Incident Response Practices Across National CSIRTs: Results from an Online Survey

Sharifah Roziah Binti Mohd Kassim, Shujun Li and Budi Arief
Institute of Cyber Security for Society (iCSS) & School of Computing, University of Kent, Canterbury, UK
Email: {sm2212, S.J.Li, B.Arief}@kent.ac.uk

***Abstract*—The aim of this study is to obtain operational insights of real-world practices across national CSIRTs, concerning cyber incident reporting channels, ticketing tools, incident classification schemes, and ways to identify appropriate responses. An online survey involving 19 staff members of 17 national CSIRTs was conducted, leading to four major findings. First, multiple reporting channels are provided by national CSIRTs for prompt incident reporting. Second, free and open-source ticketing tools are popular among national CSIRTs for tracking reported incidents. Third, different incident classification schemes are used across national CSIRTs, indicating a lack of standardised approaches that can have important implications (for example, difficulties in cross-CSIRT information sharing). Fourth, for classifying incidents and identifying appropriate responses, manual approaches are used more than automated ones. We conclude that more cross-CSIRT efforts are needed to define a more standardised cyber incident classification scheme, and to develop more automated tools to support national CSIRTs' operations.**

***Index Terms*—CSIRT, computer security incident response team, national CSIRT, cyber incident, reporting channel, ticketing tool, incident classification, survey.**

I. Introduction

Cyber incidents continue to increase at an exponential rate [1–3], due to the increasing number of vulnerable systems, software connected to the internet and users lacking security awareness. According to the Kaspersky Security Bulletin 2020 [4], over 500 thousand users became victims of ransomware, including over 100 thousand corporate users and nearly 16 thousand users from small and medium-sized businesses (SMBs). Furthermore, the COVID-19 pandemic had expanded working from home, online learning and online shopping, leading to unforeseen new vulnerabilities [5], causing an increase of new threats and cyber attacks worldwide [6].

It has become technically challenging for victims to deal with all these incidents. The ever-evolving and increasing sophistication of hacking techniques – coupled with the nature of "always on, always connected" systems – mean that there is little time for organisations to apply patches before attacks take place [7]. The lack of resources, such as tools, data and security experts, further compound these challenges [8].

Current preventive measures are no longer sufficient to mitigate the increasing threat of cyber attacks [9, 10]. For example, some widely used technologies such as intrusion detection systems (IDSs) do not have the capability to respond and handle incidents, but only detect and give alerts about possible cyber attacks [11]. Faced with concerns about the current global threat landscape, organisations need to be more cyber-resilient and equipped with alternative approaches to defend against cyber attacks [12]. This includes having an effective team with relevant experience, as well as technical skills and capacity to respond effectively to cyber incidents.

In order to address these concerns, many organisations have set up a *computer security incident response team (CSIRT)* [13, 14], a *computer emergency response (or readiness) team (CERT)* [15] or a *cyber (or computer) incident response (or readiness) team (CIRT)* [16]. In this paper, we use the acronym CSIRT because it is more widely used in the research literature.

This paper focuses on *national CSIRTs*, which are established at the national level to respond to cyber incidents within their constituencies [15, 17–19]. They have received much attention due to their key role in safeguarding national infrastructures from cyber attacks. The EU NIS Directive (EU 2016/1148, https://eur-lex.europa.eu/eli/dir/2016/1148/oj), the first piece of EU-wide cyber security legislation, has legislated the establishment of national CSIRTs in every EU member state to safeguard from cyber attacks. Similarly, the International Telecommunication Union (ITU), a UN agency, considers that national CSIRTs play an important role in effectively resolving cyber attacks; as such, ITU actively helps UN member states without a national CSIRT to establish one [16]. National CSIRTs are also entrusted at the national level to respond to cyber incidents and provide appropriate support to victims in a timely manner [15, 20–22]. A list of national CSIRTs from around the world is available on the websites of the CERT/CC of Carnegie Mellon University [23] and on the website of ITU [24].

Nonetheless, to the best of our knowledge, there is only limited existing research on how different national CSIRTs handle incident reporting and responses. In particular, there is a lack of information regarding low-level details such as how they classify incidents and how they decide what to do after receiving and investigating a reported incident. Instead, most research in the current literature focused on information sharing between CSIRTs [25], establishment of CSIRTs [9, 26], operational practices in organisational CSIRTs [27, 28], and management practices of CSIRTs [13, 14]. As a result, only limited insights are available for researchers and practitioners to understand operational practices of national CSIRTs. These limitations can cause negative consequences – for example, the existence of different practices can create barriers for cross-CSIRT collaboration.

The above observations have been echoed in other areas of cyber security, for example, some researchers found a lack of empirical studies on how security practitioners respond to cyber incidents [29]. While some researchers have started and studied operational practices of CSIRTs [30, 31], this research area remains under-studied. The present study aims to address the above-mentioned research gaps.

In this work, we used an online survey method to understand and compare operational practices of different national CSIRTs. We used purposive sampling to invite staff members from multiple national CSIRTs, in order to obtain more generalised findings for different national CSIRTs.

