Risk Assessment of Sharing Cyber Threat Intelligence

Adham Albakri[1,2] , Eerke Boiten[1] and Richard Smith[1]

[1] School of Computer Science and Informatics, De Montfort University, Leicester, UK
[2] School of Computing, University of Kent, Canterbury, UK
{adham.albakri, eerke.boiten, rgs}@dmu.ac.uk

Abstract

Sharing Cyber Threat Intelligence (CTI) is advocated to get better defence against new sophisticated cyber-attacks. CTI may contain critical information about the victim infrastructure, existing vulnerabilities and business processes so sharing CTI may carry a risk. However, evaluating the risk of sharing CTI datasets is challenging due to the nature of the CTI context which is associated with the evolution of the threat landscape and new cyber attacks that are difficult to evaluate. In this paper, we present a quantitative risk model to assess the risk of sharing CTI datasets enabled by sharing with different entities in various situations. The model enables the identification of the threats and evaluation of the impacts of disclosing this information. We present two use cases that help to determine the risk level of sharing a CTI dataset and consequently the mitigation techniques to enable responsible sharing. Risk identification and evaluation have been validated using experts' opinions.

Keywords: Cyber Threat Intelligence, Information Sharing, Risk Assessment.

1 Introduction

Sharing CTI datasets increases due to the number of attacks, threat actors' motivations and capabilities. It helps organisations get better defence and increase the accuracy of threat detection [1]. However, sharing CTI datasets has specific consequences which makes organisations reluctant to share. The barriers can be: (1) the probability of undesirable information disclosure increases when sharing with organisations that do not have a high level of trust or when sharing with the public, (2) CTI datasets can contain various kinds of information such as personal, organizational, financial and cybersecurity information [2]. Thus, evaluating the risk of sharing CTI datasets containing critical information such as the existing vulnerabilities is a challenge especially with the evolving of the cyber threat landscape and sophisticated cyber-attacks for various business sectors. When considering the different sources of CTI information and the intention to share with various entities, a risk assessment model is needed. By evaluating the associated risk of sharing CTI datasets, organisations would know how critical their CTI datasets are before sharing [2] and use the right methods and processes to manage the

risk to respect the organization's acceptable risk level. In addition, they need to obtain legal compliance as the General Data Protection Regulation (GDPR) [3] mandates organisations to undertake risk assessments and fulfill security mitigation controls.
In this paper, we will propose a specific quantitative risk model for evaluating the risk of sharing CTI datasets. This builds on the identification and partial assessment of threats in cyber incident information sharing in our earlier work [2]. This model will help improve the decision of sharing CTI information with multiple entities. During the evaluation phases, we take into consideration the threats of sharing each attribute in the CTI dataset and the likelihood of such threats occurring and the level of trust in the receiving party. The remainder of this paper is organized as follows. Section 2 discusses related work. Section 3 describes the steps of the methodology to build the model. Section 4 gives several use cases of sharing CTI datasets to validate the model through involving cybersecurity experts. Section 5 gives threats to validity. Finally, Section 5 presents the conclusion and future research directions.

2 Related work

In [4] the authors addressed the types of information that could be shared between SMEs while addressing the risk of disclosure cyber-attack scenarios. However, the study was limited to SMEs and a small size sample with specific security metrics which could be different in different business scenarios. In our work, we are evaluating the risk and proposing a more general model not related to specific business for calculating the risk of sharing CTI datasets. In [5] the authors proposed a cyber security risk model using a Bayesian network model for the nuclear reactor protection system (RPS) then applying the analytical result to an event tree model. In their model, they have only focused on four cyber threats and six mitigation measures according to the design specification of an RPS. This evaluation was only on the network layers not covering other types of possible threats. In [6] the authors proposed a quantitative asset and vulnerability centric cyber security risk assessment methodology for IT systems. They defined and extended metrics based on CVSS and presented a formula for computation and aggregation. The work focused only on the CVEs without considering other factors in the impact. Also, the calculation was based on the defined CVSS list without including zero-day attacks. The model did not consider the threat actor and the attack vector, and the focus was only on the individual asset and the vulnerabilities at the assets which satisfy the consideration of the assets and the system design. They proposed a base risk assessment model and an attack graph-based risk assessment model. However, these methods do not consider a quantitative approach for risk evaluation when sharing CTI datasets, such as the one presented in this paper. In this paper, we propose a new model to compute this risk by identifying threats, severity and probability of sharing CTI information.

3 Methodology

3.1 Risk Assessment Approach/Background

Risk is defined in the business world enterprise as "the extent to which the outcomes from the corporate strategy of a company may differ from those specified in its corporate objectives, or the extent to which they fail to meet these objectives"[7] .
There are outstanding risk assessment methodologies including ISO/IEC 27005 [8] that provide guidelines for information risk management activities as an aspect of the business process in organisations. Also, NIST SP 800-30 [9] is a framework to help conduct risk assessments of critical infrastructure systems and organizations. This framework helps senior management to select the course of action for specific threats. Octave [10] focuses on identifying vulnerabilities that exist in the organization's structure and implements security strategies and plans. There are various ways to assess risk including quantitative, qualitative, or semi-quantitative. Quantitative risk assessment is based on using mathematical methods and rules. In this type, numbers represent information, for example, a numerical value of 1 is assigned to the high probability of a specific attack that could occur. Understanding the context and explaining the constraints helps in assigning the numbers in meaningful way; thus, the meaning of the quantitative results would be clearer. However, in some cases the results need additional justifications and clarifications to understand what the numerical results represent. For example, before sharing any CTI dataset, the owner may ask if the risk assessments results are reliable based on the assumptions used in the calculations. On the other hand, qualitative risk assessment is based on applying non-numerical methods according to levels such as low, medium and high. This type of assessment has a limited number of results which make it more comprehensible to decision makers. Each value should be defined clearly and categorised by a clear description and an example. Without a clear description, experts may rely on their experience and opinion which might provide different assessment results. Finally, semi-quantitative risk assessment combines rules and methods for evaluating the risk based on numeric values and levels. For example, the range between 1 and 10 can easily be converted into qualitative expressions that help risk communications for decision makers. The role of expert judgment in assigning values in the semi-quantitative risk is more palpable than in a purely quantitative approach. Moreover, if the scales or sets of levels provide sufficient granularity, relative prioritization among results is better supported than in a purely qualitative approach. In this type, all ranges and values need to be explained and defined by clear description and examples. Semi-quantitative assessments use various methods or rules for evaluating risk based on levels, scales or numeric values that are meaningful in the context. For example, a score of 90 for a CTI dataset can represent a very high risk. The role of experts' judgment still exists in this type and similar to the qualitative and quantitative models each numeric value and range needs to be defined and explained.

