How National CSIRTs Operate: Personal Observations and Opinions from MyCERT

Sharifah Roziah Binti Mohd Kassim*†, Solahuddin Bin Shamsuddin*, Shujun Li† and Budi Arief†
*MyCERT, CyberSecurity Malaysia, Malaysia
†Institute of Cyber Security for Society (iCSS) & School of Computing, University of Kent, Canterbury, UK
Email: {roziah, solahuddin}@cybersecurity.my, {S.J.Li, B.Arief}@kent.ac.uk

***Abstract*—Computer Security Incident Response Teams (CSIRTs) have been established at national and organisational levels to respond to and mitigate cyber incidents. National CSIRTs play a critical role in defending a nation's infrastructure from cyber attacks. However, the research literature lacks studies that can provide first-hand insights on current operational practices in national CSIRTs and challenges faced by staff at national CSIRTs. This paper provides personal observations and opinions from two members of staff at MyCERT (Malaysia's national CSIRT), regarding important areas of national CSIRTs' operational practices including cross-CSIRT collaboration, the lack of systematic use of data and tools, and the lack of evaluation of data and tools used. We hope this paper can help stimulate more research and work to address some of the gaps we identified.**

I. Introduction

Computer Security Incident Response Teams (CSIRTs) have been established to coordinate cyber incident responses at the national or organisational levels [1]. Legal requirements have been established for nations in some regions to set up a national CSIRT (e.g., as required by the EU's NIS Directive), to protect those nations in the cyber space, including protecting critical national infrastructures from cyber attacks and providing support to individuals and organisations under attack [2]. Despite the importance of national CSIRTs, to the best of our knowledge, very little research has been done to share and discuss operational practices at national CSIRTs and how such practices can be improved. This paper aims to provide an example of such practices and the challenges faced by national CSIRTs, based on personal observations and opinions of two members of MyCERT (Malaysia's national CSIRT), and two researchers who have been working closely with MyCERT on related research topics. We hope that the paper can foster collaboration among researchers and staff of national CSIRTs to improve national CSIRTs' operational practices.

II. Operational Practices at National CSIRTs

National CSIRTs are established to act as a national point of contact in dealing with cyber incidents. Some of them also develop tools and methods to detect and mitigate cyber threats, promote security awareness among citizens, and alert constituency of cyber threat outbreaks. Some national CSIRTs have a long history, while others were established more recently. National CSIRTs with a longer history are more mature, with more experience and better skills on cyber incident response, and more developed operational practices. Many mature national CSIRTs have a large team, so are able to structure their operations into several tiers based on a range of factors such as the complexity of incidents, staff expertise, the size of their constituency, availability of resources, the volume and the types of incidents received. In comparison, smaller (especially newly established) national CSIRTs often cannot afford such a complicated structure, and simply operate without a hierarchical structure.

National CSIRTs normally handle cyber incidents following an established *standard operating procedure (SOP)*, which defines steps staff should follow. Such SOPs are mainly adapted from the guidelines defined by standardisation active in cyber security, such as the "Computer Security Incident Handling Guide" defined by the US National Institute of Standards and Technology (NIST) [3]. In addition to a comprehensive SOP covering all types of incidents, separate SOPs can be defined for handling different types of incidents, e.g., one for intrusion and another for malware incidents. MyCERT uses separate SOPs because the staff feel such SOPs are more practical in providing more tailored steps for handling different types of incidents. From personal conversations and informal exchanges with staff of other national CSIRTs, the first two authors of the paper learned that some other national CSIRTs choose to use a single SOP. We are not aware of any research investigating which SOP approach works better, which can be an interesting research topic.

III. Cross-CSIRT Collaboration

Many national CSIRTs actively work with each other, and a number of cross-CSIRT organisations have been established to facilitate such collaboration, including FIRST, ITU, CMU CERT/CC, APCERT, ENISA, OIC-CERT and AfricaCERT. There is evidence that more developed national CSIRTs have assisted newly established ones, through cross-CSIRT initiatives such as activities of ITU and ENISA. Among others, these initiatives provide training opportunities, resource sharing and invitation to participate in cross-CSIRT cyber exercises. For instance, MyCERT conducted incident response training for newly established national CSIRTs from the South East Asia region via initiatives of the APCERT. Among all cross-CSIRT organisations, FIRST is of particular importance because it has both national and organisational CSIRTs as

978-1-6654-1815-7/21/$31.00 © 2021 IEEE

members, and it organises a wide range of initiatives at the global level. FIRST also offers different training courses to its members to support skill development of CSIRT staff. The first author of this paper is currently a FIRST trainer. CMU CERT/CC, one of the oldest organisations supporting national CSIRTs, organises annual events for national CSIRTs to exchange knowledge. Nevertheless, the first two authors observed that it remains largely unknown how helpful such cross-CSIRT initiatives are for improving national CSIRTs' operation, hence the need for more research on this topic.