The overall aim of our study is *to obtain operational insights of real-world practices at different national CSIRTs*, in particular concerning information on *incident reporting channels*, *ticketing tools*, *incident classification schemes*, as well as *the approaches used in classifying incidents and identifying the appropriate response to a reported incident*. Our concrete **research questions** (RQs) are the following:

- RQ1: What are the reporting channels provided by national CSIRTs to facilitate reporting of cyber incidents in their constituency?
- RQ2: What are the types of ticketing tools used to record, organise and keep track of reported incidents, digitally, within national CSIRTs?
- RQ3: What are the classification schemes used across national CSIRTs to classify reported incidents and how is this done?
- RQ4: How do national CSIRTs identify appropriate responses to reported incidents?

The study makes the following main **contributions** to the existing body of knowledge:

- It outlines different types of cyber incident reporting channels provided by national CSIRTs.
- It provides a better understanding of national CSIRTs' operational practices in handling reported cyber incidents.
- It lays the foundation for some future research and provides development directions to different stakeholders, including national CSIRTs for improving their handling processes (for example, agreeing on a more standardised incident classification scheme across national CSIRTs), software developers and vendors for developing more useful tools for national CSIRTs, and researchers for conducting more targeted research (for example, developing more advanced machine learning methods for incident classification and response recommendation).

The rest of this paper is organised as follows. Section II provides an overview of previous work on incident reporting channels, ticketing tools, incident classification schemes and approaches used in classifying and identifying technical solutions for incidents. Section III explains the method used in the study, the recruitment of participants and the data analysis strategy. Section IV presents the results from the study, while Section V discusses the interpretation and the implications of the results, as well as the limitations of the study. Section VI concludes the paper and provides several suggestions for future research.

II. Related Work

Penedo (2006) [32] reported that email addresses and web forms were provided by the national CSIRT of Portugal (CERT.PT) for their citizens to report cyber incidents, while telephone calls and faxes were used for communication with victims reporting incidents. This practice conforms to the "Incident Handling Guides" defined by the US National Institute of Standards and Technology (NIST), which encourages organisations to publish a phone number and an email address for individuals and organisations to report incidents [33]. Penedo also highlighted the importance of ticketing tools such as AIRT [34] and RTIR [35] for tracking, annotating and keeping audit trails of all reported incidents. It is not clear from Penedo's work whether CERT.PT actually used these tools. The study mentioned that incidents can be classified into generic types including denial of service (DoS), malicious code, copyright infringement, non-authorised access, spam, and intrusion attempt.

Similar to the incident reporting channels reported in [32], Metzger et al. (2011) [27] stated that incidents were reported through emails, phone calls, faxes to the Liebniz Supercomputing Centre CSIRT (LRZ CSIRT), an organisational CSIRT in Germany. The study mentioned about the use of a centralised ticketing tool to generate "trouble tickets", which refer to reported incidents. However, details about the ticketing tool were not included in [27]. The study also mentioned that manual and automatic approaches were applied at the LRZ CSIRT to identify appropriate responses to reported incidents.

Koivunen (2010) [36] reported that incidents were discovered by the national CSIRT of Finland (CERT-FI) from monitoring systems and from security data feeds generated by other organisations such as Shadowserver Foundation [37] and Team Cymru (https://team-cymru.com/), but there was no mention of how individuals and organisations in Finland reported incidents to CERT-FI. The study mentioned that incidents received from system monitoring were recorded and processed using ticketing tools like CERT-FI Autoreporter [38] and AbuseHelper [30].

Riebe et al. (2021) [19] identified that incident reporting channels (emails and phone calls) were provided by Germany's national CSIRT (CERT Bund) and state-level CERTs. The study also mentioned that the ticketing tool OTRS [39] was used to collect further evidence about reported incidents, and for responding to reported incidents.

Villegas-Ch. et al. (2021) [9] pointed out the importance of ticketing tools on top of other investigative tools to include details of reported incidents and append other relevant artefacts in the incident tracking system. The authors stressed that ticketing tools need to be able to keep details of reported incidents for future retrievals and to update stakeholders of the number of incidents reported and resolved in the CSIRTs. Additionally, they also expressed the importance of classifying

incidents into different types of incidents, but they did not give any concrete incident classification schemes.

Some early efforts in classifying incidents began in the late 1990s, which includes the research work by John Howard, a PhD student at Carnegie Mellon University, USA [40]. Howard later moved to Sandia National Laboratories and developed a classification scheme "A Common Language for Computer Security Incidents" [41]. Though it is not a comprehensive classification scheme, it nonetheless has a minimum set of "high-level" terms, indicating their relationship (a taxonomy), which helps in classifying incidents. However, Howard's scheme is quite old (defined 13 years ago), suggesting the need for more modernised schemes. Our observation is echoed by Ibrishimova (2018) [42], who stated that the cyber incident classification scheme needs to be comprehensive and reflects the state of the art.

