CYBER SECURITY CAPABILITY MATURITY MODEL

USING MAQASID AL-SHARI‘AH APPROACH

BY

NADWIYAH BINTI MOHAMED RIDZA

A thesis submitted in fulfilment of the requirement for the degree of Master of Computer Science

Kulliyyah of Information and Communication Technology (KICT)
International Islamic University Malaysia

FEBRUARY 2020

ABSTRACT

Knowing how vulnerable an organisation or a country is towards cyberattacks, is referred to as Cyber Security Index or Maturity Level. Such an index is important to evaluate one's level of vulnerability to cyber threats and its defense readiness. Various cyber security models are initiated and applied across the globe as tools towards measuring the mentioned index. These models in particular provide us with indicators as to how ready an organisation or a country react to attacks and what are the steps to be taken to alleviate the situation. However, although most of the existing cyber security models excel in determining one's cyber security maturity level, the results produced only indicated the degree of practice based on the evidence presented by a country or an organisation for each criterion underlined in each model. It stops short from further explaining what the fundamental problem is: the human factor. Human beings play a very important role in cyber security. Unlike policy, technology and process which are deterministic in nature, human beings are by nature random and complex. Consequently, this unpredictive nature of people and morality issue causes humans to be regarded as the major factor affecting the level of cyber security readiness. Maqasid Al-Shari'ah supports the objectives of Shari'ah through the preservation of five elements: (1) Protection of Deen (faith), (2) Protection of Nafs (life), (3) Protection of 'Aql (intellect), (4) Protection of Nasl (lineage) and (5) Protection of Mal (wealth). Preservation of these five elements is significant for cyber security maturity. Therefore, this research is proposing the use of Maqasid Al-Shari'ah to address the human factor centred on morality as described above. Results will be categorised into the aforementioned five elements. Based on this approach, an organisation will not only be able to determine its maturity level, but interestingly the result will reveal to what extent the organisation's decision making to protect its assets comply with Islamic morality. This work aims to develop a Cyber security Capability Maturity Model guided by Maqasid Al-Shari'ah (known as MS-C2M2) which comprehensively covers both moral and physical aspects of human beings. Its success will undoubtedly demonstrate the usefulness of Maqasid Al-Shari'ah principle, as well as benefiting cyber security maturity models. The MS-C2M2 will be manifested through the development of a prototype system known as Maqasid al Shari'ah Cyber Security Barometer that captures organisations' input which later produces the corresponding cyber security maturity levels. A few subject matter experts in both areas i.e. Cyber security and Maqasid Al-Shari'ah were referred to, to evaluate and validate the reliability of the prototype's content and functionality. After being validated, eighteen organisations from various industries and backgrounds were approached to test the prototype tool. However, only three organisations had gotten back and participated. Coincidentally, the participating organisations were those with good cyber security readiness. For the purpose of comparison, two additional mock organisations were created with poor performances (after going through the barometer) to give ideas on what results do organisations with poor cyber security readiness produced. The feedback received from the survey circulated afterwards showed that the respondents are satisfied with the results produced by the Maqasid al Shari'ah Cyber Security Barometer.