3.2 Associated Risk Model (ARM)

In this section, we present our associated risk model (ARM). The first step in our ARM procedure is to examine the dataset. In this step, we will be indicating the roles

that the various attributes may play: they could contain sensitive information, or help to identify people and organisations. We then point out threats, using the ENISA threat taxonomy [11]. We compute the severity for each property in the dataset because if there is a disclosure of sensitive and critical information, there would be a risk that an associated threat could exploit the system. Then the organisation may face an unexpected cybersecurity attack, reputational damage and legal consequences. We have precisely identified the associated threat by analyzing each property in the STIX 1.2 incident model separately and mapping it to the ENISA threat taxonomy [11]. Then, for each property we have calculated the severity value that was assigned in our previous work [2]. After identifying the potential threats, we can derive the level of associated risk for this sharing by estimating the likelihood of the threats in case of property disclosure. Our goal is to reduce the risk value by selecting the appropriate privacy preserving techniques to improve the sharing between organisations. Figure 1 illustrates the flow chart of ARM which describes the risk assessment steps, including identification of risks through the disclosure of the shared dataset properties, their total risk value through the analysis of threats mapped based on the disclosed properties.

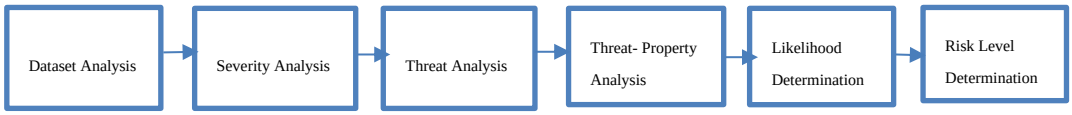

Figure 1-ARM Steps

3.3 Dataset Analysis

First, we need to identify the associated risk of disclosing any property of the shared CTI dataset. Each property may have a different severity level in an organisation. In previous work [2], we have estimated the cybersecurity severity score for each property int the STIX 1.2 incident model [12]. The severity score range is [1,8], where 1 is the lowest level of severity and 8 is the highest level of severity. Based on the severity score, severity assigned to four impact levels: negligible, limited, significant and maximum which can be represented as 10, 50, 75 and 100. Let each property be represented as a single bit in the property vector:

$$\vec{P} = \{P_i\} \in \{0,1\} \forall i, i = 1, 2, \dots n \quad (1)$$

Here, P_i represents an individual property. The value 1 indicates the existence of this property in the shared dataset, otherwise it is 0. Because disclosing any property in the shared dataset is a potential risk, we include all properties into our analysis. If we are fully sharing a dataset with 10 properties, we set n to 10 and $P_i = 1 \forall n$.

3.4 Threat Analysis

The second step in our model is to perform a threat analysis, which consists of identifying the potential threat action that may exploit the system or the organisation based

on the CTI information disclosure. Information about threats can be collected from the organisation's CTI database and threat taxonomies which can define a list of potential threats to the organisation. Let each threat be represented as a single bit in the threat vector:

$$\vec{T} = \{T_j\} \in \{0,1\} \forall j \, , j = 1, 2, \dots m. \qquad (2)$$

Here T_j represents an individual threat, the value 1 indicates the presence of this threat when sharing the CTI dataset and otherwise it is 0. Thereafter, based on the CTI dataset disclosure and the associated threats, we can match threats to the CTI property and estimate the likelihood of a threat occurring based on disclosure of CTI information. The likelihood values L_{ij} are based on how easy it is for a threat to be executed by a motivated and powerful adversary. This likelihood can adopt three values: low, medium, high represented as 0.1, 0.5 and 1. In case there is no risk, we assign value $L_{ij} = 0$. In the previous step, there will be a subjective factor - expert judgment- because of the diverse perception of associated threats for each property, what impact that would have on the organisation and likelihood of an event happening. The judgment of the likelihood value would be based on the available context which might be related to the business sector, location, perpetrator motivation, resources and abilities. Each CTI dataset comes from separate business sector, context and countries that could create different associated threats such as the legal assessment. Therefore, a specific way of calculating the associated risk and defining each risk level in terms of expected impact and expected techniques to share securely might be a mandatory pre-requirement for sharing CTI datasets. For example, the impact of gaining access over the ATM control system in order to withdraw money is different than the impact of gaining control over CCTV cameras in a critical infrastructure.

3.5 Total Associated Risk (TAR)

Total Associated Risk (TAR) is the sum of sub associated risks of disclosing CTI information and can be computed as follows:

$$TAR = \sum_{i=1}^{n} \sum_{j=1}^{m} L_{ij} * S_i * P_j * T_i \text{ where } TAR \in \mathbb{R}^+ \quad (3)$$

Where n represents the number of the properties, m represents the number of the threats, L_{ij} represents likelihood of the presence of the threat i when disclosing the property j and S_i represents the severity score. The likelihood values L_{ij} represent how easy it is for a powerful and motivated adversary to execute threat j knowing property i. Once TAR is computed, the organisation becomes aware of how this could provide the appropriate information to decision makers about how to make a clear decision about sharing this dataset and how to evaluate the associated risk.

