Unit 9 Assignment - Proposal to Grocery Business Owner

1 Introduction

Technological development is indisputably relevant to grocery retailing; both in terms of value enhancement and cyber threat (Weyer et al., 2020). In 2021, online grocery accounted for 12% of the UK grocery market and that figure is expected to rise to as much as 30% by 2030 (Simmons et al., 2022). Potential vulnerability to cyber attacks as well as fear of non-compliance with data legislation are genuine business risks, but please do not dismiss new technology on the basis of these initial concerns. Customers are vocal on their appetite for e-commerce (Saikrishnan, 2023), but trust of the online system is a key influence on whether customers make a purchase (Tyrväinen & Karjaluoto, 2022), and it is therefore imperative that the risks are properly assessed and the correct cyber security practices are implemented.

2 Benefits of an online shopping system (OSS)

Whilst e-commerce is often associated with corporations and globalisation, an online shopping system (OSS) can also offer significant benefits to a local grocery retailer.

2.1 Benefits to customer

There are obvious advantages for your customers due to the differences between physical and virtual space. 24/7 availability online gives customers more opportunity to browse products, and an online catalogue can prevent customer frustration if a product is not available after having travelled to make a purchase (Taher, 2021). This online catalogue can also facilitate a greater detail (and intuitive categorisation) of product information - the availability of which is a major influence on buying behaviour (Zhao et al., 2021).

2.2 Benefits to business

Customers' satisfaction, in turn, generates benefits to the business itself. 24/7 sales are exacerbated by an increased customer volume from the geographical advantage that customers can shop from any distance (Mason, 2019). Furthermore, the stock from these sales can be administered more effectively by using an 'as needed' stock ordering strategy to reduce business costs and avoid waste (Taher, 2021).

3 Cyber security concerns

Cyber security is a major consideration when incorporating any digital service into a business. More specifically, e-commerce is the most attacked of all industries, accounting for 32% of all cyber attacks (Bhatia et al., 2021), making security one of the highest priority issues surrounding the technology aspect of e-commerce (Liu et al., 2022).

Protecting a system begins with understanding the threat. In order to do so, we can employ threat modelling techniques that aim to facilitate the consideration of threats in a structured way (NCSC, 2023).

3.1 STRIDE threat modelling technique

This modelling technique is a mnemonic that considers threats as seven categories (Microsoft, 2022). STRIDE is used by Microsoft as a method of identifying potential security risks early, and is endorsed by the UK National Cyber Security Centre (DIST, 2023).

Table 1

STRIDE Threat Model applied to the OSS

Category	Description	OSS relevance	Mitigation
Spoofing	Legitimate credentials are used to authenticate the	A customer falls victim to a phishing attack and has inadvertently revealed	Multi-Factor Authentication - the act of requiring further authentication after a successful password entry

	wrong person, such as their username and password (Microsoft, 2022).	their password to an attacker through key-logging malware or a spoof website.	(Brookshear & Brylow, 2020). Common methods include sending a passcode to a mobile phone number, or a biometric check such as fingerprint scanning.
Tampering	Altering data either at rest or in transit (Microsoft, 2022).	Creating a backdoor into a system using SQL injection in order to access private information (Alberti et al., 2018)	Robust input validation must be implemented on any field where a user is able to enter information (DIST, 2023).
Repudiation	Claiming innocence or naivety without anyone being able to prove otherwise (Microsoft, 2022).	A customer claims they didn’t receive a refund.	Logging of transactions with appropriate digital signatures (Yang et al., 2003).

Information Disclosure	Being able to access documents for which access was not granted (Microsoft, 2022).	Customer closes their account, an administrator leaves the company, or a service provider contract ends.	Must be a solid process that withdraws access to the system and ensures that information is protected (DIST, 2023). Encryption must be enabled for data both at rest and in transit, and private keys must be adequately protected to ensure encryption cannot be compromised (DIST, 2023)
Denial of Service (DoS)	Flooding a server with messages until it becomes overloaded and unable to operate properly - effectively blocking your service from use	Customers being blocked from using the system can affect sales, disrupt transactions, and compromise user trust.	A well established and configured firewall system (Brookshear & Brylow, 2020) as well as intrusion detection systems (IDS).