All the related work reviewed above has highlighted some common problems, namely the lack of sufficient details about cyber incident reporting channels, the limited information about incident handling ticketing tools, as well as some inconsistencies in incident classification schemes or the approaches used for classifying incidents and for identifying appropriate responses. Furthermore, the mention of reporting channels, ticketing tools, classification schemes and the approaches used for classifying incidents are not comprehensive, as they represent only a smaller fragment of a large study. Additionally, most of the studies represent a single national CSIRT or an organisational CSIRT and are not representative of national CSIRTs as a whole, in other words, there is a lack of generalisability regarding their findings. This generalisability problem was also noticed by other researchers. For instance, Riebe et al. (2021) [19] mentioned that the results of their study cannot be directly generalised to provide a grounded assessment on the situation in other nations as their study was confined to a single constituency.

III. Methodology

The study used survey as the data collection method and online survey questionnaire as the instrument. Surveys (especially online surveys) have been widely used by researchers in various fields – including cyber security – to collect useful information from recruited human participants [43–48]. We found this method to be most appropriate for our study to increase the diversity of human participants recruited and the national CSIRTs they represent in different parts of the world.

The design of our online survey followed all items in the "Checklist for Reporting Results of Internet E-Surveys" (CHERRIES) [49]. Considering the security and privacy of the data collection, we used the Jisc online survey system (https://www.onlinesurveys.ac.uk/), which is compliant with the EU/UK General Data Protection Regulation (GDPR) and with the CHERRIES. The study received approval from the University of Kent's Central Research Ethics Advisory Group. On the first page of the online survey, we provided participants with a Participant Information Sheet (PIS) with details of the study and assurance to safeguard participants' personal data, by complying with the GDPR. An online consent form, which was also part of the online survey, was used to obtain participants' consent in our study. The online survey ran from 14 May to 15 July, 2021.

The survey questionnaire consists of six questions that directly relate to our research questions. Each of the six questions cover one of the following aspects: 1) cyber incident reporting channels provided, 2) level of categorising incidents, 3) the incident classification scheme(s) used, 4) the ticketing system used, 5) approaches to categorising incidents, and 6) approaches to identifying appropriate responses to incidents. Four of the six questions (1, 2, 5 and 6) are multiple-choice questions, including an "Other" option and an open-ended text box for participants to fill in further details. The third question asked participants if they used the same incident classification scheme at MyCERT (where the first author of the paper works), and asked them to provide further details of the scheme their national CSIRT used if that differs from MyCERT's. The fourth question asked participants to enter free-formatted texts to describe the ticketing system or a similar system such as a customer management system. The online survey questionnaire can be found at https://cyber.kent.ac.uk/research/CSIRTs/OIC-CERT-JCS-survey-questionnaire.html.

A. Recruitment of Participants

We used purposive sampling to recruit staff members of selected national CSIRTs. This is a technique that uses selected human participants to obtain in-depth information about the study under investigation, based on their knowledge and experience. Purposive sampling is a non-probability sampling procedure, where participants are selected because they satisfy specific characteristics needed for participation in the study [50]. This also allows to better align the sampling to the aims and objectives of a study, therefore improving trustworthiness and validity of the data and result [51]. For our study, we sampled 19 staff members from 17 national CSIRTs, as detailed in Table I. Fifteen of the participants were recruited using contacts from a past study we conducted [52], for which they gave their consent to be contacted for future research. We also recruited four participants through the first author's personal contacts within the CERT/CC of Carnegie Mellon University, USA (https://www.cert.org/) and the Forum of Incident Response Security Team (FIRST) (https://www.first.org/).

B. Data Analysis

We analysed the data using both quantitative and qualitative methods. For the quantitative part, we used descriptive statistics to understand, explore, describe and summarise the data, which consist of free-formatted answers to four open-ended questions [53]. We did not consider inferential statistics as we were not testing any hypotheses or theories. Descriptive statistics was preferred because it is more manageable and the results are easier to understand [54]. For the qualitative part, we analysed answers to the open-ended questions on reporting channels, ticketing systems and incident classification schemes. Such answers were read, categorised, and

TABLE I
LIST OF PARTICIPANTS AND THE NATIONAL CSIRTS THEY WERE AFFILIATED WITH

National CSIRT	Country/Region	#(Participants)
MyCERT	Malaysia	3
CERT.at	Austria	1
BGD eGOV CIRT	Bangladesh	1
CERT.hr	Croatia	1
CSIRT-RD	Dominican Republic	1
EcuCERT	Ecuador	1
CERT-FR	France	1
JpCERT/CC	Japan	1
NCSC-NL	Netherlands	1
CERT-PY	Paraguay	1
RNCSIRT	Portugal	1
SKCERT	Slovakia	1
INCIBE.CERT	Spain	1
Sri Lanka CERT	Sri Lanka	1
SWITCH-CERT	Switzerland	1
TwCERT/CC	Taiwan	1
US-CERT	USA	1
Total		**19**

summarised by the first author of the paper. For data from multiple participants of the same national CSIRT (only for MyCERT), the results were checked for consistency and there were no contradicting answers.

IV. RESULTS

This section presents the findings from the survey, following the order of research questions outlined in Section I.

