1. Use access control lists (ACL). 2. Use strong encryption policies (MDA 5 or SHA256).
DENIAL OF SERVICE	● Employees' application usage causes a Bandwidth overload. ● Malicious user consumes network resources. ● Tickets with VAT will not be issued.	Availability	High	Medium	1. Use web application firewalls at application layer. 2. Use reliable antivirus to all the corporate devices

	● Server would not be able to handle multiple order requests.				
ELEVATION OF PRIVILEGE	● Absence of assigned roles ● Lack of assigned rights	Authorisation	High	Medium	1.Use Access control lists. 2.Apply least privilege principles.

2. DREAD table current

Threat attack	Description	Risk	Mitigations
DAMAGE	Phishing or social engineering attacks that could retrieve customers' sensitive information violate the CIA triangle.	Risk =7.5	1. Create back up procedure in a secure cloud space to securely retried the data in the event of an attack. 2. Use WAF at application layer
REPRODUCIBILITY	Phishing and social engineering attacks can be easily reproduced due to the lack of security measures and **the** lack of training procedures about cyber-security measures.	Risk =7.5	1.Keep software up to date. 2.Apply recommended security batches
EXPLOITABILITY	A simple access to the network via the computers or the employees' personal devices can cause a big damage.	Risk =9	1.Implement strong password policies. 2. use MFA. 3. use segmented wireless access points to reduce unauthorized access.
AFFECTED USERS	Everybody: Customers and enterprise	Risk =10	1.Apply access control lists (ACL). 2.Apply security procedures in a regular basis. 3. Make user cyber-aware and provide them training. 4. Apply proxy settings. 5. Be GDPR Compliant
DISCOVERABILITY	Unable to track events and malicious activities due to the absence of secure logs, back up procedures, access rights and strong password policy.	Risk =10	1.Install and use secure logs to track events and malicious activities.

3. Timeline Details

Month 1: Network Assessment and Planning

Conduct a comprehensive assessment of the existing network and identify potential security risks. Develop a plan to address identified risks and create a roadmap for the implementation of the new network.

Month 2: Upgrading Hardware and Software

Upgrade network hardware and software, including firewall, antivirus, and intrusion detection/prevention systems. Install the latest updates and patches for all software and operating systems. Implement data backup and recovery solutions.

Month 3: Security Policies and Training

Develop and implement comprehensive security policies and procedures for all staff. Provide training to all employees on cybersecurity best practices and how to handle sensitive data. Conduct periodic security awareness training sessions.

Month 4: Access Control and Authentication

Implement access control and authentication measures to ensure that only authorised personnel can access sensitive data. Implement multi-factor authentication for remote access to the network. Develop a plan for managing and monitoring access logs.

Month 5: Security Monitoring and Incident Response

Implement a security monitoring system to detect and respond to any potential threats. Establish an incident response plan to handle security incidents in a timely and effective manner. Conduct regular security audits.

Month 6: Testing and Refinement

Conduct penetration testing and vulnerability assessments to identify any remaining security weaknesses. Refine the security measures based on the results of the testing and assessment. Develop a plan for ongoing maintenance and monitoring.

4. STRIDE Post Digitalisation

THREAT ATTACK	DESCRIPTION	POLICY VIOLATED	LIKELIHOOOD	IMPACT	Mitigations
SPOOFING	Brute force attack	Authentication	Medium	Very high	Monitor log to check user login activities.
TAMPERING	Unauthorised disabling cloud logging services. Override cloud logging data.	Integrity	Medium	Very high	Secure logging data.
REPUDIATION	Unauthorised user claims to not have access account in the cloud	Non- repudiation	Medium	High	Cloud monitoring and logging
INFORMATION DISCLOSURE	Use ADS S3 buckets to perform unauthorized access to Data stores	Confidentiality	Medium	Very high	Use authentication and authorisation to limit access to data stores
DENIAL OF SERVICE	DoS attack to cloud infrastructure	Availability	High	Very high	Whitelisting and block IP addresses
ELEVATION OF PRIVILEGE	User privilege escalation in the cloud may provide indications of inside threat	Authorisation	High	Low	Use least privilege service accounts to access resources

5. CVSS Scores and Probability of Success Domain

The CVSS scores are calculated using the CVSS V3 calculator shown in Figure 13.