4 Evaluation

To evaluate the ARM model, we have conducted an experiment on two case studies that were analyzed manually using our model by independent experts.

4.1 Expert selection

In this study, we have developed two use cases aiming to validate our model. Two use cases were analyzed by independent experts with different levels of experience working on cybersecurity and privacy during a privacy workshop. Also, we have asked PhD students (third year) during a PhD summer school to fill a questionnaire, all PhD students are working in cyber security.

4.2 Case Studies

The presented ARM is here tested through three use case studies. Case study 1 discusses sharing a CTI dataset for correlation purposes while case study 2 discusses sharing a CTI dataset for aggregation purposes. In all case studies we consider sharing with trusted and untrusted entities.

4.2.1 Case Study 1: CTI contains malware information & personal information - Sharing for detections

This scenario consists of two cyber threat companies, CyberA and CyberB. CyberA has been attacked by specific malware. This malware was designed to steal encrypted files and was even able to recover files that had been deleted. CyberA wants to share this incident dataset with others in their sharing community. The purpose of this sharing is to let recipients check if they have spotted the same malware on their system. Table *1* shows the sample CTI dataset which contains the properties that might be shared.

Table 1- Use Case 1 (CTI Dataset)

Property	Value
TTP[1] Malware Type	Capture Stored Data, Remote Access Trojan
Indicator Name	File hash for malicious malware
Indicator Description	This file hash indicates that a sample of malware alpha is present.
Indicator Value	Hashes.'SHA-256'= 'ef537f25c895bfa7jfdhfjns73748hdfjkk5d789c2b76589fjfer8fjkdndkjn7yfb6c' Windows-registry-key:= "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\MSADL3"
Vulnerability	CVE-2009-3129, CVE-2008-4250, CVE-2012-0158, CVE-2011-3544
Incident Title	Incident associated with CyberA campaign. Malware was designed to steal encrypted files - and was even able to recover files that had been deleted.
Date	2012-01-01T00:00:00
Reporter Name	Alex John
Reporter Email Address	alex@pro-it.com
Reporter Address	US - LA
Victim Name	CyberA / The CEO Device

[1] Tactics, Techniques and Procedures

Victim sector	Financial sector
Victim Device	IP address: 146.227.239.19
Victim Email Address	cybera@cyber.com / ceo-cybera@cyber.com
Victim Address	CyberA Ltd, IT Department, LONDON, W5 5YZ
Affected Assets Type	Desktop, Mobile phone, Router, Server, Person
Affected Assets Property	Confidentiality (Classified, Internal, Credentials, Secrets, System) Integrity (Software installation, Modify configuration, Alter behaviour)
Incident Status	Not solved
Total loss	£ 65,000

Associated Risk Evaluation

To compute the associated risk of sharing this CTI dataset, we apply our model as follows. The first step is to identify and analyse the severity for each property in the dataset. Table 2 defines the threats associated with disclosing the CTI dataset as derived from Table 1. We have assigned the sets of potential threats for each property and evaluated those for severity in cyber security contexts.

Table 2- Severity value and Associated threats

Property	Property ID	Threat	Severity
Victim (Name, Sector, Address, Role,)	P1	T1, T2, T3, T4, T10	10
Malware (Type, Description)	P2	T3, T6	10
IoC (Name, Desciption, Value)	P3	T2, T3, T4	10
Vulnerability	P4	T2, T3, T4	10
Affected Assets (Type, Property)	P5	T2, T4, T7, T9, T10	10
Status	P6	T2, T6	10
Total Loss	P7	T6, T11, T10	50
Impact Assessment	P8	T6, T11, T10	10
Reporter	P9	T1, T2	10

Table 3 represents the same relationship between the threats and the properties of the CTI dataset by focusing on the threats.

Table 3- Threats and matched property

Threat	Threat ID	Matched Property
Identity theft (Identity Fraud/ Account)	T1	P1, P9
Social engineering	T2	P1, P3, P4, P5, P6, P9
Unauthorized activities	T3	P1, P2, P3, P4
Targeted attacks (APTs etc.)	T4	P1, P3, P4, P6
Misuse of information/ information systems	T5	P3, P4
Compromising confidential information (data breaches)	T6	P2, P3, P4, P7, P8
Unauthorized physical access	T7	P5
Violation of laws or regulations / Breach of legislation	T8	P5
Failure to meet contractual requirements	T9	P5
Loss of reputation	T10	P1, P2, P7, P8
Judiciary decisions/court orders.	T11	P7

Based on the CTI dataset disclosure and the associated threats we estimate the likelihood of a threat occurring based on the property value and the context which varies depending on the organisations' requirements. Table 4 presents our estimates of the

likelihood L_{ij} of the threats and the total risk score TAR when sharing with public sharing communities. Table 5 presents the estimated likelihood of the threats and the total risk score value when sharing with trusted communities. Finally, we evaluated the risk in three different scenarios: sharing the CTI dataset with public communities, sharing when involving/considering a high level of trust with the receiver and finally, sharing after removing the unrelated information.