IV. Some Observed Gaps in Current Practices

1) Regarding the use of data and tools: National CSIRTs rely on data from various sources and a wide range of tools for daily incident responses. Both closed-source and public data are used by national CSIRTs to help enrich threat intelligence. Commonly used *closed-source data* sources include incident reports, cyber threat intelligence data and security feeds provided by various organisations (e.g., Shadowserver for taking down botnets and malicious sites). *Public data* mainly refer to data publicly available on the Internet, often obtained via Open Source Intelligence (OSINT) tools.

We observed that free tools especially open-source tools and free online services have been extensively used by staff of national CSIRTs. Some national CSIRTs – e.g., CIRCL (Luxembourg), JpCERT/CC (Japan) and CERT.at (Austria) – have been actively developing free tools, which are often made open source on GitHub. Many members of staff of national CSIRTs have also been actively promoting the use of free tools. Some national CSIRTs (e.g., MyCERT) have also developed in-house tools that are not shared publicly.

From the first two authors' personal perspective, free tools and public data are used in ad-hoc and informal manner. This shows a lack of systematic and standardised procedures that help guide national CSIRTs, especially new teams, to make better use of such data and tools.

The first two authors also had the impression that some free tools and public data sources may have not been utilised sufficiently by national CSIRTs. One reason is related to a lack of systematic information about such tools and data, and to search them easily. Such an impression was echoed by a recent paper, which showed that there is a general lack of open discussions, public information and research about the use of free tools and public data in national CSIRTs [4].

2) Regarding the evaluation of tools and data: We also observed a lack of a systematic approach to evaluate data and tools at national CSIRTs. This is particularly a problem for free tools and public data, which often did not go through a proper quality assurance process like commercial tools and closed-source data. It is often the case that tools and data are checked on an ad-hoc and informal basis, e.g., by checking with peers, or via an Internet search, or by conducting some lightweight self-testing. More formal evaluation is more often practised for commercial tools, as part of a standard requirement of many organisations' procurement procedure. Staff at national CSIRTs spend most time on incident responses, hence, they often do not enough time for other tasks, such as systematic tool and data evaluation. Despite the less satisfying practice, through own experience and interactions with staff of other national CSIRTs, the first two authors acknowledged that systematic evaluation of tools and data is an important area for improvement, echoing what was reported in [5].

V. Discussion and Recommendations

We summarise key points from our observations: (1) There are various opportunities of research that can help improve operational practices of national CSIRTs; (2) The primary focus on timely incident response impinges progress in developing systematic procedures for guiding operational practices of national CSIRTs, e.g., for tools and data evaluation; (3) Free tools and public data are widely used, and many national CSIRTs are actively promoting their use, including developing free tools for the national CSIRT community; (4) Collaboration among national CSIRTs is very important, particularly in which more developed national CSIRTs provide support for newly established ones; (5) Cross-CSIRT organisations have played a key role in facilitating exchanges and collaboration among national CSIRTs and the wider CSIRT and cyber security communities, around the world and within some geographic regions; (6) More collaboration between the CSIRT community (including cross-CSIRT organisations) and the cyber security research community could be strengthened in many areas to benefit both communities.

Finally, we would like to recommend some concrete actions for the wider community to consider: (i) investigating how public data and free tools can be used more effectively by national CSIRTs; (ii) compiling a repository of free tools and public data as a point of reference for – and to facilitate information exchanges among – national CSIRTs; and (iii) developing standardised and systematic procedures and frameworks for key areas of operational practices at national CSIRTs (e.g., for tool and data evaluation), to increase quality and reliability of results of incident investigation, and to facilitate information exchanges between national CSIRTs and within the wider community including cyber security professionals, public and private sector organisations, and the general public.

References

[1] 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.

[2] 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.

[3] 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, Tech. Rep. 800-61 Revision 2, 2012.

[4] 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.

[5] R. Bourgue, J. Budd, J. Homola, M. Wlasenko, and D. Kulawik, "Detect, SHARE, protect: Solutions for improving threat data exchange among CERTs," ENISA, Tech. Rep., 2013. [Online]. Available: https://www.enisa.europa.eu/publications/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs