University of Sunderland

Faculty of Technology

Department of Computer Science

PROJECT PLANNING

PROM02

MSc Dissertation

Academic Year: 2023/24

Student Name: Michael Lawrence Ayodele

Student ID: 239195368

Email: bi51tw@student.sunderland.ac.uk

Programme: Msc Cybersecurity

Mode: Full Time

Supervisor: Matthew Banton

1 Terms of Reference (50%)

1.1 Project Title

The Impact of Cyber Attacks on Cloud Security and Data Privacy (A Practical Analysis)

1.2 Project Overview

Guidance: provide the aim, objectives, research question and practical outcomes of your project:

***Aim**:* To conduct a comprehensive analysis of major privacy and data security threats faced by organizations, understand the motivations and impact of these attacks, and evaluate defensive strategies to mitigate risks.

***Objectives**:*

- Thoroughly review existing literature on privacy and data security breaches, attack vectors, threat actors and defensive controls
- Classify and analyze different types of attacks including cyber attacks, insider threats, social engineering and physical security breaches
- Examine the diverse motivations driving threat actors from financial gain to hacktivism and cyber warfare
- Assess the qualitative and quantitative impacts of data breaches on organizations including financial losses, regulatory penalties and reputational damage
- Evaluate technological solutions like encryption, access controls, intrusion detection as well as policy, training and collaboration-based defenses
- Develop a risk assessment framework tailored to privacy and data security threats
- Provide specific, actionable recommendations for organizations, policymakers and individuals

***Research Question**:* What are the major threats to privacy and data security, what impacts do they have, who are the key threat actors and their motivations, and how can a comprehensive, multi-layered defence strategy mitigate these risks?

***Practical outcomes**:*

- A detailed taxonomy and analysis of prevalent attack vectors and threat actor profiles
- A data breach impact assessment model factoring financial, operational and reputational losses
- A risk scoring methodology for privacy and data security threats
- Recommendations on best-in-class defensive technologies, processes and collaborations
- A roadmap for implementing a robust, defense-in-depth security posture
- A validated and comprehensive taxonomy for classifying and analyzing cyber-attacks on cloud environments, developed through a rigorous process involving literature review, evaluation framework, real-world case study application, and expert feedback.

1.3 Underpinning research with Literature Review

*Guidance: Complete the following table for at least **10 references from research journals and conferences** that will contribute to your work.*

Citation	*Brief summary of paper*	*Relevance to your research question*	*Relevance to practical outcome of project*
Nissenbaum, H., (2018) Respecting context to protect privacy: Why meaning matters. Science and Engineering Ethics, 24(3), pp.831-852.	• Highlights importance of context in privacy • Examines theory of contextual integrity • Notes changing boundaries blur norms	Informs ethical privacy considerations. Relevant to social/ethical issues	Insights help shape privacy-respecting defense recommendations
Bowers, C.B. and Kassen, M.A., (2017) Cyber Defense: An Insider Threat Indicator Stratification Study. Technologies for Homeland Security, p.100.	• Focuses on insider threat indicators. • Analyzes technical and behavioral indicators. • Proposes an indicator stratification model	Highly relevant for understanding insider threat risk factors. Supports insider threat analysis	Practical model can enhance insider threat mitigation strategies
Conheady, B., McReynolds, J., Rrushi, J. and Harber, E., (2018) "Quantifying the Impact from Cyber Attacks," in IEEE Systems, Applications and Technology Conference (LISAT). IEEE.	• Proposes an impact quantification model. • Factors confidentiality, integrity, availability • Provides a scoring methodology	Directly relevant for modeling breach impacts Informs research on impact assessment	Practical model can be adapted/extended for impact analysis
Nurse, J.R., Arief, B., Okholm, A., Milliken, J., Lewis, R. and Wagner, C., (2020) Towards Interpretable and Robust Data Cyber-Resilience using Normative and Descriptive Attack Trees. Cybersecurity, 3(1), pp.1-28.	• Examines attack trees for threat modelling. • Hybrid approach for normative / descriptive trees	Novel methodology for analyzing cyber threats. Relevant for understanding attack vectors	Offers a formalized technique for developing attack taxonomy.