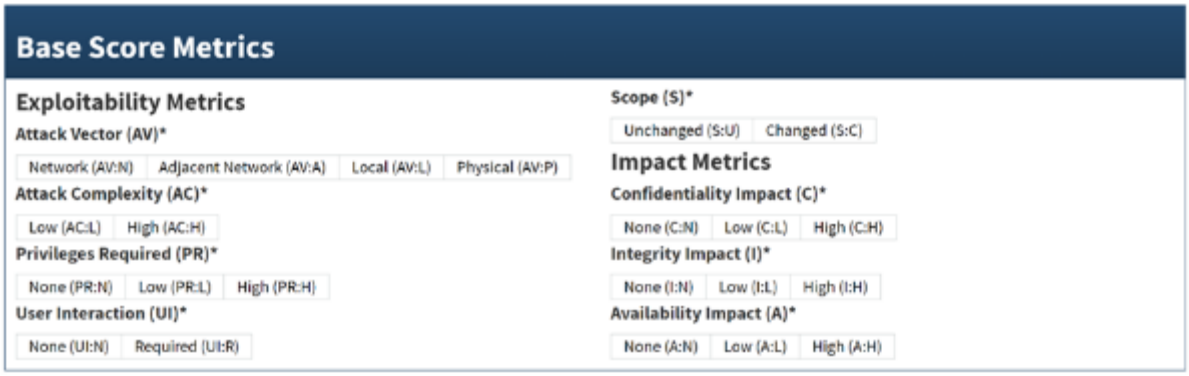

Figure 13 CVSS V3 Base Score metrics (NIST, 2023)

The calculation of the probability of success uses both CVSS scores and mitigation scores provided by the likeness of protection. This is calculated using the calculation in figure 14:

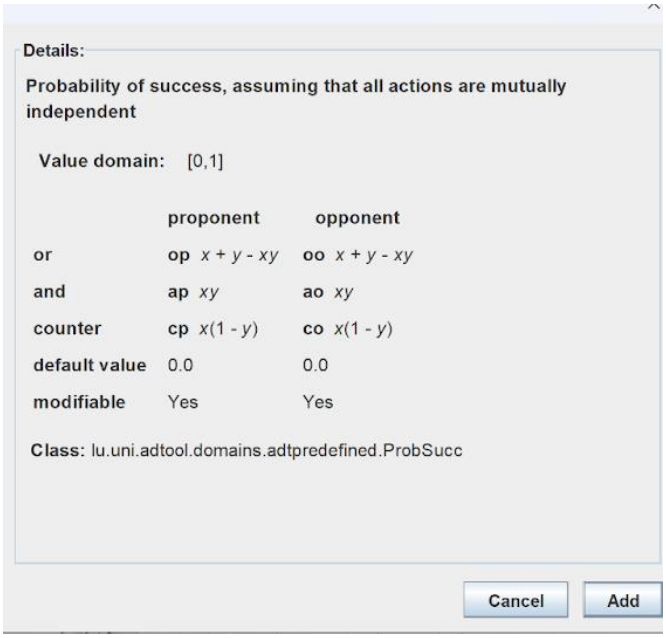

Figure 14 Equations for probability for success

Mitigation scores are given as follows:

Score	**Effectiveness rating (0-1)**
1	Completely effective (No chance of success with mitigation in place)
0.7 - 0.99	Highly Effective (Low chance of success with mitigation in place)
0.4 - 0.69	Effective (reduces the chance of success with mitigation in place)
0.1 - 0.39	Slightly Effective (Helps towards mitigation but only slight reduction of chance of success with mitigation in place)
0 - 0.09	No impact/ negligible effect

6. DREAD Rating

Critical (40–50)	Critical vulnerability; address immediately.
High (25–39)	Severe vulnerability; consider for review and resolution soon.
Medium (11–24)	Moderate risk; review after addressing severe and critical risks.
Low (1–10)	Low risk to infrastructure and data.