A. Types of Incident Reporting Channels

RQ1 of the study is for gaining insights about cyber incident reporting channels provided by national CSIRTs. The data showed that majority of national CSIRTs (12, 70.6%) provide three incident reporting channels consists of email, telephone and online form. This is consistent with previous studies on national CSIRTs [32] and those on organisational CSIRTs [27]. Interestingly, the data also revealed that email is the most common reporting channel provided by national CSIRTs (17, 100%), followed by telephone (13, 76.5%) and online form (12, 70.6%). Other less common reporting channels provided by national CSIRTs include fax (1, 5.9%), face-to-face (1, 5.9%), SMS messages (1, 5.9%), paper (1, 5.9%) and mobile application (1, 5.9%). The overall descriptive statistics are shown in Figure 1. Our study did not ask a question exploring the reasons behind the given answers regarding incident reporting channels. However, based on the first author's experience as a staff member of MyCERT, the national CSIRT of Malaysia, we understand that it is because emails give more flexibility to reporters in terms of describing an incident and appending relevant artefacts as attachments.

B. Ticketing Systems Used

RQ2 of the study is for gaining insights into ticketing systems used by national CSIRTs for tracking incident handling.

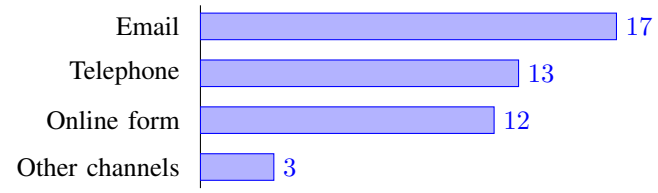

Fig. 1. Incident reporting channels mentioned by participants in the survey

All participants responded that ticketing systems are used in their national CSIRTs to record and keep track of reported incidents. This finding is consistent with previous studies [9, 27], which found that ticketing systems had been used by organisational CSIRTs to record, centralise, organise and keep track of reported incidents. Our data also revealed that nearly half of the 17 national CSIRTs used an open-source ticketing system called RTIR (Request Tracker for Incident Response, https://bestpractical.com/rtir) (8, 47.1%), followed by a commercial system called OTRS (Online Ticket Request System, https://www.otrs.com) (3, 17.65%), in-house built tools (3, 17.65%), two other commercial systems – RT (Request Tracker, https://bestpractical.com/rt) and BMC Remedy ITSM https://www.bmc.com/it-solutions/remedy-itsm.html (1 for each, 5.89%), and an unnamed open-source system (1, 5.89%), as illustrated in Figure 2.

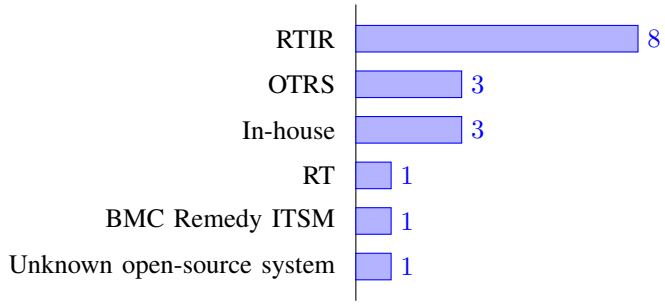

Fig. 2. Types of incident-management ticketing tools used by national CSIRTs

C. Incident Classification

RQ3 of the study is for finding out how national CSIRTs classify reported incidents. The survey data indicated that a majority (12, 70.6%) of the 17 national CSIRTs used manual approaches for classifying reported incidents, and the other five (29.4%) used hybrid (combining manual and automated) approaches. None of the 17 national CSIRTs used automated approaches only. The detailed statistics are shown in Figure 3.

One participant responded that for hybrid approaches, free tools such as IntelMQ (https://github.com/certtools/intelmq) were used to automatically classify some incidents that are reported by monitoring automated systems (for example, security feeds), while incidents reported by individuals and organisations were classified manually. Another participant mentioned that for hybrid approaches, automated approaches were performed during the initial stage of incident classification while the final classification was confirmed by assessing

each reported incident manually. This finding is largely in good agreement with a previous study that found a correlation between successful cyber incident responses with CSIRT staff's interventions and abilities to conduct reasoning during incident response processes, which is done manually [55]. This finding is also in agreement with another piece of past research that showed the importance of human interventions on top of machine automation during cyber incident responses [21].

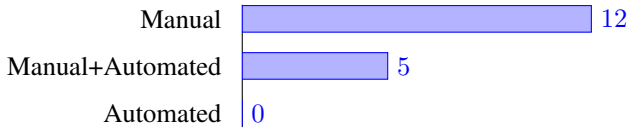

Fig. 3. Reported approaches for incident classification

For RQ3, we are also interested in knowing about the scheme used by national CSIRTs to classify incidents. The survey data showed that participants from a majority (12, 70.6%) of the 17 national CSIRTs reported the use of a hierarchical incident classification scheme, including high-level types and sub-types, while those from the rest, five (29.4%) national CSIRTs classified incidents based on a short and linear list of general incident types.