	• Focuses on cyber-resilience applications		
Soomro, Z.A., Shah, M.H. and Ahmed, J., (2016) Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), pp.215-225.	• Highlights need for holistic, multi-layered approach. • Covers people, process and technology aspects. • Emphasizes governance and metrics	Supports addressing defenses from technological, policy and collaboration angles as well as risk quantification	Provides framework for developing comprehensive defense recommendations
Hajli, N. and Lin, X., (2016) Exploring the security of information sharing on social networking sites: The role of perceived control of information. Journal of Business Ethics, 133(1), pp.111-123.	• Examines privacy risks on social media. • Highlights impact of lack of info control • Notes emerging threat from oversharing	Covers emerging attack vector of social media. Relevant to insider and social engineering threats	Informs threat analysis and defensive recommendations for social media risks
Holtfreter, R.E. and Bardwell, M.C., (2017) A Partial Test of Self-Control Theory Among Organizational Cybercrime Offenders. Criminal Justice Studies, 30(4), pp.426-444.	• Examines insider threats. • Applies self-control theory. • Notes lack of deterrence perception	Highly relevant for understanding insider threat motivations. Informs defensive policies and deterrence strategies	Builds on insider threat analysis. Supports insider threat mitigation recommendations
Khan, S.N., (2014) Qualitative study of the impacts of cyber attacks on nations. Global Policy, 5(4), pp.541-549.	• Analyzes national security impacts. • Covers cyberwarfare and espionage.	Key insights into motivations like cyber warfare and sabotage Informs understanding	Supports impact analysis for critical infra breaches. Builds cyber threat defense recommendations.

	• Notes damage due to critical infra attacks	of state-sponsored actors	
Ruan, K., (2013) "Cybercrime and Cloud Forensics: Applications for Investigation Processes," in Proceedings of the 8th International Conference on Security and Cryptography (SECRYPT), pp.1-5.	• Explores forensic techniques in cloud environments. • Highlights challenges in evidence collection. • Proposes a framework for cloud forensics	Directly relevant for forensic analysis in cyber incidents. Supports methodology for evidence gathering	Provides practical guidelines for implementing forensic procedures in cloud infrastructures
Fischer, C., and Swanson, C., (2019) "The Human Element: Reducing Insider Threats through Behavioral Science," in IEEE Security and Privacy, 17(2), pp.62-70.	• Investigates behavioural science approaches to insider threats. • Focuses on human factors and psychology. • Proposes strategies for risk mitigation	Relevant for addressing human element in cyber security. Supports comprehensive insider threat analysis	Offers practical strategies for integrating behavioural science into security protocols

1.3.1 Developing and Validating the Proposed Taxonomy

To develop a robust and comprehensive taxonomy for classifying and analyzing cyber-attacks on cloud environments, the following approach will be undertaken:

a) Conduct a thorough literature review and analysis of existing taxonomies, frameworks, and models for classifying cyber threats and attacks, with a specific focus on their applicability to cloud environments. This will involve identifying their strengths, limitations, and gaps, establishing a solid foundation for the proposed taxonomy.

b) Develop a set of evaluation criteria or framework that assesses the effectiveness and comprehensiveness of the proposed taxonomy. These criteria will consider factors such as coverage of diverse attack vectors, alignment with industry standards, and its ability to support risk assessments and mitigation strategies.

c) Implement the proposed taxonomy by classifying and analyzing a representative set of real-world cyber-attack case studies and simulated scenarios within cloud environments. The practical application will allow for validation and refinement of the taxonomy based on empirical data.

d) Engage subject matter experts and industry professionals for their feedback and evaluation of the proposed taxonomy. Their insights and recommendations will be invaluable in refining and enhancing the taxonomy's practical applicability.

2 Project Schedule (20%)

Guidance: the project schedule should be provided as a series of tables as detailed below.

