Vulnerability Audit and Assessment for ‘www.pamperedpets.org.uk’

Baseline Analysis and Plan

Bradley Graham, 2024

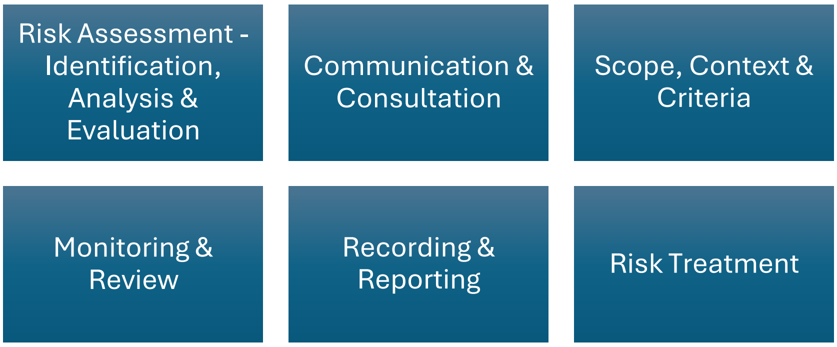
Contents

I. Vulnerability Audits and Assessments

Vulnerability audits and assessment are crucial for business risk management, and fundamental for cybersecurity. Risk is the possibility of harmful results, such as loss of capital; and in the context of cybersecurity, a risk can exist because of threats which can exploit vulnerabilities of the business information system [1]. A vulnerability audit and assessment provide a way of maintaining trust in the business information system, by providing risk communication, consultation, recording, assessment, monitoring and review [2].

[1]. Definitions of risk, threat and vulnerability are provided in the RFC 4949 standard of the Internet Engineering Task Force (IETF). Meanwhile, the term 'cybersecurity' assumes the existence of threats in 'information security' as explained by Spremić and Šimunic (2018).

[2]. The ISO 31000:2018 risk management guideline provides the following non-sequential, stage-based model of the risk management process:



Risk Assessment - Identification, Analysis & Evaluation
Communication & Consultation
Scope, Context & Criteria
Monitoring & Review
Recording & Reporting
Risk Treatment

Figure 1. ISO 31000:2018 Risk Management Process

II. Security Challenges

Examples of vulnerabilities that can affect www.pamperedpets.org.uk are outlined below:

Vulnerability Type	*Examples*
Technical Vulnerability	User Input Fields, Outdated Software
Human Vulnerability	Phishing, Bad Actors
Economic Vulnerability	Service Disruption, Recovery Costs, Ransomware
Governance Vulnerability	Unclear Policies
Management Vulnerability	Reactive Mitigation
Cyber-Intelligence Vulnerability	Lack of Threat or Black-Market Intelligence
Systems Vulnerability	Security Breach Ripples, Insecure API protocols
Ethical Vulnerability	Data Theft, Violations of GDPR, HIPAA or Animal Welfare Standards

Figure 2. Examples of Vulnerabilities for www.pamperedpets.org.uk

Prevention, detection, and correction are risk mitigation strategies, that should be selected with regards to both business impact, and technical impact of a risk. Exploitations that breach resource confidentiality, integrity, or availability can have particularly large technical impact [3].

[3]. Resource confidentiality, integrity & availability (CIA) is afforded by secure information systems, and underpins many technical services. The prevention, detection & correction (PDC) model of risk mitigation, alongside the CIA attributes are described in more detail by LaPiedra (2002).

Examples of potential risk controls for the aforementioned vulnerability types are outlined below:

Vulnerability Type	*Prevention*	*Detection*	*Correction*
Technical Vulnerabilities	Static Code Analysis	Web Application Firewalls	Patch Management Systems
Human Vulnerabilities	Security Awareness Training	Email Security Systems	Incident Ticketing
Economic Vulnerabilities	Open-Source Security Tools	Financial Assessments	Incident Runbooks
Governance Vulnerabilities	Policy Management Platforms	Employee Feedback	Incident Ticketing
Management Vulnerabilities	Risk Assessment Frameworks	Threat Intelligence Platforms	Risk Treatment Plans

Cyber-Intelligence Vulnerabilities	Threat Intelligence Platforms	Threat Hunting Tools	Threat Intelligence Platforms
Systems Vulnerabilities	Security Architecture Frameworks	Information and Event Management Platforms	CI/CD Pipelines
Ethical Vulnerabilities	Privacy Impact Assessment Frameworks	Privacy-Enhancing Technologies	Accountability Mechanisms

Figure 3. Examples of mitigations for potential vulnerabilities of www.pamperedpets.org.uk

III. Proposed Assessment Methodology

III. a. Assumptions and Limitations

Security is instrumental in protecting general ethical values, including: the duty of legal compliance, business virtues, and the customers' contextual integrity [4]. That's our directive. A probabilistic assessment will be provided due the need to identify vulnerabilities with the largest risk attached, during systematic risk management. The black-box contract prevents a client interview, but experiences will be drawn upon.