Table 4- Likelihood and total risk value (public sharing communities)

	P1	P2	P3	P4	P5	P6	P7	P8	P9	**SUB-RISK**
T1	0.1	0	0	0	0	0	0	0	0.1	2
T2	1	0	0.1	0.1	1	0.5	0	0	0.1	28
T3	0.5	1	0.5	0.5	0	0	0	0	0	25
T4	1	0	0.5	0.5	1	1	0	0	0	40
T5	0	0	0.1	0.1	0	0	0	0	0	2
T6	0	1	0.1	0.1	0	0	1	1	0	72
T7	0	0	0	0	0.5	0	0	0	0	5
T8	0	0	0	0	0.5	0	0	0	0	5
T9	0	0	0	0	0.5	0	0	0	0	5
T10	0.5	0.1	0	0	0	0	1	0.5	0	61
T11	0	0	0	0	0	0	0.1	0.1	0	6
									TAR	**251**

Table 5- Likelihood and total risk value (trusted communities)

	P1	P2	P3	P4	P5	P6	P7	P8	P9	**SUB-RISK**
T1	0.1	0	0	0	0	0	0	0	0	1
T2	0.5	0	0.1	0.1	0.5	0.1	0	0	0.1	14
T3	0.1	0.5	0.5	0.5	0	0	0	0	0	16
T4	0.1	0	0.1	0.1	0.1	0.5	0	0	0	9
T5	0	0	0.1	0.1	0	0	0	0	0	2
T6	0	0.5	0.1	0.1	0	0	0.5	0.5	0	37
T7	0	0	0	0	0.1	0	0	0	0	1
T8	0	0	0	0	0.1	0	0	0	0	1
T9	0	0	0	0	0.1	0	0	0	0	1
T10	0.1	0.1	0	0	0	0	0.5	0.5	0	32
									TAR	**114**

When sharing with public communities, the risk value is 251. On the other hand, sharing within trusted communities decreases the risk value to 114. In this scenario, the purpose of sharing is to check the existence of the same malware thus we need to know the type and description of the malware, in addition to the indicators of compromise such as hash file value and windows registry key. Therefore, the properties needed for sharing are P2 and P3. Therefore, the associated risk value if we only share these essential properties will be reduced to 34 as shown in Table *6*. Reducing the risk value is important for encouraging CTI sharing, and to achieve that, the organisation filters out the sensitive information that is not relevant to the purpose of this sharing.

Table 6- Likelihood and total risk value for sub-dataset

Threat ID	P2	P3	SUB-RISK
T2	0	0.1	1
T3	1	0.5	15
T4	0	0.5	5
T5	0	0.1	1
T6	1	0.1	11
T10	0.1	0	1
T11	0	0	0
		TAR	**34**

Our model allows for each risk assessment to be combined in different ways for different purposes. For instance, Figure *2* demonstrates a risk assessment visualisation for the same CTI dataset. For each field in the CTI dataset, we displayed the sum of the risks posed by that property in case of disclosure. This visualisation shows which properties of CTI dataset are the greatest risk when sharing and might be used in the context of raising organisational awareness of the CTI dataset properties.

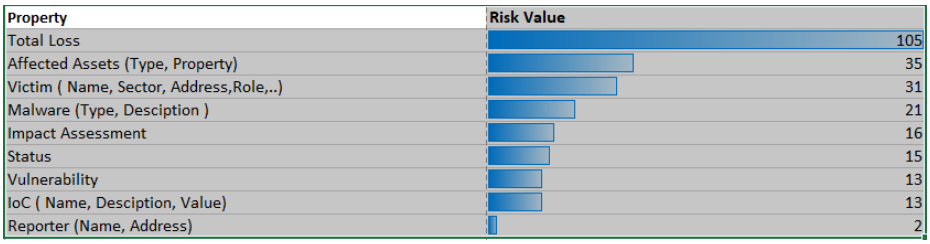

Figure 2 - A risk assessment visualisation showing risk value per type of information.

Evaluation - Data Collection and Analysis

This section presents the results of the data collection from a questionnaire [2] conducted within privacy and cybersecurity workshops with 15 experts in privacy and cybersecurity. The study provided anonymity to the participants. The questionnaire contains 3 parts. The first part focuses on identifying the threats associated with disclosing the CTI dataset. We proposed a list of threats and free text for extra suggestions. The second part focuses on the security controls that might be applied to preserve privacy of the dataset such as redaction/selection, anonymisation, aggregation, encryption and so on. Finally, the third part focuses on giving a risk value to the dataset in both cases, before and after applying the security controls. Fifteen experts filled out the questionnaire and a summary of the data collected is presented in Table *7* and discussed in more detail below. The question Q1 was answered by 15 experts for sharing the CTI dataset with public sharing communities and by 12 when sharing with trusted communities. Nine experts selected in detail the possible associated threats of disclosing this dataset. Table *8* presents the threats and how many experts have selected that threat as a possible threat in case of disclosing this CTI dataset. For example, six experts out of nine agreed that

[2] https://docs.google.com/document/d/1y0N18P-C34b93AVc2u-I44BX7uRLuobS0kkQyXudXCw/edit?usp=sharing

disclosing this dataset would be associated with “Compromising confidential information” and “Loss of reputation” threat. The remaining did not consider these as possible threats. The result indicates that the list we have proposed in Table *3* matches the experts’ selections in Table 8.

Table 7- UC1 Summary: Responses Returned

Question	Part 1- Sharing with public (Number of responses)	Part2- sharing with trusted entities (Number of responses)
Q-1	15	12
Q-2	15	13
Q-3.1(Redaction/Selection)	8	0
Q-3.2 (Anonymisation)	7	7
Q-3.3 (Aggregation)	6	7
Q-3.4 (Enc)	7	7
Q-3.5(others)	3	3
Q4	14	14

Table 8- UC1-Part1-Threat Summary

Threat	**Count**	**Threat**	**Count**
Social engineering (Phishing, Spear phishing)	4	Loss of reputation	6
Failure to meet contractual requirements	3	Unauthorized physical access	0
Violation of laws or regulations	2	Failed business process	1
Compromising confidential information	6	Man-in-the-middle	0
Identity theft (Identity Fraud/ Account)	4	Terrorists attack	0
Abuse of authorizations	0	Targeted attacks (APTs etc.)	2
Misuse of information/ information systems	4	Unauthorized activities	4
Generation and use of rogue certificates	0	Manipulation of information	3

Table 9 presents the number of experts who decided which threats might be associated with disclosing the CTI dataset when sharing with trusted entities. The possible threats have decreased due to the increase of trust level among the sharing organisations. However, the result still shows that the list we have proposed in Table 3 matches the experts’ selections in Table 9.