2.1 Table 1: Effort

Task Id	Task Name	Start	Deadline	Hours	Deliverable
Major Task Name (mapped to objectives / method)					
1.0	Literature review.	07/06/2024	17/06/2024	120	D1.1 Annotated Bibliography D1.2 Literature Review Draft
1.1	Search for data security publications	07/06/2024	09/06/2024	25	
1.2	Search for privacy breach research	10/06/2024	11/06/2024	25	
1.3	Review and annotate key publications	12/06/2024	14/06/2024	50	D1.1 Annotated Bibliography
1.4	Synthesize literature findings	14/06/2024	15/06/2024	20	
1.5	Write and revise literature review draft	17/06/2024	17/06/2024	30	D1.2 Literature Review Draft
Major Task Name (mapped to objectives / method)					
2.0	Research Methodology	18/06/2024	26/06/2024	60	D2.1 Methodology Section Draft
2.1	Evaluate potential research approaches	18/06/2024	19/06/2024	15	
2.2	Define specific methods	20/06/2024	22/06/2024	20	
2.3	Plan for data collection and analysis	23/06/2024	24/06/2024	15	
2.4	Consider ethical implications	25/06/2024	25/06/2024	20	
2.5	Document limitations and delimitations	26/06/2024	26/06/2024	10	
2.6	Write methodology section draft	26/06/2024	26/06/2024	20	D2.1 Methodology Draft
3.0	Data Collection and Analysis	25/06/2024	22/07/2024	200	D3.1 Attack Taxonomy D3.2 Threat Actor Profiles

					D3.3 Impact Analysis D3.4 Defense Evaluation
3.1	Research attack types and examples	27/06/2024	04/07/2024	60	D3.1 Attack Taxonomy
3.2	Investigate threat actor motivations	05/06/2024	10/07/2024	40	D3.2 Threat Actor Profiles
3.3	Conduct breach impact assessment	11/07/2024	16/07/2024	60	D3.3 Impact Analysis
3.4	Evaluate defensive control effectiveness	17/07/2024	17/07/2024	40	D3.4 Defence Evaluation
3.5	Develop taxonomy evaluation criteria and framework	11/07/2024	16/07/2024	20	D3.5 Taxonomy Evaluation Framework
4.0	Writing & Integration	23/07/2024	29/07/2024	220	D4.1 Complete Draft D4.2 Final Thesis
4.1	Write introduction, conclusion chapters	23/07/2024	24/07/2024	40	
4.2	Write attack types of chapters	25/07/2024	26/07/2024	40	
4.3	Write threat actor motivations chapter	28/07/2024	27/07/2024	20	
4.4	Write breach impacts chapter	23/07/2024	25/07/2024	40	
4.5	Write defensive strategies chapter	23/07/2024	28/07/2024	40	
4.6	Integration and revision	23/07/2024	29/07/2024	60	D4.1 Complete Draft
4.7	Final formatting and submission prep	23/07/2024	29/07/2024	20	D4.2 Final Thesis

2.2 Table 2: Deliverables

Del. No.	Name	Deadline
D1.1	Annotated Bibliography	14/06/2024
D1.2	Literature Review Draft	17/06/2024
D2.1	Methodology Section Draft	26/06/2024
D3.1	Attack Taxonomy	04/07/2024
D3.2	Threat Actor Profiles	10/07/2024
D3.3	Impact Analysis	16/07/2024
D3.4	Defense Evaluation	22/07/2024
D4.1	Complete Draft	29/07/2024
D4.2	Final Thesis	29/07/2024

2.3 Table 3: Milestones

Milestone	Name	Deadline	Evidence
M1	Literature Review Complete	17/06/2024	D1.2 Literature Review Draft deliverable

M2	Research Methodology Defined	26/06/2024	D2.1 Methodology Section Draft
M3	Data Collection and Analysis Complete	22/07/2024	D3.1, D3.2, D3.3, D3.4 deliverables
M4	First Complete Draft	29/07/2024	D4.1 Complete Draft deliverable
M5	Dissertation Writing Complete	29/07/2024	D4.2: Final Dissertation