	(Brookshear & Brylow, 2020).		
Elevation of Privilege	A path for an attacker to elevate their permissions and access to a point where they can control the entire system (Microsoft, 2022).	A string of vulnerabilities is in place which allow small steps up in permissions.	regularly updating, patching and maintaining your service.

3.2 Attack Trees

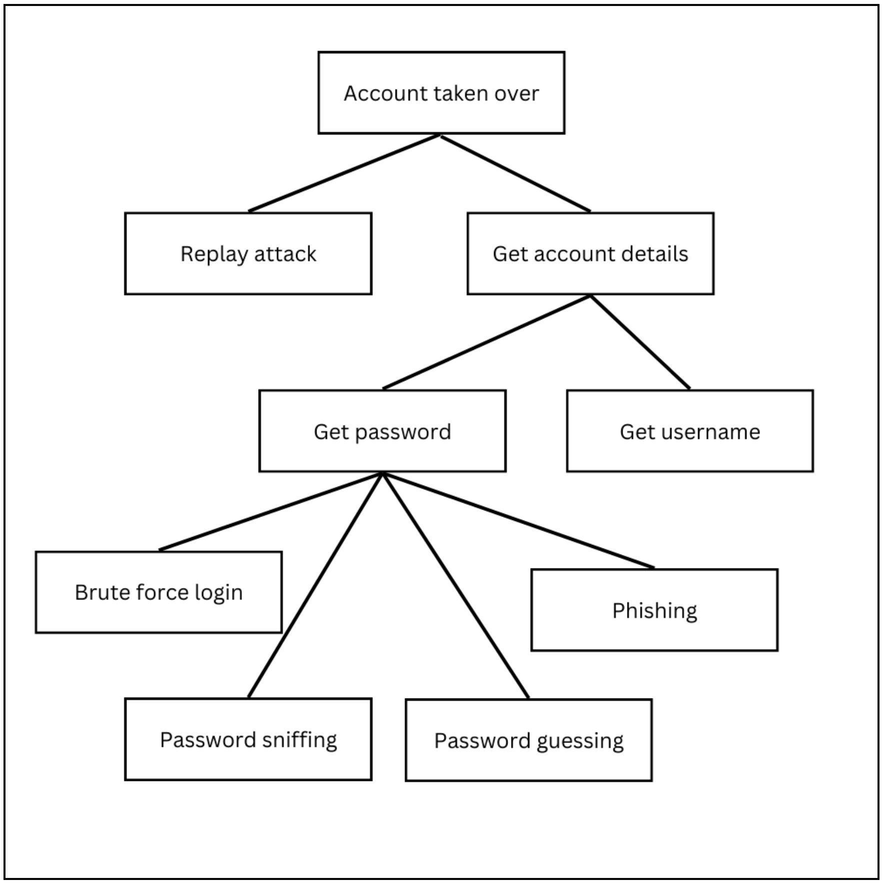
Whilst the STRIDE technique above allows us to plan against common threat vectors, attack trees and protection trees let us consider the system at hand more specifically and demonstrates the process of a successful attack (Edge et al., 2007). These trees are constructed by choosing a system failure and considering the possible pathways that lead to it (Anderson, 2020). Let's consider the failures of an account takeover and a data breach.