Our survey data also showed that 10 out of the 17 national CSIRTs (58.8%) used their self-developed cyber incident classification schemes, three (17.6%) used the ENISA's Reference Incident classification Taxonomy (https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy/), and participants from the rest (four) national CSIRTs (23.5%) did not disclose the scheme their national CSIRT used. Table II shows the incident classification schemes used by national CSIRTs, as reported by our participants.

D. Approaches to Identifying Appropriate Incident Responses

RQ4 of our study is for gaining insights into the approaches used by national CSIRTs for identifying appropriate responses to reported incidents. As shown in Figure 4, the survey data revealed that 14 out of the 17 national CSIRTs (82.4%) used manual approaches to identify appropriate responses, two (11.8%) combined manual and automated approaches, and the last one participant did not mention the approach(es) used.

The most interesting observation is that none of the 17 national CSIRTs surveyed reported relying solely on automated approaches. Perhaps this was not surprising, since previous studies have shown that cyber incident response tasks are very human-dependent due to the complexity of the tasks, thus making it very challenging to automate [11]. According to one participant, manual approaches were used to identify appropriate responses for incidents reported by individuals and new threats reported by external researchers, while hybrid (combining automated and manual) approaches were used for incidents generated by automated monitoring systems.

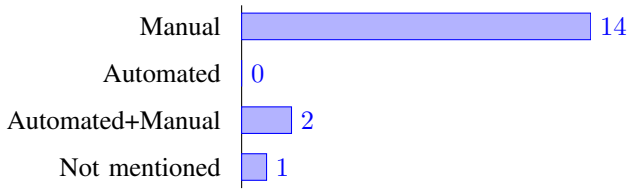

Fig. 4. Approaches for identifying appropriate responses to reported incidents

V. Further Discussions

A. Key Findings

In this subsection, we summarise the key findings for the four research questions we defined, and discuss the implications for future research and development work.

1) Incident Reporting Channels Provided (RQ1): The main finding here is that national CSIRTs largely provide multiple incident reporting channels, especially email, telephone and online form. A few national CSIRTs still provide very traditional channels such as face-to-face, paper and fax, probably to serve citizens and organisations who cannot or choose not to use the three main channels. While using multiple channels helps support citizens and organisations with diverse needs, it can complicate the incorporation of incidents reported via different channels into the same ticketing system and the same processing pipeline – this means more research into and development of suitable tools are required.

2) Types of Ticketing Systems Used (RQ2): The main finding here is the observation that all of the surveyed national CSIRTs reported the use of a ticketing system for cyber incident handling. Free and open-source ticketing tools are popular among national CSIRTs, indicating that – at least for this part – dependencies on (potentially expensive) commercial tools will not be a factor affecting the setup of new national CSIRTs. However, it remains unclear if such ticketing systems have been fully validated, or if they can support all the reporting channels effectively. This is part of a bigger research gap regarding validation of free and open-source tools used by national CSIRTs, reported recently by us in another study [52].

3) Incident Classification Schemes and Approaches Used (RQ3): For the first part of this RQ, we noticed the use of different incident classification schemes by different national CSIRTs, indicating that a more standardised classification scheme would be very useful for facilitating more effective information sharing and other types of collaboration between national CSIRTs. It would be better if this effort were initiated by cross-CSIRT bodies such as FIRST or ITU, or international standardisation bodies such as ISO/IEC or NIST. For the second part of the RQ, the main finding is that all national CSIRTs used manual or hybrid approaches to classify reported incidents. We noticed that the use of automated approaches was still limited, so developing more advanced automated incident classification methods and tools will be an important direction for future research and development.

4) Approaches Used for Identifying Appropriate Incident Responses (RQ4): For this RQ, our main finding is the dom-

TABLE II
LIST OF INCIDENT CLASSIFICATION SCHEMES USED BY NATIONAL CSIRTS

National CSIRT	Country/Region	Classification Scheme
CERT.hr	Croatia	https://www.cert.hr/wp-content/uploads/2018/06/National-taxonomy-for-computer-security-incidents.pdf
CSIRT-RD	Dominican Republic	https://cncs.gob.do/csirt-rd/recursos/guias-y-recomendaciones/
EcuCERT	Ecuador	https://www.arcotel.gob.ec/wp-content/uploads/2018/11/Catalogo_y_priorizacion_vulnerabilidades.pdf
JpCERT/CC	Japan	https://www.jpcert.or.jp/english/doc/IR_Report202Q3_en.pdf
MyCERT	Malaysia	https://www.mycert.org.my/portal/full?id=44976922-60b2-4740-8cbf-0839907fcf8c
CERT-PY	Paraguay	https://www.cert.gov.py/servicios/gestion-de-incidentes-ciberneticos
RNCSIRT	Portugal	https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.0.pdf
SKCERT	Slovakia	https://www.csirt.gov.sk/graf-83d.html
TwCERT/CC	Taiwan	https://www.twncert.org.tw/Incident_Handling_Statistics
US-CERT	USA	https://us-cert.cisa.gov/CISA-National-Cyber-Incident-Scoring-System
CERT.at	Austria	https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy/
SWITCH-CERT	Switzerland	
INCIBE.CERT	Spain	
BGD eGOV CIRT	Bangladesh	Undisclosed
NCSC-NL	Netherlands	
Sri Lanka CERT/CC	Sri Lanka	
CERT-FR	France	

inating use of manual approaches for identifying appropriate responses to reported incidents.