Table 9- UC1-Part2-Threat Summary

Threat	**Count**	**Threat**	**Count**
Social engineering (Phishing, Spear phishing)	1	Loss of reputation	6
Failure to meet contractual requirements	4	Unauthorized physical access	0
Violation of laws or regulations	1	Failed business process	2
Compromising confidential information	4	Man-in-the-middle	0
Identity theft (Identity Fraud/ Account)	1	Terrorists attack	0
Abuse of authorizations	0	Targeted attacks (APTs etc.)	0
Misuse of information/ information systems	1	Unauthorized activities	0
Generation and use of rogue certificates	0	Manipulation of information	0

For question Q2, eight experts indicated that we cannot share this dataset. On the other hand, 7 indicated that we can share after mitigation. This result indicates that sharing this dataset without applying any security controls will be a high risk to CyberA.

For questions Q3.1 and Q3.2 experts selected values that should be anonymized or removed from the dataset before sharing, such as “Reporter Name”, “Reporter Email”, “Reporter Address”, “Victim Name”, “Victim Sector”, “Victim Device”, “Victim Email”, “Victim Address” and “Total Loss”.
Many experts agreed to remove any personal data, such as the victim information which will reduce possible threats such as “Violation of laws or regulations” and make the decision of sharing compliant with the regulation such as the GDPR [13]. In our model we looked at the properties that will be useful for the purpose of sharing and the analysis as it is presented in Table 6. These fields are (Malware, observed-data, Indicator). Therefore, the experts’ selection is relevant to our model of risk value evaluation because the excluded properties will not be useful for the purpose of this sharing.
For question Q3.3, six experts gave an answer which included Address, Date and Affected Assets Type. This indicates that some information needs to be grouped and aggregated before sharing as part of reducing the risk of sharing individual information.
Also, sharing the full dataset would not be necessary to achieve the goal of this analysis, and it could reveal sensitive information which might be unimportant to other organisations and highly risky to share. Therefore, after evaluating the dataset we have extracted a sub-dataset which contains only the relevant information. For question Q3.4, seven experts indicated that some attributes should be encrypted, such as indicator of compromise values, email addresses and victim information. This decision will work properly when CyberA needs to share the sub-dataset with other organisations where the level of trust is low and to avoid any inferring of sensitive information, such as network infrastructure from the network traces [14]. We can apply one of the several techniques to protect privacy in correlation, such as salted hashes [15] and homomorphic encryption [16]. By applying these techniques, an analyst can ask for a correlation and analysis without revealing extra information about what they are looking for. For question Q3.5, three experts confirmed that specific fields such as IP addresses and email addresses should be generalized. For question Q4.1, experts were asked to evaluate overall risk on a 1-5 scale, with 5 being the worst. Nine experts indicated that the risks are between 4 and 5 which constitutes a high level of risk. On the other hand, after applying the suggested controls, five experts suggested that the risk value would be between 1 and 2 which constitutes a low risk level. However, when sharing the CTI dataset with trusted entities, the overall value changed from a medium risk level to a low risk level. Eight experts stated that the risk value is between 2 and 3, and after applying the security controls, eight stated it was between 1 and 2. As a result, the case study findings suggest that sharing this CTI dataset is possible after applying specific security controls, mainly by removing unrelated data and applying encryption. From the questionnaire results we find out that our model reached an acceptable match with respect to the cybersecurity and privacy experts. All the threats we identified were also identified by the experts. Experts identified different controls to reduce the risk of sharing and they agreed that sharing this dataset without applying these controls is high risk. Although some experts had different decisions, this difference was due to the different expertise levels and the experts’ subjective view of how they define the granularity level of the risk. Also, threat and technical details such as network information can have different meaning between security experts. For example, five experts have

not selected the encryption as a security control which should have been applied before sharing, and others focused mainly on the anonymization techniques as a security control. In our model the dataset admin is free to select the security control of choice, for example homomorphic encryption [16] [17] or Secure multi-party computation [18][19].

4.2.2 Use Case 2: "CTI contains Malware information & personal information – Aggregation of data"

This scenario consists of cyber threat companies, CyberA and other companies which share threat intelligence with one another. CyberA has been attacked by a specific threat actor and would like to know how many companies have been attacked by the same threat actor. Sharing the threat actor information is sensitive due to the possibility of identifying the techniques and procedures used in the attack, the victim information and the targeted sector such as oil business, health and diplomatic offices. The incentive of this sharing is to understand and analyse this threat actor. CyberA needs to determine how many companies have been targeted by the same threat actor. In this case study, we have used the STIX report about the "Red October" Campaign [20]. Before sharing the STIX report, we need to evaluate the associated risk of sharing this information within the CTI sharing communities. Table 10 shows the sample CTI dataset which contains the properties that might be shared.