3.2.1 Account takeover

Figure 1

Account takeover attack tree

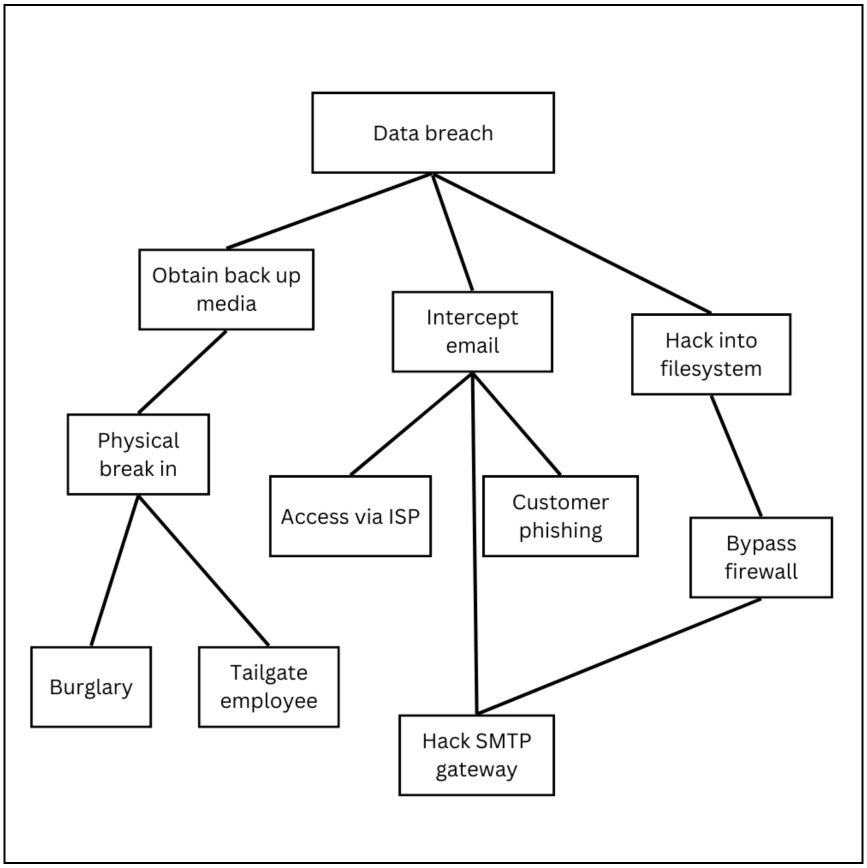
Note: adapted from Talukder & Pais, 2009.



3.2.2 Data breach

Figure 2

Data breach attack tree



3.3 Lockheed Martin Cyber Kill Chain

Another invaluable method of defending against cyber attacks is examining the process that a cyber criminal follows to infiltrate your system. Although the specifics can vary, the Lockheed Martin Cyber Kill Chain demonstrates the general steps that an attack follows which can highlight potential countermeasures (Yadav & Rao, 2015).

3.3.1 Reconnaissance

At this stage attackers will be looking to acquire information in your system and looking for potential weaknesses to exploit (Yadav & Rao, 2015). Tracking and logging visitor records, and setting up alerts for suspicious user behaviour patterns is key to defence here (Lockheed Martin, 2015).

3.3.2 Weaponization

The information acquired in reconnaissance is used to design an attack specific to the system (Yadav & Rao, 2015). Although it is not entirely possible to respond directly to this stage, it is imperative that any suspicious behaviour found prompts analysis and comparison to known attack vectors - as well as ensuring malware tracking is up to date (Lockheed Martin, 2015).

3.3.3 Delivery

Attackers will now be looking to find a way to get the malware into the system (Lockheed Martin, 2015). The majority of the time, this will require human intervention although ‘zero-click’ attacks are possible (Tn & Shailendra Kulkarni, 2023). Attackers may develop a social engineering technique such as phishing, or compromise a website (Yadav & Rao, 2015). User awareness and training is crucial here as described in 4.3.5.

3.3.4 Exploitation

The weaknesses found in reconnaissance will now be exploited to gain access and find routes through the system (Lockheed Martin, 2015). This makes it imperative to have firewalls and IDS (section 4.3.3) as well as keeping your system up to date (4.3.2).

3.3.5 Installation

Malware will be installed into the system and a persistent back door is likely to be created to provide ease of future access (Lockheed Martin, 2015). Anti-virus packages should be up to date and scanning but many attackers will be using anti-anti-virus software (Yadav & Rao, 2015). Configuring your antivirus against these types of attack as opposed to using default settings is known to have good results against anti-anti-virus software (Samociuk, 2023).

3.3.6 Command & control (C&C)

Now that the system is compromised, the attacker can create a remote controlling capability (Lockheed Martin, 2015). These communication channels are often unobservable and may not be distinguishable from legitimate traffic (Yadav & Rao, 2015). As much as 90% of C&C communications are HTTP based (Wang et al., 2016) so intelligent analysis of this type of traffic and use of a data loss prevention system is imperative.

3.3.7 Actions on objectives

At this stage, many of the elements of STRIDE can become reality. You may become part of a botnet for a distributed DoS attack or elevation of privilege may take place until the entire system is under control (Yadav & Rao, 2015). At this point, it is important to have disaster recovery in place and deployment of forensic data experts may be necessary (Lockheed Martin, 2015).

4 Data Privacy

Data has become arguably the most valuable commodity on the planet (California Senate Judiciary Committee, 2018). It is true, therefore, that cyber criminals are trying to capitalise on the wealth of knowledge that companies are accumulating.