خلاصة البحث

يُشار إلى معرفة مدى تأثر أي منظمة أو بلد بالهجمات الإلكترونية ، كمؤشر أمان الإنترنت أو مستوى النضج. مثل هذا الفهرس مهم لتقييم مستوى تعرض الفرد للتهديدات السيبرانية واستعداده للدفاع. يتم إطلاق نماذج أمان الإنترنت المختلفة وتطبيقها في جميع أنحاء العالم كأدوات لقياس الفهرس المذكور. تزودنا هذه النماذج على وجه الخصوص بمؤشرات حول مدى استعداد منظمة أو دولة للرد على الهجمات وما هي الخطوات التي يجب اتخاذها لتخفيف الضرر من هذه الهجمات. ومع ذلك ، على الرغم من أن معظم نماذج الأمن السيبراني الحالية تتفوق في تحديد مستوى نضج الأمن السيبراني ، فإن النتائج التي تم الحصول عليها تشير فقط إلى درجة الممارسة القائمة على الأدلة المقدمة من بلد أو مؤسسة لكل معيار تم التأكيد عليه في كل نموذج . توقف – باختصار- عن شرح المشكلة الأساسية: هو العامل البشري. يلعب البشر دوراً مهماً جداً في مجال الأمن السيبراني. على عكس السياسة والتكنولوجيا والعملية الحتمية في الطبيعة ، فإن البشر بطبيعتهم عشوائيون ومعقدون. وبالتالي ، فإن هذه الطبيعة غير المتوقعة للأشخاص وقضية الأخلاق تجعل البشر يعتبرون العامل الرئيسي الذي يؤثر على مستوى استعداد الأمن السيبراني. يدعم "مقاصد الشريعة" أهداف الشريعة من خلال الحفاظ على خمسة عناصر: (1) حماية الدين ، (2) حماية النفس، (3) حماية العقل ، (4) حماية النسل (5) حماية المال. الحفاظ على هذه العناصر الخمسة مهم لنضج الأمن السيبراني .لذلك ، يقترح هذا البحث استخدام مقاصد الشريعة لمعالجة العامل البشري المتمركز حول الأخلاق كما هو موضح أعلاه. سيتم تصنيف النتائج في العناصر الخمسة المذكورة أعلاه. بناءً على هذا النهج ، لن تكون المنظمة قادرة على تحديد مستوى نضجها فحسب ، ولكن المثير للاهتمام أن النتيجة ستكشف إلى أي مدى يتوافق قرار المنظمة لحماية أصولها مع الأخلاق الإسلامية. يهدف هذا العمل إلى تطوير نموذج نضج القدرة على الأمن السيبراني يسترشد بمقاصد الشريعة (المعروفة باسم-MS C2M2) والتي تغطي بشكل شامل الجوانب المعنوية والمادية للبشر. مما لا شك فيه أن نجاحها سوف يُظهر فوائد لمبادئ المقاصد الشرعية ، وكذلك الاستفادة من نماذج نضج الأمن السيبراني. سوف يتجلى نموذج MS-C2M2 من خلال تطوير نظام نموذجي أولي يعرف باسم مقاصد الشريعة للأمن السيبراني الذي يلتقط مدخلات المنظمات التي تنتج فيما بعد مستويات نضج الأمن السيبراني. تمت الإشارة إلى عدد قليل من خبراء الموضوعات في كلا المجالين ، أي الأمن السيبراني ومقاصد الشريعة ، لتقييم وموثوقية محتوى النموذج الأولي ووظائفه. بعد التحقق من صحتها ، تم الاتصال بثمانية عشر منظمة من مختلف الصناعات والخلفيات لاختبار أداة النموذج الأولي. ومع ذلك ، فإن ثلاث منظمات فقط قد عادت وشاركت. من قبيل الصدفة ، كانت المنظمات المشاركة هي تلك التي لديها استعداد جيد للأمن السيبراني. لغرض المقارنة ، تم إنشاء منظمتين وهميتين إضافيتين بأداء ضعيف (بعد المرور بالمقياس) لإعطاء أفكار حول النتائج التي تنتجها المؤسسات ذات الاستعداد السيئ للأمن السيبراني. أظهرت التعليقات التي تم تلقيها من الاستطلاع الذي تم توزيعه بعد ذلك أن المشاركين راضون عن النتائج التي تم الحصول عليها من مقاييس الأمن الشرعي في مقاصد الشريعة.

APPROVAL PAGE

I certify that I have supervised and read this study and that in my opinion, it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a thesis for the degree of Master of Computer Science.

……..
Normaziah Binti Abdul Aziz
Supervisor

……..
Aznan Zuhid Bin Saidin
Co-Supervisor

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a thesis for the degree of Master of Computer Science.

……..
Noor Hasrul Nizan Bin
Mohammad Noor
Internal Examiner

……..
Omar Bin Zakaria
External Examiner

This thesis was submitted to the Department of Computer Science and is accepted as a fulfilment of the requirement for the degree of Master of Computer Science.

……..
Raini Binti Hassan
Head, Department of Computer Science

This thesis was submitted to the Kulliyyah of Information and Communication Technology (KICT) and is accepted as a fulfilment of the requirement for the degree of Master of Computer Science.

……..
Abdul Wahab Bin Abdul Rahman
Dean, Kulliyyah of Information and Communication Technology (KICT)

DECLARATION

I hereby declare that this thesis is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Nadwiyah binti Mohamed Ridza

Signature ..... Date .....