Table 10- UC3 Dataset

Property	Value
TTP Malware Type	Command and Control, capture stored data, Scan network, Exploit vuln, Remote Access Trojan, Downloader, Export data, Spyware/Keylogger, Brute force
TTP Attack Patterns[3]	CAPEC-98
Vulnerability[4]	CVE-2009-3129, CVE-2010-3333, CVE-2012-0158, CVE-2011-3544
Title	Incident associated with Red October campaign. Phishing email with malware attachment leading to infection, C2, credential compromise, and lateral movement through network. Goal to steal classified info and secrets
External ID	4F797501-69F4-4414-BE75-B50EDCF93D6B
Incident Date	2012-01-01T00:00:00
Reporter	Alex John, W-baker org, alex@w-baker.org, (LE1 9BH, Leicester, UK)
Victim	Japan Fair Trade Commission – intnldiv@jftc.go.jp
Victim Address	International Affairs Division (16th floor), Japan Fair Trade Commission, 6-B building, Chuo Chosha, 1-1-1 Kasumigaseki, Chiyoda-ku Tokyo 100-8987
Affected Assets Type	Desktop, Mobile phone, Router or switch, Server, Person
Affected Assets Property	Confidentiality (Classified, Internal, Credentials, Secrets, System) Integrity (Software installation, Modify configuration, Alter behaviour)
Security Compromise	Yes
Discovery Method	Ext - suspicious traffic
Threat Actor Title	Lone Wolf Threat Actor Group

[3] Common Attack Pattern Enumeration and Classification - https://capec.mitre.org/index.html
[4] Common Vulnerabilities and Exposures (CVE) https://cve.mitre.org/

Threat Actor Description	Notes: Basing on registration data of command and control servers and numerous artifacts left in executables of the malware, we strongly believe that the attackers have Russian-speaking origins. Current attackers and executables developed by them have been unknown until recently, they have never related to any other targeted cyberattacks
Threat Actor	The Lone Wolf / Gookee Organisation
Threat Actor/ Country	Russia
Threat Actor /Area	Moscow
Threat Actor/Address Identifier	lone-wolf@stealthemail.com / facebook.com/theLonewolf
Threat Actor Language	Russian
Threat Actor Motivation	Espionage
Threat Actor Observed TTPs	"example:ttp-fcfe52c2-3060-448b-b828-3e09341485b1" / "example:ttp-2a884574-bf2b-4966-91ba-3e9ff6fea2e3" / "example:ttp-22290611-0125-4c62-abcc-ddd4b8d3fb5d"

Associated Risk Evaluation

Analogous to use case 1, we have evaluated the associated risk of sharing the CTI dataset, we are applying our model as follows. Table 11 defines the threats associated with disclosing the CTI dataset and identifies the cybersecurity severity for each property as derived from Table 10.

Table 11 Associated threats and Severity value

Property	Property ID	Threat ID	Severity
TTPs	P1	T1, T2, T3	50
Reporter	P2	T2, T4, T7	10
Victim	P3	T2, T3, T5, T6, T7	50
Affected Asset	P4	T2, T3, T7, T8	10
Threat Actors	P5	T1, T2, T3	50
Security Compromise	P6	T6	10
Discovery Method	P7	T6	10

Then we have Table 12 which represents Table 11 in a different way by focusing on the threats.

Table 12 Threats and matched property

Threat	Threat ID	Matched Property
Compromising confidential information	T1	P1, P5
Social engineering	T2	P1, P2, P3, P4, P5
Targeted attacks (APTs etc.)	T3	P1, P3, P4, P5
Identity theft (Identity Fraud/ Account)	T4	P2, P3
Unauthorized activities	T5	P3
Loss of reputation	T6	P3, P6, P7
Violation of laws or regulations	T7	P2, P3, P4, P5
Failure to meet contractual requirements	T8	P4

We estimate the likelihood of a threat occurring based on the property value and the context. For example, targeting high profile victims such as embassies will increase the probability of the “Misuse of information” threat in case of disclosing victim and attack vector information. The total associated risk (TAR) is the sum of sub associated risks

of disclosing CTI information. Table 13 presents the likelihood L_{ij} of the threats and the total associated risk score TAR when sharing with public sharing communities. Table 14 presents the likelihood of the threats and the total risk score value when sharing with trusted communities.

Table 13 Likelihood and total risk value (public sharing communities)

Threat ID	P1	P2	P3	P4	P5	P6	P7	SUB RISK
T1	1	0	0	0	1	0	0	100
T2	1	0.1	1	0.5	0.5	0	0	131
T3	0.5	0	0.5	0.5	0.5	0	0	80
T4	0	0.1	0.1	0	0	0	0	6
T5	0	0	0.1	0	0	0	0	5
T6	0	0	1	0	0	0.1	0.1	52
T7	0	0.1	0.1	0.1	0.1	0	0	12
T8	0	0	0	0.1	0	0	0	1
T9	0.5	0.1	1	0.5	0.5	0	0	106
							TAR	**493**

Table 14- Likelihood and total risk value (trusted communities)

Threat ID	P1	P2	P3	P4	P5	P6	P7	SUB RISK
T1	0.5	0	0	0	0.5	0	0	50
T2	0.5	0.5	0.5	0.1	0.1	0	0	61
T3	0.5	0	0.5	0.1	0.1	0	0	56
T4	0	0.1	0	0	0	0	0	1
T6	0	0	0.5	0	0	0.1	0.1	27
T7	0	0	0	0	0.1	0	0	5
T9	0	0.1	0.1	0.1	0	0	0	7
							TAR	**207**

When sharing with public communities, the risk value is 493. On the other hand, sharing within trusted communities decreases the risk value by 58% making the value 207. To reduce the risk of sharing and preserve the privacy in the shared information, minimization should be applied to exclude sensitive information that is not relevant to the analysis from the original dataset. The sanitized dataset would fulfil the purpose and usefulness of sharing. In this use case we keep two properties which are “TTPs” and “Threat_Actors”. The total risk score of the sub dataset after removing unrelated properties will be reduced to 280 as explained in Table 15.