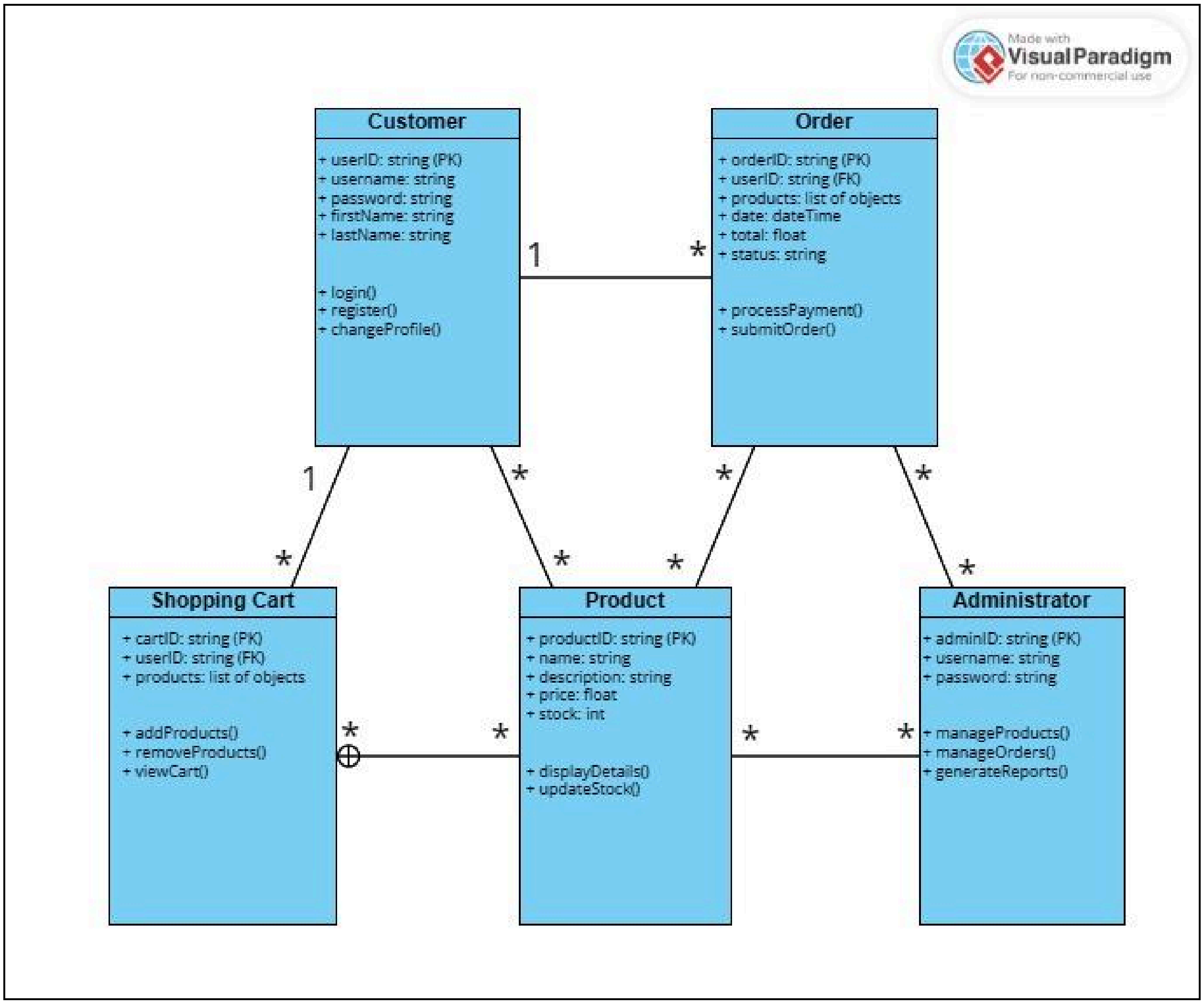
4.1 The UK GDPR

The UK General Data Protection Regulation (GDPR) explains the rights of the data subjects and the duties of the data processors who execute the rules put in place by the data controllers (Suokannas, 2019).

Much of the GDPR is in the interest of protecting the data subjects - in this case your customers such as abilities to view their data, correct any mistakes, transfer it to another controller, and, unless there is a legal reason for the contrary, have their data deleted (Suokannas, 2019). Below is a class diagram demonstrating different objects and data that they are likely to contain.

Figure 3

OSS Class Diagram



4.2 Data capture in an OSS

There are four main types of data that your new system is likely to capture about the customer: personal data, behavioural data, engagement data, and feedback data (Krysik, 2021). The GDPR applies to personal data only, although determining whether the data you are processing is ‘personal’ is not necessarily trivial (Finck & Pallas, 2020). The ICO explains that if data can be used to identify a person then it is liable to GDPR (ICO, 2018). Typical personal data includes customer names, addresses, contact information, payment details, and less obvious online identifiers such as IP addresses and cookie information.

5 Recommendations

5.1 Encryption

Ensuring your website uses the transfer protocol HTTPS (which adds public key encryption to the HTTP protocol) is a crucial step to securing your customers accounts (Brookshear & Brylow, 2020). Public key encryption uses a private key which will ‘sign’ a transaction but doesn’t need to share the private key as there is a public key that can verify the signature. This allows trust and non-repudiation as only the private key owner could have authorised the transaction (Awati, 2022).

5.2 Firewalls, IDS and DLPS

Simply put, firewalls are the boundary between a system and the surrounding networks; intrusion detection systems (IDS) look for anomalies entering that boundary; and data leakage prevention systems (DPLS) prevent data from being wrongfully taken out of the boundary (Anderson, 2020). There are several types of firewall and incorporating the right one into the OSS will require striking a balance between sufficient security, and resource intensity bottlenecking the flow of data.

5.3 User access control

Access control is described by Kissel (2013) as “the process of granting or denying specific requests” and is a combination of authentication and authorisation (Lampson, 1992). In particular, Role Based Access Control (RBAC) allows different permissions and access to different areas of a system depending on what type of user they are (CyBOK, 2021). In the case of your OSS, different users would include registered and unregistered customers, and system administrators - each with different capabilities. See the use case diagram below (fig 4) for a more detailed proposition of RBAC in your OSS as well as an abuse case diagram (fig 5) which demonstrates potential unwanted users.