Our work and past research [11, 21, 55, 56] showed that it is important to involve CSIRT staff in the incident response processes. To help support staff of national CSIRTs, we can develop more advanced decision-support methods and tools, for example, human-in-the-loop machine learning method reported in [57], which allow security analysts to work more closely with AI models.

B. Limitations

This study has a couple of limitations. First, the number of participants (19) and the number of national CSIRTs involved (17) are both relatively low, which might affect the generalisability of the results reported. Conducting a large-scale study involving more national CSIRTs – potentially during large conferences of national CSIRTs such as those organised by FIRST – can be useful.

Second, our study focused on collecting factual information about operational practices at national CSIRTs, not the reasons behind such practices. To this end, some follow-up empirical studies such as semi-structured interviews and focus groups will be very helpful to extend the reported work.

VI. CONCLUSION

Through an online survey involving 19 staff members of 17 national CSIRTs, this study came up with the following four main findings regarding incident handling practices at different national CSIRTs. First, multiple reporting channels are provided by national CSIRTs to ensure incidents are promptly reported, detected and dealt with. Second, free and open-source ticketing tools are largely used in national CSIRTs to keep track of cyber incidents; however, the validity of these tools remains questionable. Third, different incident classification schemes are used across national CSIRTs, indicating a lack of a standardised incident classification scheme for national CSIRTs. Fourth, manual approaches are predominantly used by national CSIRTs to classify incidents and to identify appropriate responses to incidents, indicating that incident response tasks still largely depend on manual tasks. These four findings help inform future research and development activities of national CSIRTs and other stakeholders, in particular towards (i) cross-CSIRT efforts in developing a more standardised incident classification scheme, and (ii) the development of more automated tools that can help national CSIRT staff to classify incidents and identify appropriate responses more effectively and efficiently.

REFERENCES

[1] APCERT, "APCERT annual report 2019," Tech. Rep., 2020. [Online]. Available: https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2019.pdf

[2] Verizon, "2020 data breach investigations report," Tech. Rep., 2020. [Online]. Available: https://enterprise.verizon.com/en-gb/resources/reports/dbir/

[3] PricewaterhouseCoopers, "Cyber threats 2019: A year in retrospect," Tech. Rep., 2020. [Online]. Available: https://www.pwc.co.uk/issues/cyber-security-services/insights/cyber-threats-2019-retrospect.html

[4] Kaspersky, "Kaspersky security bulletin 2020. statistics," Tech. Rep., 2020. [Online]. Available: https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_en.pdf

[5] E. B. Korn, D. M. Fletcher, E. M. Mitchell, A. A. Pyke, and S. M. Whitham, "Jack pandemus – cyber incident and emergency response during a pandemic," *Information Security Journal: A Global Perspective*, vol. 30, no. 5, pp. 294–307, 2021.

[6] G. Iakovakis, C.-G. Xarhoulacos, K. Giovas, and D. Gritzalis, "Analysis and classification of mitigation tools against cyberattacks in COVID-19 era," *Security and Communication Networks*, vol. 2021, pp. 3 187 205:1–3 187 205:21, 2021.

[7] W. A. Arbaugh, W. L. Fithen, and J. McHugh, "Windows of vulnerability: A case study analysis," *Computer*, vol. 33, no. 12, pp. 52–59, 2000.

[8] Z. Pokorny, Ed., *The Threat Intelligence Handbook: Moving Toward a Security Intelligence Program*, 2nd ed. CyberEdge Group, LLC, 2019. [Online]. Available: https://go.recordedfuture.com/book-2

[9] W. Villegas-Ch., I. Ortiz-Garces, and S. Sánchez-Viteri, "Proposal for an implementation guide for a computer security incident response team on a university campus," *Computers*, vol. 10, no. 8, pp. 102:1–102:23, 2021.

[10] S. Mitropoulos, D. Patsos, and C. Douligeris, "On incident handling and response: A state-of-the-art approach," *Computers & Security*, vol. 25, no. 5, pp. 351–370, 2006.

[11] S. H. Hashemi, M. Babaeizadeh, M. Nowruzi, H. H. Jazi, M. Shahmoradi, and E. B. B. Samani, "A comprehensive semi-automated incident handling workflow," in *Proceedings of the 6th International Symposium on Telecommunications*. IEEE, 2012, pp. 1065–1070.

[12] M. Tariq, B. Aslam, I. Rashid, and A. Waqar, "Cyber threats and incident response capability- a case study of Pakistan," in *Proceedings of the 2013 2nd National Conference on Information Assurance*. IEEE, 2013, pp. 15–20.

[13] R. Ruefle, A. Dorofee, D. Mundie, A. D. Householder, M. Murray, and S. J. Perl, "Computer security incident response team development and evolution," *IEEE Security & Privacy*, vol. 12, no. 5, pp. 16–26, 2014.

