Improving the Effectiveness of CSIRTs

Maria Bada*[1] Sadie Creese* Michael Goldsmith* and Chris J. Mitchell[†]

* University of Oxford, Global Cyber Security Capacity Centre, Oxford, UK
[†] University of London, Royal Holloway, London, UK
E-mail: {maria.bada | sadie.creese | michael.goldsmith}@cs.ox.ac.uk | C.Mitchell@rhul.ac.uk

***Abstract*-This paper reports on research designed to measure the effectiveness of national Computer Security Incident Response Teams (CSIRTs). Specifically, our aim is to identify: 1) the ways in which a CSIRT might be considered to be effective; 2) the issues which may limit the performance of a CSIRT; and 3) approaches towards developing CSIRT effectiveness metrics. A primary motive for doing so is to enable more effective CSIRTs to be implemented, focusing on activities with the maximum impact on threat mitigation. The research was conducted using both online survey and interviews, in two phases. The study participants were experts within the existing CSIRT community. In total, 46 participants responded to the survey, from 27 countries in Europe, Africa, South and North America, and Asia. Three experts working for CSIRTs in the UK and USA were also interviewed. Questions asked during the interviews and the online survey queried the personal knowledge and experience of participants regarding CSIRTs. In our analysis, issues such as cooperation, data-sharing and trust are discussed as crucial components of an effective CSIRT. Existing measurement approaches for computer security incident response are presented, before a set of suggested direct and indirect measures of the effectiveness of a CSIRT is defined.**

Keywords-Cybersecurity; CSIRT; Metrics; Effectiveness.

I. INTRODUCTION

This paper considers the problem of assessing the effectiveness of Computer Security Incident Response Teams (CSIRTs). In order to be able to tackle any kind of cybersecurity incident, it is imperative for an incident response capacity to be available at least in some organisational form, in particular as a CSIRT.

The name Computer Emergency Response Team is the historic designation for the first such response team (CERT/CC) [1], established at Carnegie Mellon University (CMU). The term CERT is now a registered service mark of Carnegie Mellon University that is licensed to other teams around the world. Some teams have taken on the more generic name of CSIRT, in particular to clarify that they are involved with the task of handling computer security incidents rather than other technical support work. CSIRTs [2] have as their main responsibility detecting and informing a wider public about vulnerabilities, making patches available to organisations and to the general public, providing technical assistance in dealing with computer incidents, and coordinating responses in emergencies. CSIRTs can operate on a nationwide basis, either inside or outside of the governmental sector. Apart from their main mission, CSIRTs need to be able to adapt to a continuous changing environment and have the flexibility to deal with unexpected incidents. Today's challenges have an impact on the effectiveness of CSIRTs. CSIRTs need effective methods to collaborate and share information, efficient mechanisms to triage incoming information, and policies and procedures that are well-established and understood. Their effectiveness can be affected by a variety of factors [3].

Before considering ways of improving the effectiveness of a CSIRT, it is vital to understand how to assess its effectiveness. Issues such as cooperation, data-sharing and trust are crucial in order for a CSIRT to accomplish high levels of performance. In this paper, we will try to describe the factors which can enhance the capacity of a national CSIRT and improve its processes.

In Section II, we describe existing measurement approaches for computer security incident response before defining a set of measures. Following more information on issues such as cooperation, data-sharing and trust is provided, which are crucial in order a CSIRT to accomplish high levels of performance. In Section III, related work internationally is presented while section IV describes the methodology. Section V presents our results and finally section VI describes our conclusions.

The results presented in this paper are intended to be particularly valuable for CSIRT experts, Chief Information Officers (CIOs), Chief Information Security officers (CISOs), Senior Agency Information Security Officers (SAISOs), Information System Security Officers (ISSOs), and Community Support Officers (CSOs) and (CISOs).

The measures presented can be used both within government and industry contexts.

II. METRICS TO ASSESS THE EFFECTIVENESS OF A CSIRT

Well-defined metrics are essential to determine which security practices are worth investing in. Every CSIRT will need to develop mechanisms to evaluate the effectiveness of its practice. This should be done in conjunction with its management and its constituency [4]. Effectiveness, as well as efficiency measures address two aspects of security control implementation results: the robustness of the result itself (effectiveness) and the timeliness of the result (efficiency). These measures can provide important information for security decision makers in order to improve the performance of CSIRTs, and they help in determining the effectiveness of security controls.

 ISBN: 978-1-61208-605-7

By measuring the effectiveness of information security, there can be [5]:

a) Increases in accountability: Measuring effectiveness can help in identifying specific security controls that are implemented incorrectly or are ineffective.

b) Improvements in Information Security Effectiveness: Measuring information security can determine the effectiveness of implemented information security processes and procedures by interrelating the results of various activities and events to security controls and investments.

c) Demonstration of Compliance: Organisations can demonstrate compliance with applicable laws and regulations by maintaining an information security measurement program.