Figure 4

Use Case Diagram for OSS

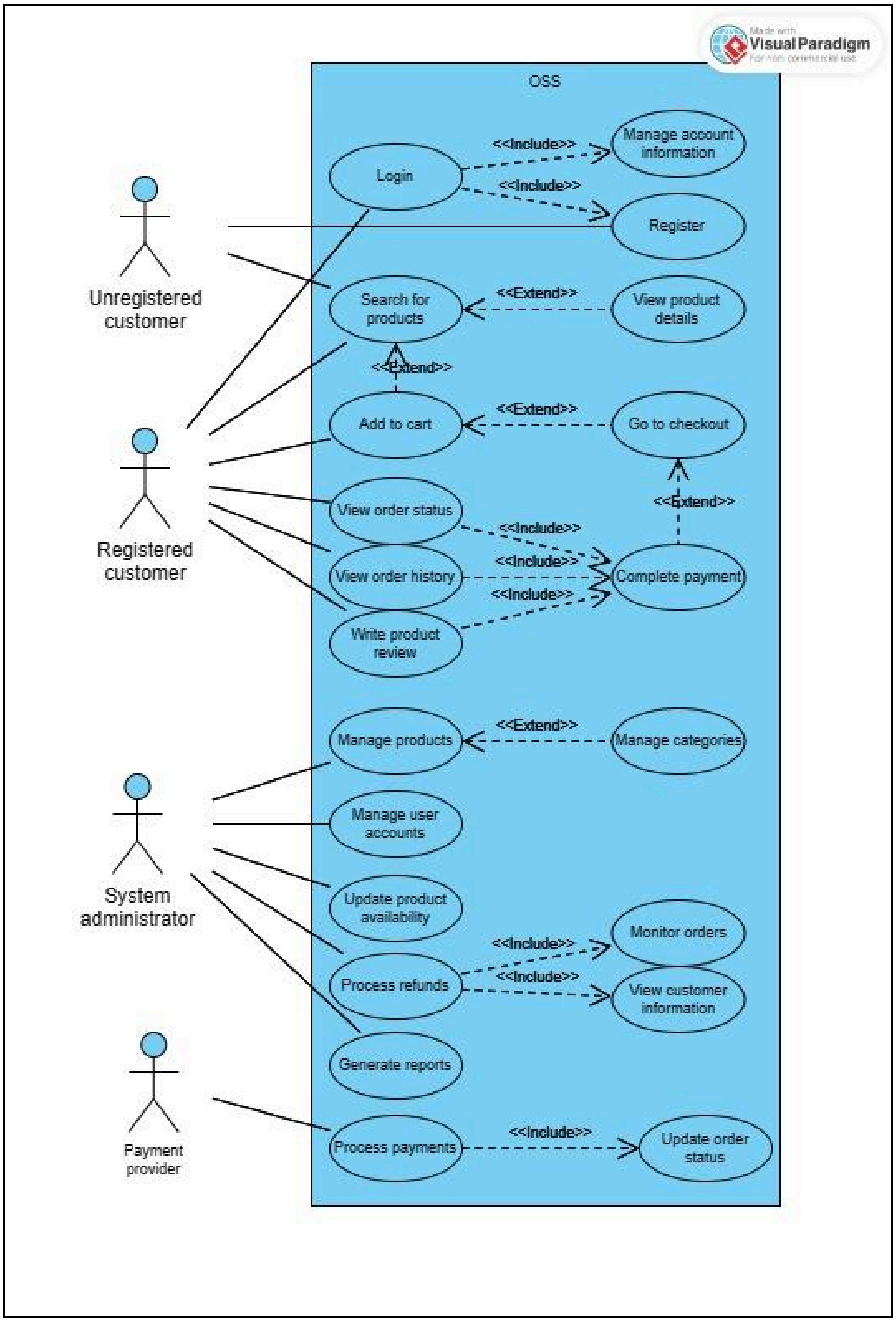
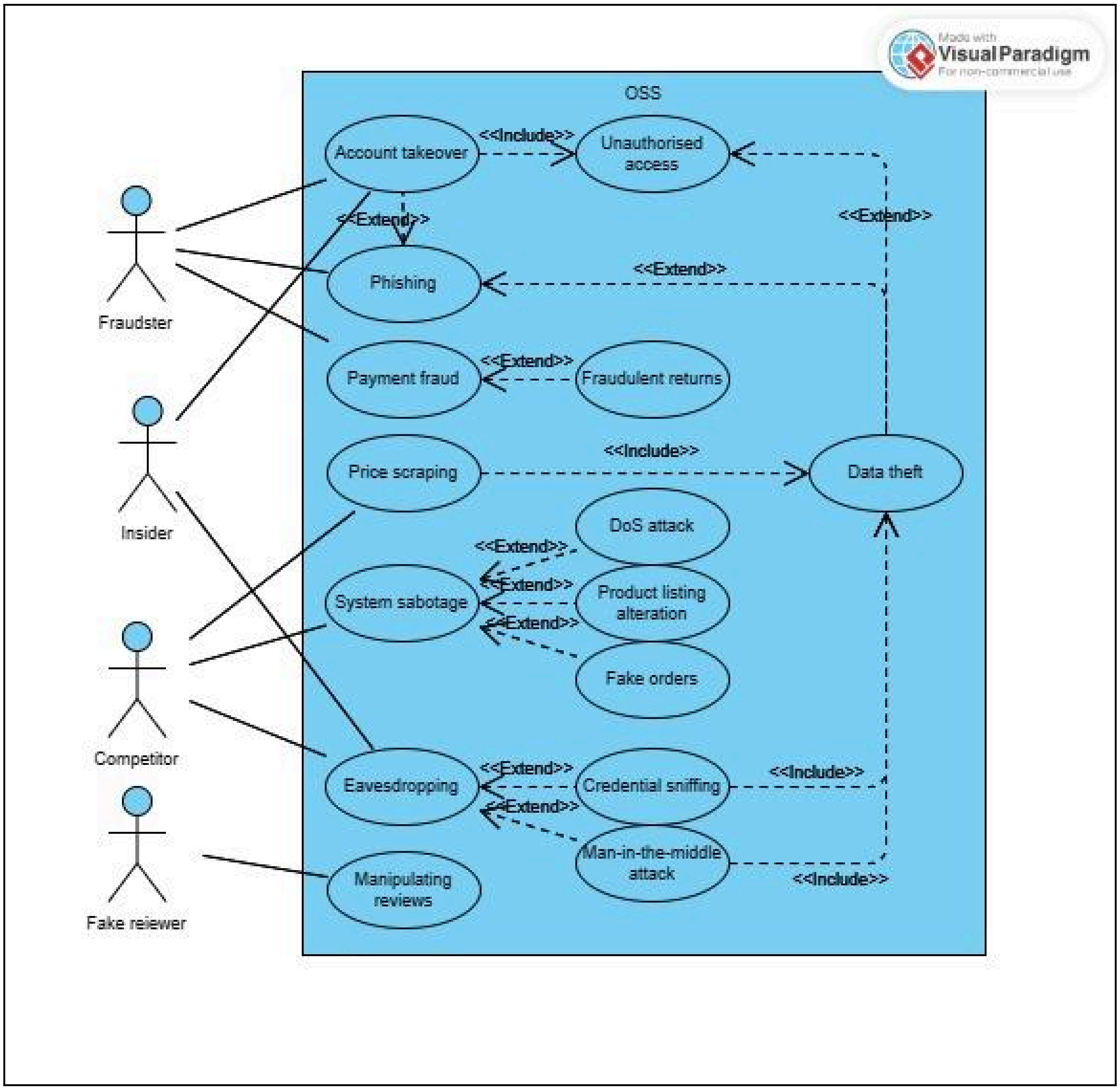


Figure 5

Abuse Case Diagram for OSS



5.5 User training

The human factor in a cyber attack cannot be understated. All of the above techniques are useless if an employee/customer (knowingly or unknowingly) allows an attack to bypass security measures. Training and awareness on the topics discussed in the threat models above (section 3.1 specifically) can reduce the likelihood of a successful attack (Evans et al., 2016).

5.6 Further recommendations

- Complete a full data protection impact assessment from the UK ICO;
- Ensure your payment provider is fully PCI DSS compliant;
- Enforce a strong password policy and enable MFA for customers and administrators;
- Create an incident response plan.
- Have a regimented update and patch management plan to stay current with security releases.

6 Conclusion

This proposal has demonstrated how the benefits of an online shop can be enjoyed by your business and your customers regardless of cybersecurity concerns. Threat models allow you to view attacks from different perspectives: the perspective of the attacker in the case of the Lockheed Martin Cyber Kill Chain; the perspective of the system in the case of attack and protection trees; and the perspective of established cybersecurity professionals in the case of STRIDE. Together, these defences will allow you to embrace technology and ultimately future proof your business for the ever growing next generation of customers.

References

Aggarwal, C. C., Ashish, N. & Sheth, A. (2013) The internet of things: A survey from the data-centric perspective. *Managing and mining sensor data:* 383-428.

Alberti, M., Pondenkandath, V., Wursch, M., Bouillon, M., Seuret, M., Ingold, R. & Liwicki, M. (2018) Are you tampering with my data? *Proceedings of the European Conference on Computer Vision (ECCV) Workshops*

Anderson, R. (2020) Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed. Indianapolis: Wiley Publishing.

Awati, R. (2022) What is non-repudiation and how does it work? Available from: https://www.techtarget.com/searchsecurity/definition/nonrepudiation [Accessed 24 January 2024].

Bhatia, N. L., Shukla, V. K., Punhani, R. & Dubey, S. K. (2021) Growing Aspects of Cyber Security in E-Commerce. *2021 International Conference on Communication information and Computing Technology (ICCICT)*: 1-6

Brookshear, J. G. & Brylow, D. (2020) Computer Science: an overview. 13th ed. New York: Addison Wesley Longman Inc.

California Senate Judiciary Committee (2018) AB 375 Legislative History. *Historical and Topical Legal Documents* 1748 Available from: https://digitalcommons.law.scu.edu/historical/1748 [Accessed 24 January 2024].

CyBOK Knowledgebase v1.1.0 (2021)

de Neira, A.B., Kantarci, B. & Nogueira, M. (2023) Distributed denial of service attack prediction: Challenges, open issues and opportunities. *Computer Networks* 222: 109553.

DSIT (Department for Science, Innovation & Technology) (2023) Conducting a STRIDE-based threat analysis. Available from: https://assets.publishing.service.gov.uk/media/645bb8142226ee00130ae612/Conducting_a_STRIDE-based_threat_analysis.pdf [Accessed on 24 January 2024].

Edge, K. Raines, R., Grimaila, M., Baldwin, R., Bennington, R & Reuter C. (2007) The Use of Attack and Protection Trees to Analyse Security for an Online Banking System. *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*. Waikoloa, HI, USA: IEEE. 144b-144b.

Evans, M., Maglaras, L. A., He, Y. & Janicke, H. (2016) Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks* 9(17): 4667-4679.

Finck, M. & Pallas, F. (2020) They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law* 10(1): 11-36.

Jin, X., Ye, D. & Chen, C. (2021) Countering spoof: towards detecting deepfake with multidimensional biological signals. *Security and Communication Networks*: 1-8.

Kissel, R. (2013) Revision 2: Glossary of key information security terms. *NIST IR 7298.* Darby, PA, USA: Diane Publishing.

Krysik, A. (2021) Customer Data in eCommerce: How Do Online Stores Collect and Manage Information About Website Users? Available from: https://recostream.com/blog/customer-data-ecommerce [Accessed 23 January 2024].

Lampson, B., Abadi, M., Burrows, M. & Wobber, E. (1992) Authentication in distributed systems: Theory and practice. *ACM Transactions on Computer Systems* 10(4): 265–310.

Liu, X., Ahmad, S.F., Anser, M.K., Ke, J., Irshad, M., Ul-Haq, J. & Abbas, S. (2022) Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in Psycho*logy 13: 927398.

Lockheed Martin (2015) GAINING THE ADVANTAGE: Applying Cyber Kill Chain® Methodology to Network Defense. Available from: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf [Accessed on 24 January 2024].

Mason, R., (2019) Developing a profitable online grocery logistics business: Exploring innovations in ordering, fulfilment, and distribution at ocado. *Contemporary Operations and Logistics: Achieving Excellence in Turbulent Times*: 365-383.

NCSC (National Cyber Security Centre) (2023) Risk Management - Threat Modelling https://www.ncsc.gov.uk/collection/risk-management/threat-modelling [Accessed on 24 January 2024].

PCI (2018) PCI DSS Quick Reference Guide. Available from: https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf [Accessed on 24 January 2024].

Saikrishnan, D. (2023) CONSUMER PERCEPTION AND AWARENESS ON E-COMMERCE. *Journal of Service Industry Management* 15(1): 102-121.

Samociuk, D. (2023) Antivirus Evasion Methods in Modern Operating Systems. *Applied Sciences* 13(8): 5083.

Simmons, V., Spielvogel, J., Timelin, B. & Tjon Pian Gi, M. (2022) The next S-curve of growth: Online grocery to 2030. *Navigating the market headwinds: The State of grocery retail*: 30-35.

Suokannas, V. (2019) GDPR Compliance check for Ecommerce platforms.

Taher, G. (2021) E-commerce: advantages and limitations. *International Journal of Academic Research in Accounting Finance and Management Sciences* 11(1): 153-165.

Talukder, A.K. & Pais, A.R. (2009) Suraksha: A Security Designers' Workbench. Available from: https://www.academia.edu/download/67406071/sdw.pdf [Accessed 25 January 2024].

Tn, N. & Shailendra Kulkarni, M., (2023) Zero click attacks–a new cyber threat for the e-banking sector. *Journal of Financial Crime* 30(5): 1150-1161.

Tyrväinen, O. & Karjaluoto, H. (2022) Online grocery shopping before and during the COVID-19 pandemic: A meta-analytical review. *Telematics and Informatics* 71: 101839.

Wang, X., Zheng, K., Niu, X., Wu, B. & Wu, C. (2016) Detection of command and control in advanced persistent threat based on independent access. *2016 IEEE International Conference on Communications (ICC)*: 1-6

Weyer, J., Tiberius, V., Bican, P. & Kraus, S. (2020) Digitizing grocery retailing: The role of emerging technologies in the value chain. *International Journal of Innovation and Technology Management* 17(08): 2050058.

Yadav, T. & Rao, A. M. (2015) Technical aspects of cyber kill chain. *Security in Computing and Communications: Third International Symposium, SSCC*: 438-452.

Yang, S., Su, S.Y. & Lam, H. (2003) A non-repudiation message transfer protocol for e-commerce. *IEEE International Conference on E-Commerce*: 320-327

Zhao, H., Yao, X., Liu, Z. & Yang, Q. (2021) Impact of pricing and product information on consumer buying behavior with customer satisfaction in a mediating role. *Frontiers in Psychology*: 12: 5016.