[14] M. J. West-Brown, D. Stikvoort, K.-P. Kossakowski, G. Killcrece, R. Ruefle, and M. Zajicek, "Handbook for computer security incident response teams (CSIRTs)," Software Engineering Institute, Carnegie Mellon University, Pittsburg, USA, Tech. Rep. CMU/SEI-2003-HB-002, 2003. [Online]. Available: https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf

[15] R. A. Ahmad and M. S. Hashim, "The organisation of Islamic Conference—Computer Emergency Response Team(OIC-CERT): Answering cross border cooperation," in *Proceedings of the 2011 2nd Worldwide Cybersecurity Summit*. IEEE, 2011. [Online]. Available: https://ieeexplore.ieee.org/document/5978783

[16] International Telecommunication Union (ITU), "National CIRTs," Web page. [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx

[17] J. Wiik, J. J. Gonzalez, and K. P. Kossakowski, "Effectiveness of proactive CSIRT services," in *Proceedings of the 18th Annual FIRST Conference*. FIRST, 2006. [Online]. Available: https://www.first.org/conference/2006/papers/kossakowski-klaus-papers.pdf

[18] H. Duijnhoven, T. van Schie, and D. Stikvoort, *Stimulating the development and maturity enhancement of national CSIRTs*. TNO Publication, 2021. [Online]. Available: https://repository.tno.nl//islandora/object/uuid:e1ba969e-7ab4-4bd5-83fb-7c029db15265

[19] T. Riebe, M.-A. Kaufhold, and C. Reuter, "The impact of organizational structure and technology use on collaborative practices in computer emergency response teams: An empirical study," *Proceedings of the ACM on Human-Computer Interaction*, vol. 5, no. CSCW2, pp. 478:1–478:30, 2021.

[20] O. Hellwig, G. Quirchmayr, E. Huber, G. Goluch, F. Vock, and B. Pospisil, "Major challenges in structuring and institutionalizing CERT-communication," in *Proceedings of the 2016 11th International Conference on Availability, Reliability and Security*, no. 2. IEEE, 2016, pp. 661–667.

[21] M. Nyre-Yu, R. S. Gutzwiller, and B. S. Caldwell, "Observing cyber security incident response: qualitative themes from field research," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 63, no. 1, pp. 437–441, 2019.

[22] C. J. Alberts, A. J. Dorofee, G. Killcrece, R. Ruefle, and M. Zajicek, "Management processes for CSIRTs: A work in progress," Software Engineering Institute, Carnegie-Mellon University, Pittsburgh, Pennsylvania, USA, Tech. Rep. CMU/SEI-2004-TR-015, 2004. [Online]. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7153

[23] Software Engineering Institute, Carnegie Mellon University, "National Computer Security Incident Response Teams (CSIRTs): List of national CSIRTs," Web page, 2021. [Online]. Available: https://www.sei.cmu.edu/our-work/cybersecurity-center-development/national-csirts/

[24] ITU, "National CIRTs world-wide," Web page, 2021. [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/CIRT_Status.pdf

[25] A. Ahmad, J. Hadgkiss, and A. B. Ruighaver, "Incident response teams – challenges in supporting the organisational security function," *Computers & Security*, vol. 31, no. 5, pp. 643–652, 2012.

[26] Y. M. Wara and D. Singh, "A guide to establishing computer security incident response team (CSIRT) for National Research and Education Network (NREN)," *African Journal of Computing & ICT*, vol. 8, no. 2, 2015.

[27] S. Metzger, W. Hommel, and H. Reiser, "Integrated security incident management – concepts and real-world experiences." IEEE, 2011, pp. 107–121.

[28] P. Mana and V. Friligkos, "EUROCONTROL/EATM-CERT services-supporting aviation to better manage cyber threats," in *Proceedings of the 2019 Integrated Communications, Navigation and Surveillance Conference*. IEEE, 2019, pp. 1B1:1–1B1:15.

[29] R. Werlinger, K. Muldner, K. Hawkey, and K. Beznosov, "Preparation, detection, and analysis: the diagnostic work of IT security incident response," *Information Management & Computer Security*, vol. 18, no. 1, pp. 26–42, 2010.

[30] M. Krstić, M. Čabarkapa, and A. Jevremović, "Machine learning applications in computer emergency response team operations," in *Proceedings of the 2019 27th*

Telecommunications Forum. IEEE, 2019.

[31] J. M. Spring and P. Illari, "Review of human decision-making during computer security incident analysis," *Digital Threats: Research and Practice*, vol. 2, no. 2, pp. 11:1–11:47, 2021.

[32] D. Penedo, "Technical infrastructure of a CSIRT," in *Proceedings of the 2006 International Conference on Internet Surveillance and Protection*. IEEE, 2006, pp. 27:1–27:6.

[33] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide," National Institute of Standards and Technology, U.S. Department of Commerce, NIST Special Publication 800-61 Revision 2, 2012.

[34] K. Leune and S. Tesink, "Designing and developing an application for incident response teams," in *Proceedings of the 2006 Forum for Incident Response Teams Conference*. FIRST, 2006.