Table 15. Likelihood and total risk value for sub-dataset

Threat	ID	P1	P5	Sub Risk
Compromising confidential information	T1	1	1	100
Social engineering	T2	1	0.5	75
Targeted attacks (APTs etc.)	T3	0.5	0.5	50
Violation of laws or regulations	T7	0	0.1	5
Misuse of information	T9	0.5	0.5	50
			TAR	280

Evaluation - Data Collection and Analysis

This section presents the result of the data collection from a questionnaire [5]. Eleven experts filled the survey and a summary of the data collected is presented in Table *16* and discussed in more detail below.

Table 16 - UC2 Analysis Summary: Responses Returned

Question	Part 1- Sharing with public	Part2- sharing with trusted entities
Q-1	11	10
Q-2	11	9
Q-3.1(Redaction/Selection)	7	5
Q-3.2 (Anonymisation)	3	5
Q-3.3 (Aggregation)	3	1
Q-3.4 (Enc)	3	4
Q-3.5(others)	0	0
Q4.1	9	9
Q4.2	6	6

The first question was answered by 11 experts for sharing the CTI dataset with public sharing communities and by 10 when sharing with trusted communities. Nine experts selected in detail the possible associated threats of disclosing this dataset. Table 17 presents the threats and how many experts selected that threat as a possible threat in case of disclosing this CTI dataset. For example, seven experts agreed that disclosing this dataset would be associated with "Compromising confidential information" and six experts agreed on "Social engineering" and "Loss of reputation" threat. The result indicates that the list we have proposed in Table 11 is very similar to the experts' selections in Table 17. For example, we have not considered the "Man-in-the-middle" (MITM) threat. MITM relies on weakness of the communication between two components and based on the report context and the dataset information, we found difficulty in executing this threat. Also, this threat was identified by only one expert.

Table 17 UC2-Part1-Threat Summary

Threat	Count	Threat	Count
Social engineering	6	Loss of reputation	6
Failure to meet contractual requirements	2	Unauthorized physical access	0
Violation of laws or regulations	4	Failed business process	2
Compromising confidential information	7	Man-in-the-middle	1
Identity theft (Identity Fraud/ Account)	3	Terrorist attack	3
Abuse of authorizations	2	Targeted attacks (APTs etc.)	5
Misuse of information	5	Unauthorized activities	3
Generation and use of rogue certificates	1	Manipulation of information	4

[5] https://docs.google.com/document/d/1y0N18P-C34b93AVc2u-I44BX7uRLuobS0kkQyXudXCw/edit?usp=sharing

Table 18 presents the number of experts who decided which threats might be associated with disclosing the CTI dataset when sharing with trusted entities. As shown in Table 18 the set of possible threats has been reduced due to the increase of trust level among the sharing organisations. However, the result still shows that the list we have proposed in Table 11 is very similar to the experts' selections in Table 18.

Table 18 UC2-Part2-Threat Summary

Threat	Count	Threat	Count
Social engineering	1	Loss of reputation	5
Failure to meet contractual requirements	3	Unauthorized physical access	0
Violation of laws or regulations	2	Failed business process	1
Compromising confidential information	3	Man-in-the-middle	0
Identity theft (Identity Fraud/ Account)	1	Terrorists attack	1
Abuse of authorizations	0	Targeted attacks (APTs etc.)	1
Misuse of information	2	Unauthorized activities	1
Generation and use of rogue certificates	0	Manipulation of information	1

For question Q2, eleven experts indicate that we cannot share this dataset, or we can share after applying specific security controls. This result indicates that we need to apply security controls before sharing this dataset in order to reduce the risk of sharing.
For questions Q3.1 and Q3.2 experts select values that should be anonymized or removed from the dataset before sharing. Many of the experts propose that we need to remove all personal information and victim information such as the organisations name. In this case the victim information is not related to the purpose of sharing which matches our model and evaluation. For question Q3.3, three experts gave answers which included Address, Date and Affected Assets. This indicates that some information needs to be grouped and aggregated before sharing as part of reducing the risk of sharing individual information. For question Q3.4, three experts indicate that some attributes should be encrypted, such as threat actor and TTPs information and we can use techniques that support operations on encrypted data such as homomorphic encryption and multiparty computation. Finally, for question Q4.1, nine experts indicate that the risks are between 5 and 4 which constitute a high level of risk. On the other hand, after applying the suggested controls, five experts suggest that the risk value would be between 1 and 2 which constitutes a low risk level. When sharing the CTI dataset with trusted entities, the overall value changed from a medium risk level to a low risk level. eight experts state that the risk value is between 2 and 4, and after applying the security controls, six state that it is between 1 and 2. Table 17 and Table 18 show that the number of selected individual threats in this use case is higher than the first use case. In addition, Table 13, Table 14 and Table 15 present that the total risk value of this use case is higher than the first use case risk value. This is rational due to the context of the second use case. The second use case is about an attack and threat actor targeting diplomatic institutions worldwide [21]. The threat actor developed their own malware for stealing sensitive information and used techniques such as valid accounts to get access to the victim network. From the questionnaire results we find that our model matches the experts' decisions. The risk value is high, so sharing this information publicly will put the

organisation at a higher risk. Therefore, sharing this dataset with trusted communities or applying multiparty computation to get the analytics result will decrease the sharing risk.