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

CYBER SECURITY CAPABILITY MATURITY MODEL USING MAQASID AL-SHARI'AH APPROACH

I declare that the copyright holders of this thesis are jointly owned by the student and IIUM.

By signing this form, I acknowledged that I have read and understand the IIUM Intellectual Property Right and Commercialization policy.

Affirmed by Nadwiyah binti Mohamed Ridza

……..…….. ……..
Signature Date

This thesis is dedicated to my parents

Mohamed Ridza and Latifah.

Thank you for supporting and believing in me.

Alhamdulillah, I did it!

ACKNOWLEDGEMENTS

First and foremost, I express my gratitude to Allah s.w.t for through His blessings I managed to complete this Thesis.

My utmost appreciation to my principal supervisor Dr. Normaziah binti Abdul Aziz and co-supervisor Dr. Aznan Zuhid bin Saidin for their continuous guidance and supervision. Thank you also to my parents (Mohamed Ridza & Latifah), close family (siblings Sulaiman and Nasuha; sister-in-law Nurul ‘Amirah; nephews Naqib Rayyan, Naufal Rifqi, Najmi Rayqal and grandmother Halijah) and friends (Siti Aisyah Ismail and Narieta Bukhari) for being there for me.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ASPI	Australian Strategic Policy Institute
BSA	Business Software Alliance
C2M2	Cyber security Capability Maturity Model
CI	Critical Infrastructure
CIO	Chief Information Officer
CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integrated
CRI	Cyber Readiness Index
DMO	Destination Management Organisation
DOS	Denial-of-Service
eTcoMM	eTourism Communication Maturity Model
GCI	Global Cybersecurity Index
GDP	Gross domestic products
HTTPS	Hyper Text Transfer Protocol Secure
IIUM	International Islamic University Malaysia
ISMS	Information Security Management System
ITU	International Telecommunication Union
MCMC	Malaysian Communications and Multimedia Commission
MMO	Massively Multiplayer Online
MS-C2M2	Cyber security Capability Maturity Model guided by Maqasid Al-Shari‘ah
MyCERT	The Malaysian Emergency Response Team
NAO	National Audit Office
NSA	National Security Agency
NACSA	National Cyber Security Agency
NGO	Non-Governmental Organisation
NHS	National Health Service
NIST	National Institute of Standards and Technology
PDPA	Personal Data Protection Act
PHP	Hypertext Preprocessor (A Programming Language)
R&D	Research and Development
SEI	Software Engineering Institute
SOP	Standard Operating Procedure
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
WEF	World Economic Forum

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND

1.1.1 The Need for Cyber security

Cyber security is a term referring to efforts and counter measures used to safeguard and protect cyber users as well as their data and work from criminal hackers (Stallings & Brown, 2012). This is undeniably important especially in an era where most of our work and assets are carried out in the cyber world using latest technologies that the world has to offer. In any security matters, threats that relate to the asset to be protected, are a major concern. Threats are anything or anyone that can bring harm to our assets (Stallings & Brown, 2012).

In the 14th edition Global Risks Report 2019, an annual initiative done by World Economic Forum (WEF), it was found that cyberattacks were among the top 10 risks in term of its likelihood to harm us and our assets as well as its impact (Collins, 2019). Likelihood here refers to the chances or probability that a risky incident (as defined by WEF) to occur in our everyday life and impact refers to how severe the effects are. Both are measured in the scale of 1 to 5 which the latter indicates the highest probability or severity. See Figure 1.1. Cyberattacks (the one circled in red) was ranked number 5 and 7 in terms of its likelihood and impact respectively. This signifies the need to address the risk with high importance, and not lightly.