[4]. Contextual integrity is a term used by Loi & Christen. (2020) referring to how customer expectations are context-based. A consideration of virtues is inspired by Howard (2017) who explains the importance of virtue-based security frameworks.

Key Assumptions
Duty for GDPR Compliance
Duty for PCI DSS Compliance
Duty for ISO/IEC 27001 Compliance
For-Profit Organisation
Pet Pampering Service
Customer Record Storage for Personalised Customer Services
Media Presence for Marketing
Payment System for Online Booking
Staff Record Storage for Human Resource Services
Stock Inventory Management Storage for Logistics Services
Customer Expectations that Business is Fashion Conscience
Customer Expectations that Business is Science Conscience

Figure 4. Key Assumptions made about www.pamperedpets.org.uk

III. b. Proposed Action Plan

The step-by-step plan is as follows [5]:

1. Perform Reconnaissance
    a. Gather Publicly Available Information
    b. Try Phishing via Email
2. Perform an Automated Scan for Vulnerabilities
3. Check for Known Vulnerabilities
    a. Check for Content Management System vulnerabilities.
4. Test for Common Web Application Vulnerabilities
    a. Try Code Injections
    b. Try Weak Credentials
    c. Try Insecure Direct Object Reference
    d. Check Security Certificate Expiration Dates
5. Report Findings
    a. Provide Clear and Detailed Information about Vulnerabilities
    b. Provide Potential Impact Report
    c. Provide Compliance Report
    d. Offer Mitigations

[5]. This is a derivation of McNab (2017)'s network security assessment methodology.

IV. Business Impact

The vulnerability audit and assessment will take approximately one week to complete. During this time, there is a very small chance of disruption of service while automated scans are taking place, which should take no longer than fifteen minutes in total, so will be conducted out of business hours.

Upon completion of the vulnerability audit and assessment, the business will be equipped with knowledge of the current state of business risk, to be utilised in future, strategic, decision-making.

V. References

Howard, D. (2017) ‘Civic Virtue and Cybersecurity’ in: Demont-Biaggi, F. (eds) *The Nature of Peace and the Morality of Armed Conflict*. Cham, Germany: Palgrave Macmillan. 181-201. Available from: https://doi.org/10.1007/978-3-319-57123-2_10 [Accessed 19 February].

LaPiedra, J. (2002) *The Information Security Process Prevention, Detection and Response* [pdf]. GIAC Certifications. SANS Institute. Available from: https://www.giac.org/paper/gsec/501/information-security-process-prevention-detection-response/101197 [Accessed 19 February 2024].

Loi, M. & Christen, M. (2020) ‘Ethical Frameworks for Cybersecurity’, in: Christen, M., Gordijn, B. & Loi, M. (eds) *The Ethics of Cybersecurity*. The International Library of Ethics, Law and Technology: Springer Open. 73-95. Available from: https://library.oapen.org/bitstream/handle/20.500.12657/22489/1/1007696.pdf [Accessed 19 February 2024].

McNab, C. (2017). *Network Security Assessment: Know your Network*. 3rd ed. Beijing: O’Reilly Media.

Spremić, M., Šimunic, A. (2018) 'Cyber security challenges in digital economy', *Proceedings of the World Congress on Engineering 2018 Vol I WCE 2018*. London, U.K, 4-6 July. Hong Kong: IAENG. Available from: https://www.iaeng.org/publication/WCE2018/WCE2018_pp341-346.pdf [Accessed 19 February 2024].

VI. Bibliography

European Commission. (2016). Data Protection in the EU. Available from: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en [Accessed 19 February 2024].

The IETF Trust. (2007) RFC 4949, Internet Security Glossary, Version 2. Available from: https://datatracker.ietf.org/doc/html/rfc4949 [Accessed 19 February 2024].

ISO. (2018) ISO 31000:2018(en) Risk Management - Guidelines. Available from: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en [Accessed 19 February 2024].

ISO. (2022) ISO/IEC 27001:2022(en) Information security, cybersecurity and privacy protection – Information security management systems - Requirements. Available from: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en [Accessed 19 February 2024].

NIST. (2023). National Vulnerability Database. Available from: https://nvd.nist.gov/vuln [Accessed 19 February 2024].

PCI. (2018). PCI DSS v3.2.1 Quick Reference Guide. Available from: https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf [Accessed 19 February 2024].