5 Threats to validity

In terms of the participants and sample size, 23 experts (3rd year PhD students, Academics and industrial practitioners all working in cybersecurity) participated in this study where their feedback and evaluation used to evaluate the model. The experts were introduced to the use cases they had in order to evaluate without a previous tutorial, so it is possible that the experts were not completely familiar with the cyber threat intelligence and cyber incident reports. We neither tracked the time of the evaluation nor created a controlled environment where experts are tracked more closely. Concerning maturation, we have started with four use cases to be validated by each expert, but we noticed that the participants became tired and did not complete the full use cases. Therefore, we just used fifteen experts to validate the two use cases. Finally, concerning the generalization, using academic and professional experts might help the generalization of the results to be used in the industrial context. On the other hand, we might need more use cases to be able to generalize to real-world cyber threat intelligence platforms.

6 Conclusion and Future Work

In this work, we present a new quantitative risk model for sharing CTI datasets. The main objective of this model is to develop a framework to support sharing decisions regarding which information to share, and with whom. We have extended our previous works, in [2] we performed a comprehensive analysis of incident reporting information through the STIX incident model to identify the threats of disclosing sensitive and identifying information and in [13] we addressed the legal risks associated with sharing datasets. Here we have identified the potential threats associated with sharing a CTI dataset, computed the severity for each property, and we propose an estimating of the likelihood of the threats in case of property disclosure. Finally, we have calculated the total risk score of sharing a CTI dataset, and we addressed all risks associated with the data which will be shared. Based on the risk value, the organisations can select appropriate privacy preserving techniques to reduce the risk of sharing. In order to evaluate the model, we have asked experts' opinions for risk identification and evaluation for three different use cases. As future work, we intend to consider the level of trust among the organisations which might be beneficial to implement the model to be included and integrated in existing cyber threat intelligence platform such as MISP [22]. Furthermore, the future work involves further assessment to confirm our risk assessment model practicality through applying it to more real-world scenarios.

References

[1] S. Katti, B. Krishnamurthy, and D. Katabi, “Collaborating against common enemies,” in Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC, 2005.

[2] A. Albakri, E. Boiten, and R. De Lemos, “Risks of Sharing Cyber Incident Information,” in Proceedings of the 13th International Conference on Availability, Reliability and Security - ARES 2018, 2018, pp. 1–10.

[3] European Union, “Regulation 2016/679 of the European parliament and the Council of the European Union of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/,” Official Journal of the European Communities, vol. 59, no. May. pp. 1–88, 2016.

[4] R. Lewis, P. Louvieris, P. Abbott, N. Clewley, and K. Jones, “Cybersecurity information sharing: A framework for information security management in UK SME supply chains,” in ECIS 2014 Proceedings - 22nd European Conference on Information Systems, 2014.

[5] J. Shin, H. Son, and G. Heo, “Cyber Security Risk Evaluation of a Nuclear I&C Using BN and ET,” Nucl. Eng. Technol., 2017.

[6] M. U. Aksu et al., “A quantitative CVSS-based cyber security risk assessment methodology for IT systems,” in Proceedings - International Carnahan Conference on Security Technology, 2017.

[7] G. Dickinson, “Enterprise Risk Management: Its Origins and Conceptual Foundation,” Geneva Pap. Risk Insur. Issues Pract., vol. 26, no. 3, pp. 360–366, 2001.

[8] ISO 27005, “Information Technology- Security techniques-Information security risk management,” 2011.

[9] NIST, “Guide for Conducting Risk Assessments - Information Security,” 2012.

[10] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, “Introduction to the OCTAVE Approach,” in Pittsburgh, PA, Carnegie Mellon University, 2003.

[11] ENISA, “ENISA Threat Landscape Report 2016: 15 Top Cyber-Threats And Trends,” 2017. [Online]. Available: https://goo.gl/N3xP1F. [Accessed: 25-Apr-2018].

[12] MITRE, “STIX Incident Model,” 2018. [Online]. Available: https://stixproject.github.io/data-model/1.2/incident/IncidentType/. [Accessed: 10-Dec-2019].

[13] A. Albakri, E. Boiten, and R. De Lemos, “Sharing Cyber Threat Intelligence Under the General Data Protection Regulation,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2019, vol. 11498 LNCS, pp. 28–41.

[14] S. E. Coull, C. V Wright, F. Monrose, M. P. Collins, M. K. Reiter, and others, “Playing Devil’s Advocate: Inferring Sensitive Information from Anonymized Network Traces.,” in NDSS, 2007.

[15] A. D. Kent and L. M. Liebrock, “Secure communication via shared knowledge and a salted hash in Ad-hoc environments,” in Proceedings - International Computer Software and Applications Conference, 2011.

[16] C. Gentry, “A fully homomorphic encryption scheme,” Stanford University, 2009.

[17] F. Armknecht et al., “A Guide to Fully Homomorphic Encryption,” Cryptol. ePrint Arch., 2015.

[18] A. C. Yao, “PROTOCOLS FOR SECURE COMPUTATIONS.,” in Annual Symposium on Foundations of Computer Science - Proceedings, 1982.

[19] D. Bogdanov, R. Talviste, and J. Willemson, “Deploying Secure Multi-Party Computation for Financial Data Analysis,” in Financial Cryptography and Data Security, 2012, vol. 7397, no. 8124, pp. 57–64.

[20] MITRE, “Red October.” [Online]. Available: https://github.com/STIXProject/schemas-test/blob/master/veris/. [Accessed: 09-Dec-2019].

[21] Kaspersky, “Attackers Created Unique, Highly-Flexible Malware to Steal Data and Geopolitical Intelligence from Target Victims’ Computer Systems, Mobile Phones and Enterprise Network Equipment.” [Online]. Available: https://www.kaspersky.com/about/press-releases/2013_kaspersky-lab-identifies-operation--red-october--an-advanced-cyber-espionage-campaign-targeting-diplomatic-and-government-institutions-worldwide. [Accessed: 25-Feb-2020].

[22] MISP-Project, “MISP,” 2016. [Online]. Available: http://www.misp-project.org/. [Accessed: 12-Dec-2017].