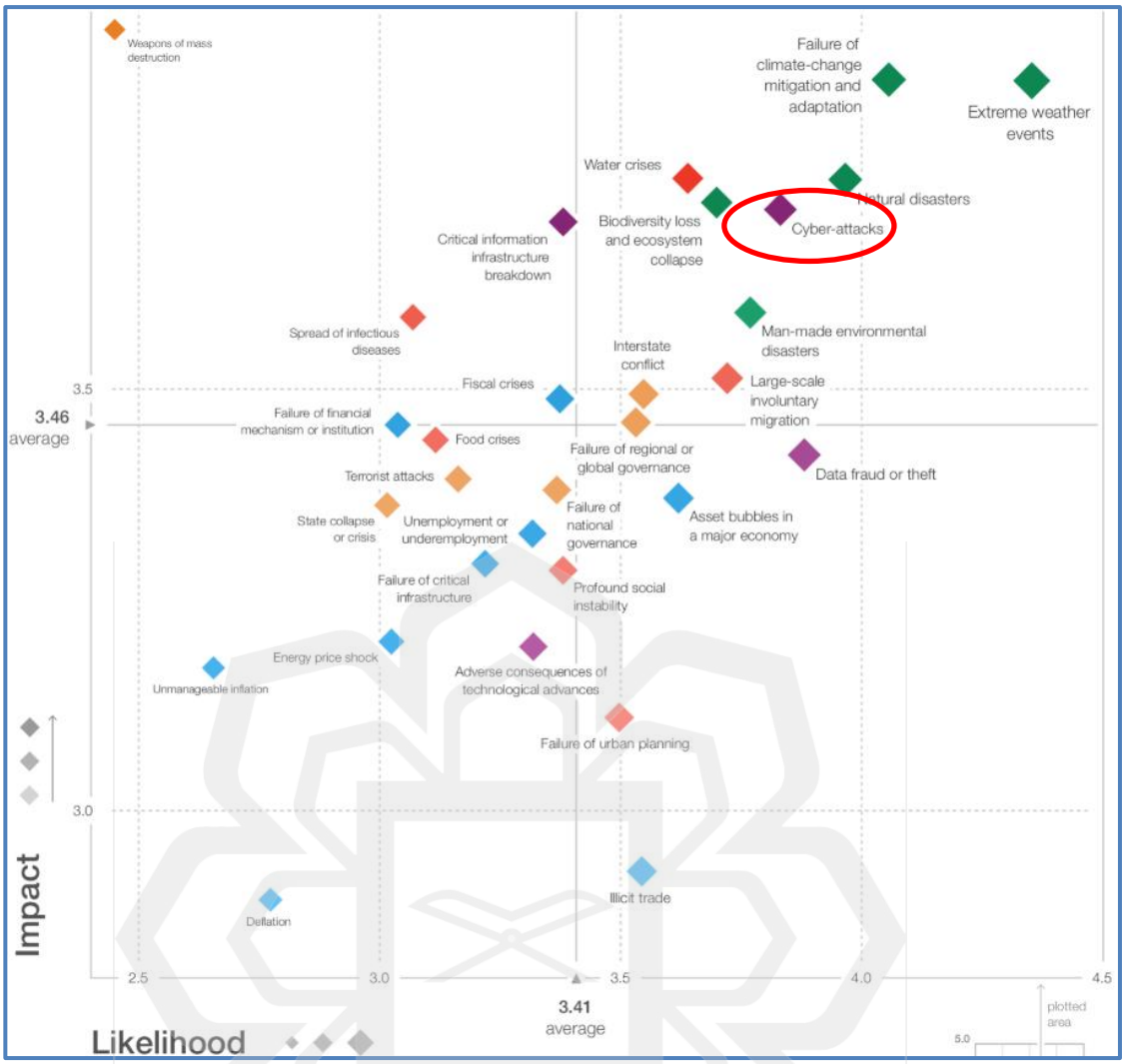

Figure 1.1: A Graph of Impact Against Likelihood (Collins, 2019)

The criminals who perform these threats usually have financial gain and individual satisfaction as their core motivation. There are many terminologies used to classify threats, such as (1) cyber-warfare, (2) cyber-espionage, (3) cybercrime, (4) cyber-terrorism and (5) etc. Table 1.1 gives an overview of their definitions.

Table 1.1: Examples of Terminologies Used to Describe the Nature of Cyber Threats with their Definitions

Terminology	Definition
cyberwar/ cyber-warfare	• Operations done on rival nation-state by the military in the cyber space. It is for the benefit of the state (Brenner, 2006). • Civilians are not supposed to be targeted (Brenner, 2006).
cybercrime	• Unauthorised infiltration into computer networks, usually for economic gains (Morag, 2014). • Similar to cyberwar but differs in term of scale. Cybercrime has a much smaller scale than cyberwar (Elkus, 2011). • Crimes that are committed using technologies (Brenner, 2006).
cyberattack	• The use of malicious codes to take advantage of other people's computer network, computer information system, etc. (Gangadeen, 2016) • 2 types: (1) Syntactic (the use of malicious software). Example: Virus, Worms, Trojan Horses, Spyware, Malware (Gangadeen, 2016) (2) Semantic (misleading information for the purpose of covering your track). Example: Phishing, Denial-of-Service (DOS) and Spoofing. (Gangadeen, 2016)
cyber-terrorism	• Similar to cybercrime, but in cyber-terrorism it is for reasons other than personal gains i.e. political (Brenner, 2006). • It targets civilians as opposed to cyber-warfare (Brenner, 2006).
cyber related crime	• Crimes that does not necessarily require the use of technologies. • Sometimes referred to as social engineering. • Social engineering is simply a skill harnessed in order to trick victim into giving their valuable information just by talking or impersonating someone else (Peters, 2015).
cyber-sabotage	• The act of causing a disturbance to the computer network (Morag, 2014). • Similar to cyber-terrorism but in cyber-sabotage, it does not harm people directly (Morag, 2014).
cyber-espionage	• Usually associated with the involvement of spies to devise a strategy in order to retrieve a government or an organisation's sensitive information by the means of breaking the computer system or network (Morag, 2014).

From Table 1.1, one would be able to understand that cyber threats can exist in many different forms and each form may differ in terms of its scale, purpose and methods of attacking.

Just as much technology is improving, the cyber threats are also continuing to evolve. In May 2017, about 150 countries were attacked by a Wannacry Ransomware virus (Dwoskin & Adam, 2017). Once infected, a computer for example, would have all data and information stored within it encrypted and unless the owner of the computer paid the demanded ransom, nothing can be done to retrieve them. The National Health Service (NHS) in United Kingdom was one of the organisations that fell victim to this phenomenon. Due to the attack, X-Ray imaging was unable to be carried out causing delay for patients to get treatment (Rawlinson, 2017). Experts had also warned that it is still highly unlikely that the data would be decrypted once the ransom had been paid (Collins, 2017; Yalburgi, 2017).

In January 2018, the disclosure of Meltdown and Spectre vulnerabilities has practically put every operating system and device at risk ("10 Must-Know 2018 Cybersecurity Statistics", 2018). These vulnerabilities allow attackers to get access to data previously considered completely protected in computing device (Fruhlinger, 2018).

The year 2019 falls nothing short of the cyberattacks when in January, a bug was discovered in iPhone FaceTime application (Mayo, 2019). The bug allowed a caller to hear the recipient's audio even though he or she has yet to answer or reject the call. The following figures (Figure 1.2 and 1.3) depicted the various forms of cyber threats in Malaysia as well as international in 2018.

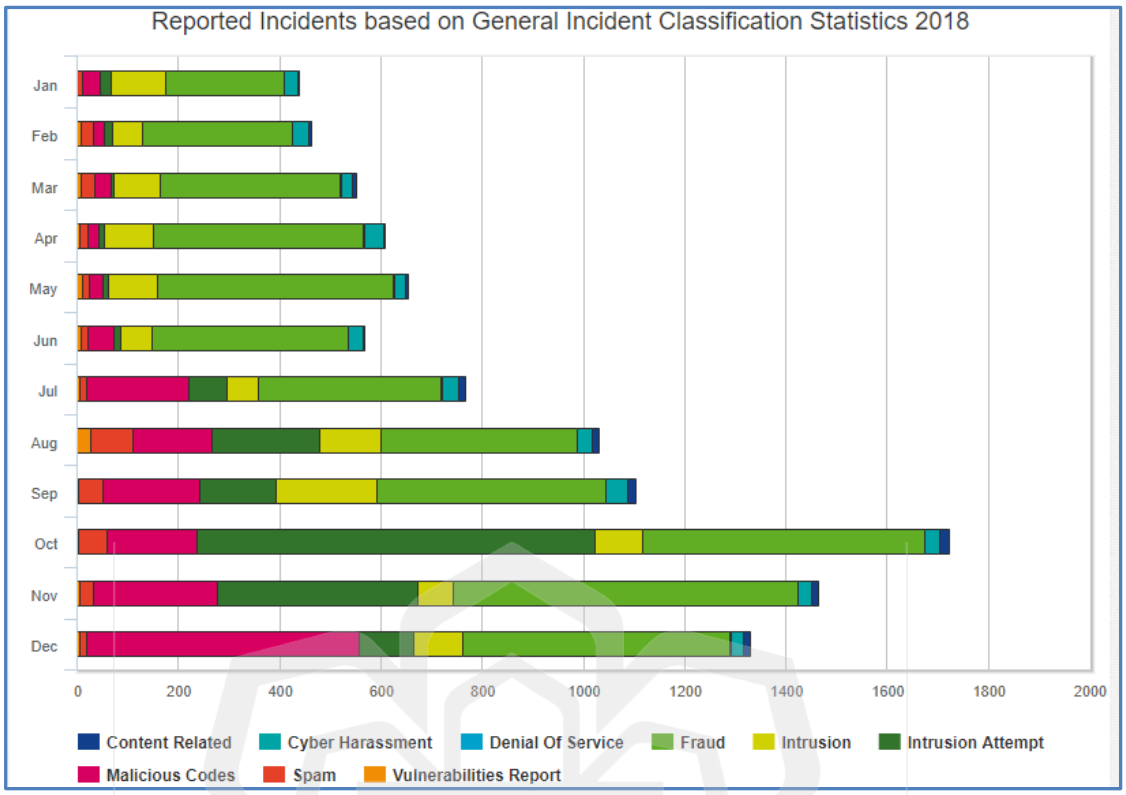

Figure 1.2: Reported Incidents in Malaysia 2018 (MyCERT - The Malaysian Computer Emergency Response Team, 2019)

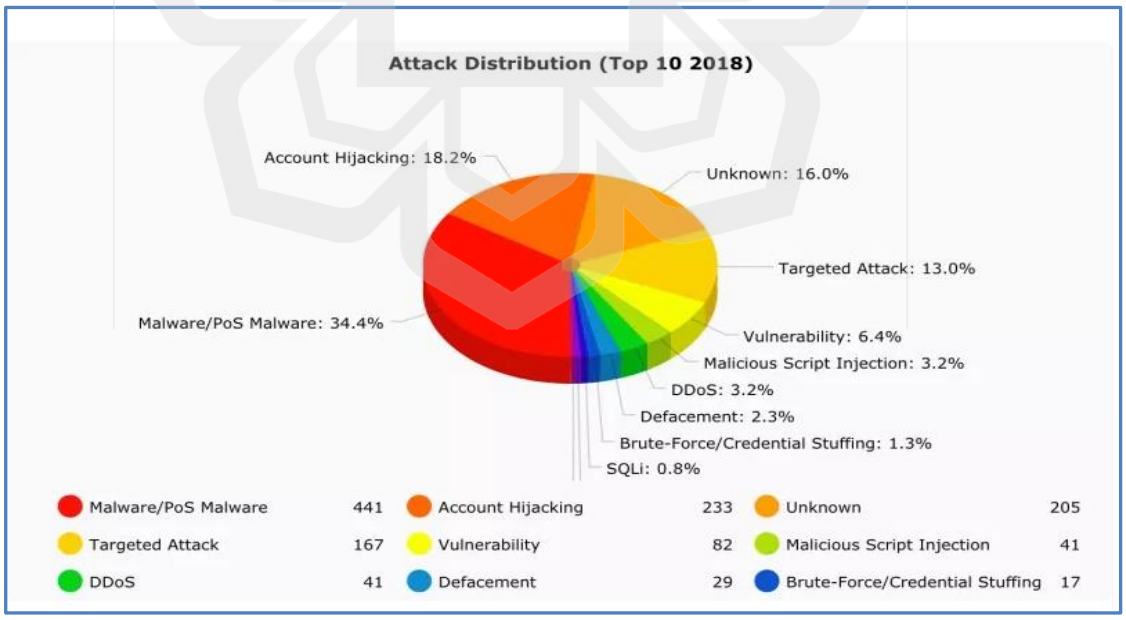

Figure 1.3: Reported Incidents in the World, 2018 (Passeri, 2019)