

**ENTERPRISE CYBERSECURITY RISK ASSESSMENT WITH THREAT  
MODELING: CASE STUDY XYZ INSURANCE COMPANY**

By

**BINTANG RAMDHANI  
2-1851-011**

**MASTER'S DEGREE  
in**

**MASTER OF INFORMATION TECHNOLOGY  
ENGINEERING AND INFORMATION TECHNOLOGY FACULTY**

**SWISS GERMAN UNIVERSITY**

**SWISS GERMAN UNIVERSITY  
The Prominence Tower  
Jalan Jalur Sutera Barat No. 15, Alam Sutera  
Tangerang, Banten 15143 - Indonesia**

**August 2021**

**Revision after Thesis Defense on 30 July 2021**

## STATEMENT BY THE AUTHOR

I hereby declare that this submission is my work and to the best of my knowledge, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgement is made in the thesis.

Bintang Ramdhani

Student

Date

Approved by:

Dr. Ir. Mohammad Achmad Amin Soetomo, M.Sc.

Thesis Advisor

Date

Dr. Charles Lim B.Sc. M.Sc.

Thesis Co-Advisor

Date

Dr. Maulahikmah Galinium, S.Kom, M.Sc.

Dean

Date

Bintang Ramdhani

## ABSTRACT

### ENTERPRISE CYBERSECURITY RISK ASSESSMENT WITH THREAT MODELING: CASE STUDY XYZ INSURANCE COMPANY

By

Bintang Ramdhani  
Dr. Ir. Mohammad Achmad Amin Soetomo. M.Sc.  
Dr. Charles Lim B.Sc. M.Sc.

SWISS GERMAN UNIVERSITY

XYZ Insurance is a company that always try to meet the needs of its customers, one of the customer's needs during this pandemic is health services, therefore, XYZ insurance develops a telemedicine application. In order to ensure the reliable operation of the application, it is necessary to pay attention to the security issues for the application. To overcome security problems. In this research, a risk assessment is carried out using threat modeling with STRIDE, where Data Flow Diagrams (DFD) is the main input, its help identifies and differentiate existing threats, researcher found 40 threats on telemedicine application, where these threats are in process as many as 28 threats, data flow as many as 8 threats, and data store as 4 threats.

Meanwhile, to measure the identified threat, researcher used DREAD to get threat score and CVSS to get vulnerability score. From the results of that threats and vulnerabilities, a risk value is obtained, where in this telemedicine application there are 2 very high risks, there are on the webserver process - SQL Injection and Directory traversal. By knowing the risks that exist, the appropriate controls to mitigate these risks are recommended.

*Keywords: Threat Modeling, Risk Assessment, DFD, STRIDE, DREAD, CVSS.*



## DEDICATION

I dedicate this works for the future of the country I loved: Indonesia  
and  
my beloved family

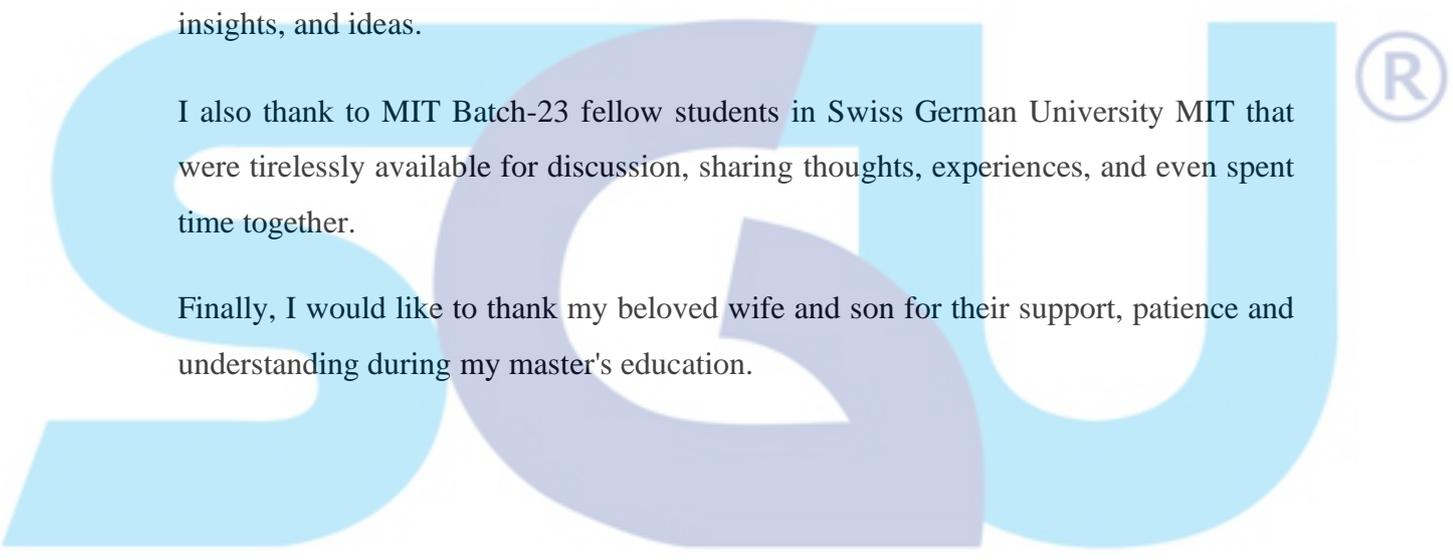


## ACKNOWLEDGEMENTS

I wish to thank Dr. Ir. Moh. A. Amin Soetomo, M.Sc, as my Thesis Advisor for his time and advice, and suggestions, and Dr. Charles Lim, BSc., MSc., CTIA, CHFI, EDRP, ECSA, ECSP, ECIH, CEH, CEI my Thesis Co-Advisor or his time, advice, guidance, insights, and ideas.

I also thank to MIT Batch-23 fellow students in Swiss German University MIT that were tirelessly available for discussion, sharing thoughts, experiences, and even spent time together.

Finally, I would like to thank my beloved wife and son for their support, patience and understanding during my master's education.



SWISS GERMAN UNIVERSITY

## Table of Contents

|   | Page |
|---|------|
| STATEMENT BY THE AUTHOR.....                                  | 2    |
| ABSTRACT.....   | 3    |
| DEDICATION.....   | 5    |
| ACKNOWLEDGEMENTS.....   | 6    |
| Table of Contents.....  | 7    |
| LIST OF FIGURES.....  | 10   |
| LIST OF TABLES.....   | 11   |
| CHAPTER 1 - INTRODUCTION.....                                 | 12   |
| 1.1 Background.....   | 12   |
| 1.2 Research Problems.....                                    | 13   |
| 1.3 Research Objectives.....                                  | 13   |
| 1.4 Research Questions.....                                   | 13   |
| 1.5 Significance of Study.....                                | 13   |
| 1.6 Scope.....  | 14   |
| 1.7 Limitations.....  | 14   |
| 1.8 Hypothesis.....   | 14   |
| 1.9 Thesis Structure.....                                     | 14   |
| CHAPTER 2 - LITERATURE REVIEW.....                            | 15   |
| 2.1 Insurance.....  | 15   |
| 2.2 Security attributes.....                                  | 16   |
| 2.2.1 Assets.....   | 16   |
| 2.2.2 Threat.....   | 16   |
| 2.2.3 Vulnerability.....                                      | 16   |
| 2.2.4 Risk.....   | 17   |
| 2.3 Information Security Principles.....                      | 17   |
| 2.3.1 Confidentiality.....                                    | 17   |
| 2.3.2 Integrity.....  | 18   |
| 2.3.3 Availability.....                                       | 18   |
| 2.4 OJK Regulation.....                                       | 18   |
| 2.5 Framework for Risk Management.....                        | 19   |
| 2.5.1 NIST 800:30 r1.....                                     | 19   |
| 2.5.2 ISO/IEC 31000 – Risk Management Guidelines.....         | 20   |
| 2.5.3 ISO/IEC 27005 Information security risk management..... | 21   |
| 2.6 Threat Modeling.....                                      | 22   |
| 2.6.1 Threat Modeling Approach.....                           | 22   |
| 2.6.1.1 Attack-Centric.....                                   | 22   |
| 2.6.1.2 Asset-Centric.....                                    | 23   |