[35] JANET CSIRT, "RTIR incident handling work-flow," Technical Report JANET(UK) WI/JCSIRT/003, 2011. [Online]. Available: https://static1.squarespace.com/static/567aecb71115e084cc4cee26/t/579263da59cc68ec9b749e23/1469211612764/janet-workflow.pdf

[36] E. Koivunen, ""why wasn't I notified?": Information security incident reporting demystified," in *Information Security Technology for Applications: 15th Nordic Conference on Secure IT Systems, NordSec 2010, Espoo, Finland, October 27-29, 2010, Revised Selected Papers*, ser. Lecture Notes in Computer Science, vol. 7127. Springer, 2010, pp. 55–70.

[37] K. Kaemarungsi, N. Yoskamtorn, K. Jirawannakool, N. Sanglerdsinlapachai, and C. Luangingkasut, "Botnet statistical analysis tool for limited resource computer emergency response team," in *Proceedings of the 2009 5th International Conference on IT Security Incident Management and IT Forensics*. IEEE, 2009, pp. 27–40.

[38] A. Leppänen and T. Kankaanranta, "Co-production of cybersecurity: A case of reported data system break-ins," *Police Practice and Research*, vol. 21, no. 1, pp. 78–94, 2020.

[39] P. Kácha, "OTRS: streamlining CSIRT incident management workflow," in *Proceedings of the WSEAES 13th International Conference on Computers*. WSEAS, 2009, pp. 121–126.

[40] R. Slayton and B. Clarke, "Trusting infrastructure: The emergence of computer security incident response, 1989–2005," *Technology and Culture*, vol. 61, no. 1, pp. 173–206, 2020.

[41] J. D. Howard and T. A. Longstaff, "A common language for computer security incidents," Sandia National Laboratories, Sandia Report SAND98-8667, 1998. [Online]. Available: https://www.osti.gov/servlets/purl/751004

[42] M. D. Ibrishimova, "Cyber incident classification: issues and challenges," in *Advances on P2P, Parallel, Grid, Cloud and Internet Computing: Proceedings of the 13th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC-2018)*. Springer, 2018, pp. 469–477.

[43] R. D. Goddard and P. Villanova, "Designing surveys and questionnaires for research," in *The Psychology Research Handbook: A Guide for Graduate Students and Research Assistants*. SAGE, 2006, pp. 114–125.

[44] P. H. Rossi, J. D. Wright, and A. B. Anderson, Eds., *Handbook of Survey Research*. Academic Press, 2013.

[45] W. E. Saris and I. N. Gallhofer, Eds., *Design, Evaluation, and Analysis of Questionnaires for Survey Research*, 2nd ed. John Wiley & Sons, Inc., 2014.

[46] K. Kelley, B. Clark, V. Brown, and J. Sitzia, "Good practice in the conduct and reporting of survey research," *International Journal for Quality in Health Care*, vol. 15, no. 3, pp. 261–266, 2003.

[47] H. L. Ball, "Conducting online surveys," *Journal of Human Lactation*, vol. 35, no. 3, pp. 413–417, 2019.

[48] M. Callegaro, K. L. Manfreda, and V. Vehovar, *Web Survey Methodology*. SAGE, 2015.

[49] G. Eysenbach, "Improving the quality of web surveys: the checklist for reporting results of Internet e-surveys (CHERRIES)," *Journal of Medical Internet Research*, vol. 6, no. 3, 2004.

[50] J. Daniel, "Choosing between nonprobability sampling and probability sampling," *Sampling essentials: Practical guidelines for making sampling choices*, pp. 66–80, 2012.

[51] S. Campbell, M. Greenwood, S. Prior, T. Shearer, K. Walkem, S. Young, D. Bywaters, and K. Walker, "Purposive sampling: complex or simple? research case examples," *Journal of Research in Nursing*, vol. 25, no. 8, pp. 652–661, 2020.

[52] S. R. B. Mohd Kassim, S. Li, and B. Arief, "How national CSIRTs leverage public data, OSINT and free tools in operational practices: An empirical study," *Cyber Security: A Peer-Reviewed Journal*, vol. 5, no. 3, pp. 1–26, 2022.

[53] M. J. Fisher and A. P. Marshall, "Understanding descriptive statistics," *Australian Critical Care*, vol. 22, no. 2, pp. 93–97, 2009.

[54] M. Kaushik and B. Mathur, "Data analysis of students marks with descriptive statistics," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 2, no. 5, pp. 1188–1190, 2014.

[55] B. Schneier, "The future of incident response," *IEEE Security & Privacy*, vol. 12, no. 5, p. 96, 2014.

[56] M. Nyre-Yu, "Identifying expertise gaps in cyber incident response: Cyber defender needs vs. technological development," in *Proceedings of the 54th Hawaii International Conference on System Sciences*. University of Hawai'i, 2021, pp. 1978–1987.

[57] K. Veeramachaneni, I. Arnaldo, V. Korrapati, C. Bassias, and K. Li, "AI^2: Training a big data machine to defend," in *Proceedings of the 2016 IEEE 2nd International Conference on Big Data Security on Cloud*, 2016, pp.

49–54.