2.4 Table 4: Outline Schedule / Gantt chart

	June				July				August				September		
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Literature Review							T1.0 T1.1	🟦	🟦	T1.2	🟦	T1.3	🟦	D1.1	T1.4
Methodology															
Data Collection and Analysis	🟧	🟧	🟧	D3.1	🟧	🟧	🟧	🟧	🟧	D3.2	T3.3 T3.5	🟧	🟧	🟧	🟧
Dissertation Writing & Integration															

	June				July				August				September		
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Literature Review	🟦	MS1 T1.5 D1.2													
Methodology			T2.0 T2.1	🟦	T2.2	🟦	🟦	T2.3	🟦	T2.4	MS2 T2.5 D2.1				
Data Collection and Analysis	🟧	D3.3 T3.4	🟧	🟧	🟧	🟧	D3.4 M3			T3.0	🟦	T3.1			
Dissertation Writing & Integration								T4.0 T4.1 T4.4 T4.5 T4.6 T4.7	🟧	T4.2	🟧	🟧	T4.3	M4 D4.1 D4.2	

3 Evaluation Plan (10%)

Guidance: Complete the following table - one page maximum.

Objective	Evaluation Approach	Evidence
Thoroughly review existing literature on privacy and data security breaches, attack vectors, threat actors and defensive controls	Conduct a structured, comprehensive review following best practices for literature reviews in cybersecurity.	D1.1 Annotated Bibliography D1.2 Literature Review Draft
Classify and analyse different types of attacks including cyber-attacks, insider threats, social engineering, and physical security breaches	Research and document prevalent attack types, techniques, and real-world examples through reliable sources	D3.1 Attack Taxonomy
Examine the diverse motivations driving threat actors from financial gain to hacktivism and cyber warfare	Investigate actor profiles and motivations behind major breaches and attacks reported in the media and research publications	D3.2 Threat Actor Profiles
Assess the qualitative and quantitative impacts of data breaches on organizations including financial losses, regulatory penalties, and reputational damage	Review documented breach impacts from reports, databases and construct an impact assessment model	D3.3 Impact Analysis
Evaluate technological solutions like encryption, access controls, intrusion detection as well as policy, training, and collaboration-based defenses	Critically analyze existing defensive controls and strategies based on their effectiveness reported in literature	D3.4 Defense Evaluation
Develop a risk assessment framework tailored to privacy and data security threats	Synthesize findings into a holistic risk framework factoring threat likelihood and potential impacts	Chapter content on risk analysis
Provide recommendations for organizations, policymakers, and individuals	Based on research insights, prescribe actionable recommendations for a robust security posture covering people, process & technology aspects	Chapter 8 conclusions and recommendations

4 Social, Ethical, Legal and Professional issues (20%)

4.1 Social, Ethical, Legal and Professional Issues Table

Social issues	Privacy and data breaches can significantly impact individuals, causing issues like identity theft, financial fraud, personal data exposure and loss of trust in institutions. Understanding and mitigating these threats is a key societal need.
Ethical issues	Evaluating defensive technologies, policies and processes needs to factor in ethical considerations like user privacy,

	consent, data collection practices, surveillance concerns and ethical/acceptable use boundaries for certain controls.
Professional issues	For cybersecurity and privacy professionals, the research highlights critical knowledge needs around emerging threats, risks, and proven defensive strategies to adequately protect systems and data. It can guide professional development and best practices.
Legal Issues	The research needs to account for data protection regulations like GDPR as well as laws around cybercrime, identity theft, computer misuse and any sector-specific compliance mandates that organizations need to follow.

4.2 Ethics Approval

No primary research involving human participants is planned as part of this thesis. If the research direction changes to involve any human participants, ethics approval will be sought from the university ethics committee beforehand.