|  |   |     |
|--|---|-----|
| 2.6.2  | Threat Modeling Framework .....             | 24  |
| 2.6.2.1  | STRIDE.....                                 | 24  |
| 2.6.2.2  | Attack Tree.....                            | 27  |
| 2.6.2.3  | Trike .....                                 | 28  |
| 2.6.2.4  | OCTAVE .....                                | 29  |
| 2.6.2.5  | PASTA.....                                  | 29  |
| 2.6.3  | DREAD & CVSS Scoring .....                  | 30  |
| 2.6.3.1  | DREAD.....                                  | 31  |
| 2.6.3.2  | CVSS.....                                   | 32  |
| 2.7  | Related Work .....                          | 35  |
| CHAPTER 3 - RESEARCH METHODS.....                |   | 38  |
| 3.1  | Research Methodology .....                  | 38  |
| 3.2  | Research Framework.....                     | 40  |
| CHAPTER 4 - RESULTS AND DISCUSSIONS .....        |   | 45  |
| 4.1  | Data Collection .....                       | 45  |
| 4.1.1  | Investigation.....                          | 45  |
| 4.1.2  | Analysis.....                               | 45  |
| 4.1.3  | Document Review.....                        | 45  |
| 4.2  | Decompose Application.....                  | 45  |
| 4.3  | Threat & Vulnerability Identification ..... | 48  |
| 4.3.1  | Threat Identification.....                  | 48  |
| 4.3.2  | Vulnerability Identification.....           | 52  |
| 4.4  | Threat & Vulnerability Scoring .....        | 53  |
| 4.4.1  | Threat Scoring.....                         | 53  |
| 4.4.2  | Vulnerability Scoring.....                  | 54  |
| 4.5  | Risk Measurement.....                       | 55  |
| 4.6  | External Pentest.....                       | 58  |
| 4.7  | Risk Control.....                           | 59  |
| 4.8  | Validation.....                             | 60  |
| CHAPTER 5 - CONCLUSIONS AND RECOMMENDATIONS..... |   | 62  |
| 5.1  | Conclusions.....                            | 62  |
| 5.2  | Recommendations.....                        | 63  |
| 5.3  | Future Work .....                           | 63  |
| GLOSSARY.....                                    |   | 64  |
| APPENDIX A.....                                  |   | 70  |
| APPENDIX B .....                                 |   | 72  |
| APPENDIX C .....                                 |   | 76  |
| APPENDIX D.....                                  |   | 82  |
| APPENDIX E .....                                 |   | 94  |
| APPENDIX F.....                                  |   | 96  |
| APPENDIX G.....                                  |   | 98  |
| REFERENCES.....                                  |   | 102 |



## LIST OF FIGURES

| Figures   | Page |
|---|------|
| 2.1 - Information Security Principles.....      | 17   |
| 2.2 - NIST 800-30 Risk Assessment Process ..... | 20   |
| 2.3 - ISO 31000 Process .....                   | 21   |
| 2.4 - ISO 27005 Process .....                   | 22   |
| 2.5 - Attack Tree .....                         | 28   |
| 3.1 - Stage Of The Research Process .....       | 38   |
| 3.2 - The Risk Management Process .....         | 40   |
| 3.3 - Proposed Research Framework .....         | 41   |
| 4.1 - Data Flow Diagram Telemedicine.....       | 46   |

SWISS GERMAN UNIVERSITY

## LIST OF TABLES

| Table  | Page |
|--|------|
| 2.1 - Stride.....                                  | 25   |
| 2.2 - Stride Classification Model .....            | 27   |
| 2.3 - Comparison Threat Modelling .....            | 30   |
| 2.4 - Threat Scoring Dread .....                   | 31   |
| 2.5 - Total Threat Scoring Dread .....             | 32   |
| 2.6 - Related Work.....                            | 36   |
| 3.1 - Input Process Output Map To Iso 27005.....   | 41   |
| 4.1 - Data Flow Diagram Information .....          | 46   |
| 4.2 - Data Flow Diagram Telemedicine Process ..... | 47   |
| 4.3 - Security Conditions .....                    | 49   |
| 4.4 - Mapping Dfd With Stride.....                 | 49   |
| 4.5 - Summary Threat List Stride .....             | 50   |
| 4.6 - Mapping Threat To Vulnerability .....        | 52   |
| 4.7 - Risks Rating With Dread.....                 | 53   |
| 4.8 - Vulnerability Scoring .....                  | 55   |
| 4.9 - Risk Matrix .....                            | 56   |
| 4.10 - Risk Scoring .....                          | 56   |
| 4.11 - Risk Mitigation.....                        | 59   |