IMSISS Dissertation Feedback & Mark Sheet

Student Matriculation No.	**Glasgow** 2781162 **DCU** **Charles** 10880793 **Trento** 241420
Dissertation Title	CyberHunter: Preventive Framework Development for Data Breaches Using Routine Activity Theory

INDIVIDUAL INSTITUTION GRADING

		Late Submission Penalty *no penalty*
Word Count Penalty *(1-15% over/under = 1gr point; 15-20% over/under = 2 gr points; 20-25% over/under = 3 gr points; more than 25% over/under = 0 fail)* ***Word Count:*** 22.350 ***Suggested Penalty:*** *no penalty*		

JOINT GRADING (subject to agreement of the external examiner and approval at Joint Exam Board)

Final Agreed Mark. *(Following correspondence reviewers should list the agreed final internal grade taking before and after any penalties to be applied).*

Before Penalty: A3 [20] ***After Penalty:*** A3 [20]

DISSERTATION FEEDBACK

Assessment Criteria	***Rating***
A. Structure and Development of Answer This refers to your organisational skills and ability to construct an argument in a coherent and original manner	
• *Originality of topic*	Excellent
• *Coherent set of research questions and/or hypothesis identified*	Excellent
• *Appropriate methodology and evidence of effective organisation of work*	Excellent
• *Logically structured argument and flow of ideas reflecting research questions*	Very Good
• *Application of theory and/or concepts*	Very Good
B. Use of Source Material This refers to your skills to select and use relevant information and data in a correct manner	
• *Evidence of reading and review of published literature*	Very Good
• *Selection of relevant primary and/or secondary evidence to support argument*	Excellent
• *Critical analysis and evaluation of evidence*	Very Good
• *Accuracy of factual data*	Excellent
C. Academic Style This refers to your ability to write in a formal academic manner	
• *Appropriate formal and clear writing style*	Very Good
• *Accurate spelling, grammar and punctuation*	Excellent
• *Consistent and accurate referencing (including complete bibliography)*	Excellent
• *Is the dissertation free from plagiarism?*	Yes

IMSISS Dissertation Feedback & Mark Sheet

• *Evidence of ethics approval included (if required based on methodology)*	Not required
• *Appropriate word count*	Yes

ADDITIONAL WRITTEN COMMENTS

Reviewer 1

The present paper offers an interesting synthesis of criminological approaches and strategies in the field of cyber security. Specifically, it aims to show the potential of Routine Activity Theory to predict data breaches. I find the idea itself very original and interesting. It confirms the apparent trend of focusing on the "soft" or societal aspects of cybersecurity. The paper draws appropriately on existing disciplinary literature. However, its focus is methodological, where, in an analogy to the machine learning process, the authors test selected variables on past (training) cases. That said, the methodological implementation itself is very convincing. The variables are clearly operationalized and allow individual cases to be evaluated. Given the interdisciplinary synthesis that I indeed appreciate, the paper should also pay some attention to the limits of the given approach. All in all, this is an orginial and well-thought paper that fulfills its goals as well as high academic standards.

Reviewer 2

This dissertation offers a novel and interdisciplinary examination of data breaches within the cybersecurity landscape, using Routine Activity Theory (RAT) as its foundation. The structure of the thesis is very well organised, beginning with a thorough literature review, progressing through a detailed exposition of the conceptual framework, and concluding with the practical application and empirical testing of the proposed model. The methodology used is robust. It integrates an exhaustive review of existing literature, rigorous data collection from credible sources, and the implementation of artificial intelligence and machine learning (AI/ML) techniques to develop and evaluate the predictive model. This approach ensures that the framework is grounded in both strong theoretical underpinnings and empirical research, lending credibility to its findings.

However, there are challenges in applying criminological concepts to the cyber domain. Routine Activity Theory was originally developed to address physical crime, and its translation to the digital domain may not fully capture the multifaceted nature of cybercrime.

Certainly, the interdisciplinary approach enriches the study by bringing together human and technical perspectives in cybersecurity, but maintaining theoretical coherence across different fields is a significant challenge: adapting RAT elements to the cyber context is an ambitious endeavour.

This thesis represents a significant and commendable effort to bridge the disciplines of criminology and cybersecurity.