5 Appendices

Risk Management Plan			
Risk Description	**Probability**	**Impact**	**Mitigation Strategy**
Difficulty in obtaining relevant data on cyber-attacks, breaches, or defensive controls	Medium	High	• Identify multiple potential data sources early (research databases, breach reports, security communities) • Establish relationships with organizations/experts who can provide data. • Utilize publicly available datasets and case studies
Challenges in recruitment for data collection methods like interviews or surveys (if applicable)	Medium	High	• Develop a thorough recruitment plan targeting cybersecurity professionals/organizations. • Offer participation incentives if feasible and leverage existing networks, contacts, and professional groups
Delays in literature review, data analysis or writing phases	Medium	Medium	• Allocate sufficient time for these critical tasks in the schedule. • Regularly monitor progress and adjust timelines as needed. • Seek guidance from supervisor or subject matter experts
Limitations in developing risk models, frameworks, or analysis methods	Low	High	• Conduct thorough planning of technical/analytical requirements early. • Allocate adequate time for model development and testing. • Seek technical guidance or expertise if issues arise. • Adjust scope of frameworks if necessary
Unforeseen circumstances like illness, equipment issues	Low	Medium	• Build contingency buffers into the project schedule. • Maintain regular backups and documentation

Resource Management Plan		
Resource Type	**Resource Description**	**Acquisition Strategy**
Personnel	Primary Researcher (**Michael Lawrence**)	N/A
Supervisor	**Matthew Banton**	
Subject Matter Experts	Identification and collaboration of relevant experts in the field.	
Equipment	Laptop or Desktop Computers.	Utilize personal or University-provided equipment.
Data Storage Devices (e.g., external drves)	Purchase or utilize existing resources	
Software	Qualitative Data Analysis (e.g., NVivo, ATLAS)	Utilize university-provided software or open-source alternatives.
Quantitative Data Analysis Software (e.g., SPDD, R)	Utilize university-provided software or open-source alternatives.	
Prototyping/Development Tools (e.g., IDE's frameworks)	Utilize open source of existing resources	
Facilities	Workspace (e.g., library,office).	Utilize university-provided facilities.
Meeting Rooms (for data collections, presentations).	Reserve university facilities as needed.	
Other Resources	Online Research Databases and Journals publications.	Utilize university subscriptions and library resources.
Reference Management Software (e.g., Mendeley, Zotero)	Utilize open-source or existing resources.	

Communication Plan			
Stakeholder	**Communication Channel**	**Frequency**	**Purpose**
Supervisor	In-person Meetings	Bi-weekly or as needed	Progress updates, guidance, feedback
Email	As needed	Quick queries, sharing documents	
Data Collection Participants	Email, Online Surveys	As needed	Seeking expertise, guidance, feedback
Subject Matter Experts	Email, Video Conferences	As needed	Seeking expertise,

			guidance, feedback
University Administration	Email	As needed	Administrative queries, approvals

Reference:

- Nissenbaum, H., (2018). Respecting context to protect privacy: Why meaning matters. Science and Engineering Ethics, 24(3), pp.831-852.
- Bowers, C.B. and Kassen, M.A., (2017). Cyber Defense: An Insider Threat Indicator Stratification Study. Technologies for Homeland Security, p.100.
- Conheady, B., McReynolds, J., Rrushi, J. and Harber, E., (2018). "Quantifying the Impact from Cyber Attacks," in IEEE Systems, Applications and Technology Conference (LISAT). IEEE.
- Nurse, J.R., Arief, B., Okholm, A., Milliken, J., Lewis, R. and Wagner, C., (2020). Towards Interpretable and Robust Data Cyber-Resilience using Normative and Descriptive Attack Trees. Cybersecurity, 3(1), pp.1-28.
- Soomro, Z.A., Shah, M.H. and Ahmed, J., (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), pp.215-225.
- Hajli, N. and Lin, X., (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. Journal of Business Ethics, 133(1), pp.111-123.
- Holtfreter, R.E. and Bardwell, M.C., (2017). A Partial Test of Self-Control Theory Among Organizational Cybercrime Offenders. Criminal Justice Studies, 30(4), pp.426-444.
- Khan, S.N., (2014). Qualitative study of the impacts of cyber attacks on nations. Global Policy, 5(4), pp.541-549.
- Ruan, K., (2013). "Cybercrime and Cloud Forensics: Applications for Investigation Processes," in Proceedings of the 8th International Conference on Security and Cryptography (SECRYPT), pp.1-5.
- Fischer, C., and Swanson, C., (2019). "The Human Element: Reducing Insider Threats through Behavioral Science," in IEEE Security and Privacy, 17(2), pp.62-70.