CYBER INCIDENT RESPONSE PRACTICES ACROSS NATIONAL CSIRTS' OPERATIONS: RESULTS FROM AN ONLINE SURVEY

Abstract: An online survey of 19 staff members of 17 national Computer Security Incident Response Teams (CSIRTs) was conducted to gain insights into the reporting channels, ticketing systems, classification schemes and approaches to facilitating cyber incident responses in national CSIRTs. The study led to four key findings of the operations in national CSIRTs with regard to cyber incident response. We conclude that more cross-CSIRT efforts are needed to define a standardised cyber incidents classification scheme. Additionally, further research is needed to develop more automated tools and procedures for the validation of tools to support national CSIRTs' incident response.

Research Aims

The aim of this study is to gain insights of real-world operational practices across national CSIRTs concerning reporting channels, ticketing tools, incident classification schemes, and approaches to identify appropriate responses to cyber incidents.

Research Questions

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?

Data Collection Method

In this study, survey was used as the method to collect data and the instrument used is online survey questionnaires. We used the Jisc online survey platform (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 with Ethics reference: (CREAG054-04-2021). An online consent form was used to obtain participants' consent in our study. The online survey ran from14 May to 15 July, 2021.

Data Analysis Method

The survey data was downloaded into the Researcher's computer from online survey platform for subsequent analysis. Descriptive statistics method was used to understand, explore, describe and summarise the data in numbers and percentage, without making inferences, illustrated in graphs.

Sampling strategy

We used purposive sampling to recruit staff members of selected national CSIRTs, who have wide knowledge and experiences in cyber incident response operations in national CSIRTs. In total, there were 19 participants from 17 national CSIRTs: three participants from Malaysia CSIRT, and one participant each from national CSIRTs of Austria, Bangladesh, Croatia, Dominican Republic, Ecuador, France, Japan, Netherlands, Paraguay, Portugal, Slovakia, Spain, Sri Lanka, Switzerland, Taiwan and USA.

Validity of Data

Purposive sampling was used to obtain in-depth information about the study under investigation, therefore improving trustworthiness and validity of the data and findings.

University of Kent | Computing

Result: Different Incident Classification Schemes Across National CSIRTs

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 SWITCH-CERT INCIBE.CERT	Austria Switzerland Spain	https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy/
BGD eGOV CIRT NCSC-NL Sri Lanka CERT/CC CERT-FR	Bangladesh Netherlands Sri Lanka France	Undisclosed

Result: Patterns in Reporting Channels, Ticketing Systems, Reporting Approaches and Approach to Identify Responses Across National CSIRTs

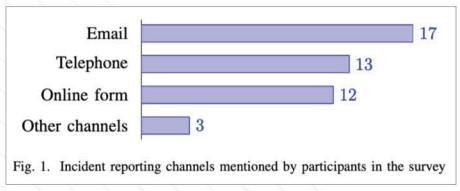

Fig. 1. Incident reporting channels mentioned by participants in the survey

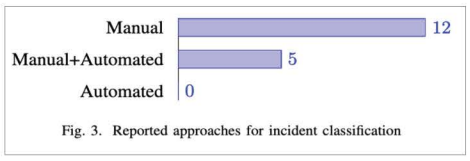

Fig. 3. Reported approaches for incident classification

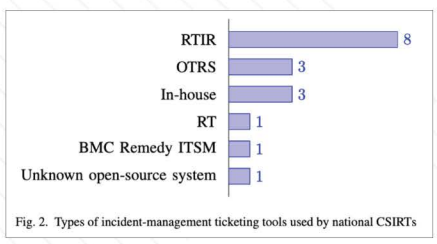

Fig. 2. Types of incident-management ticketing tools used by national CSIRTs

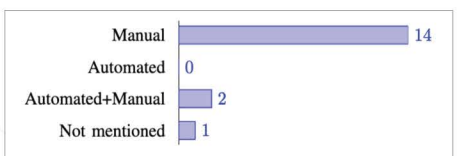

Fig. 4. Approaches for identifying appropriate responses to reported incidents

Discussion: Key Findings

1. Incident Reporting Channels	2. Types of Ticketing Systems Used	3. Incident Classification Schemes	4. Approaches to Identify Responses to Incident
• Email, telephone and online form are used across national CSIRTs to facilitate incident reporting. • More research into development of suitable tools to consolidate incident reports from multiple channels into a incident ticketing system.	• Free and open-source ticketing tools are more popular among national CSIRTs compared to commercial tools. • A research gap lies in validation of free and open-source tools, i.e. ticketing tools used in national CSIRTs.	• Different incident classification schemes are used across national CSIRTs -- more standardised classification scheme is necessary. • Manual and hybrid approaches are used to classify compared to automated approach – a limitation in current practices.	• Manual approaches predominantly used for identifying responses to incidents in national CSIRTs compared to hybrid or automated approaches.

Conclusion and Recommendation

1. The findings help inform future research and development initiatives, needed for national CSIRTs to improve cyber incident responses.
2. Cross-CSIRT efforts with relevant organisations in developing a more standardised incident classification scheme is recommended. This ensures a common understanding of cyber incident classifications among national CSIRTs.
3. Development of more automated tools is needed in helping national CSIRTs' staff to classify incidents and identify appropriate responses to cyber incidents, more effectively and efficiently.
4. Development of procedures for evaluation of tools in national CSIRTs is suggested, to ensure only quality tools are used to facilitate incident responses.

Authors: Sharifah Roziah Binti Mohd Kassim, Professor Shujun Li & Dr Budi Arief
Contact details: sm2212@kent.ac.uk

Full Paper: https://www.oic-cert.org/en/journal/vol-4-issue-1/5.html#.YqN-IJBBzlw