The International Telecommunication Union (ITU) [6], is helping countries to establish National Computer Incident Response Teams (CIRTs), which serve as a national focus point for coordinating cybersecurity incident response to cyber-attacks in the country. The objective of the Assessment of a CSIRT is to define the readiness to implement a national CSIRT. Part of this assessment includes the incident response capabilities of a country and the existence of an intrusion detection service offered to the constituents.

In order to improve the effectiveness of a CSIRT, it is vital to understand how to assess its effectiveness. Following we will be providing more information on issues such as cooperation, data-sharing and trust which are crucial in order a CSIRT to accomplish high levels of performance [3], [4], [7], [8].

A. Cooperation

The OECD report (2005) [9], describes the importance of international cooperation for fostering a culture of security and the role of regional facilitating interactions and exchanges. Moreover, national CSIRTs can help foster a cybersecurity culture by providing activities for awareness and education to the public, educating national stakeholders on the impact of virtual activities to their organisations, and the implications of their activities for cyber and information security. International cooperation is considered an integral part of the activities of a national CSIRT, and a number of countries have already established operational networks through which they exchange information and good practice. Most countries cooperate at the regional (European TF-CSIRT and EGC, APCERT) or global level (FIRST).

ENISA [10] while discussing the subject of the effectiveness of CSIRTs, has focused on possible barriers that can inhibit it. Specifically, four areas of benefit from a possible cooperation were identified: Incident Handling; Project establishment; Resource and information sharing; Social networking.

B. Information sharing

ENISA [10] has dealt with the issue of threat and incident information exchange and sharing practices used among CSIRTs in Europe, especially, but not limited to, national/governmental CSIRTs. ENISA identified the functional and technical gaps that limit threat intelligence exchanges between national/governmental CSIRTs and their counterparts in Europe, as well as other CSIRTs within their respective countries.

Interactions between CSIRTs can include asking other teams for advice, disseminating knowledge of problems, and working cooperatively to resolve an incident affecting one or more of CSIRT constituencies. Response teams have to decide what kinds of agreements can exist between them in order to share but still safeguard information, as well as which information can be disclosed and to whom. A peer agreement refers to simple cooperation between CSIRTs, where a team contacts another and asks for help and advice [11].

ENISA [7] presented a variety of issues which can hinder information sharing. The main barriers to cooperation between CSIRTs are: a) poor quality of information; b) poor management of information sharing; c) misaligned incentives stemming from reputational risks; d) uncertainty about senior level awareness of cybersecurity; and e) the disincentive for private sector organisations to disclose information because of possible reputational damage. ENISA defines basic requirements for improved communications interoperable with existing solutions in order to improve information sharing. Better utilization of current communication tools and practices is needed. Local detection of incidents accompanied by trusted forms of information exchange, can ultimately lead to improved prevention of cyber incidents on a global scale.

The Information Sharing Framework (ISF, MACCSA, 2013) [8] provides guidance on establishing the capability to increase an organisation's cyber Situational Awareness, enabled by sharing information across a trusted community of interest to achieve Collaborative Cyber Situational Awareness (CCSA).

C. Trust

CSIRT cooperation is based on trust. Without trust, national/governmental CSIRTs will be less willing to share information and less open to work together on incident response and handling when needed. Measuring trust and defining criteria by which to measure a CSIRT trustworthiness is an ongoing challenge, particularly when the aim of the cooperation is to exchange and share sensitive information. Key criteria that national CSIRTs look for include: technical expertise with a proven track record; membership in CERT initiatives; ability to respond quickly and act on security threats; and a stable team [3].

Trust can be one of the biggest obstacles to enhanced and effective communication between CSIRTs but also between CSIRTs and other stakeholders. Lack of trust between stakeholders can lead to a lack of sharing of security incident information. This component is of vital importance for cooperation and information sharing, as discussed above.

According to Messenger (2005) [12], trust in public/private partnerships has a very significant role which can be enhanced through frequency of contact between

 ISBN: 978-1-61208-605-7

counterpart individuals, identification and sharing of common intentions and objectives, or technical credibility of technical staff.

According to the Information Sharing Framework [8], Trust depends on an AAA Model: Authentication (Are you who you claim you are?), Authorisation (Do you have permission to undertake the activities?) and Accountability (Can you evidence compliance in any court of law?).

D. Resources

The effectiveness of CSIRTs can be limited as a result of growing work load and limited resources [13], [14]. It seems obvious, but a national incident response team without a steady source of funding will not be able to function beyond the short term [15]. The typical work overload situation in a CSIRT, limits its effectiveness [14]. A CSIRT that has over-stretched its resources over a long time period must be prepared to go through a worse-before-better scenario to escape the "Capability Trap". Such a transition process can be quite painful to the CSIRT and its surrounding environment, for example, through adjustments to scope of service to release resources for improvement [13].

III. RELATED WORK

The key to security metrics is obtaining measurements that have the following ideal characteristics: they should measure organisationally meaningful things; they should be reproducible; they should be objective and unbiased; they should be able to measure some type of progression towards a goal.

There are existing publications which refer to how we can measure the performance and create accountability for the capabilities of a CSIRT. The NIST Special Publication 800-55 Revision 1 (2008) [16] defined measurement types for information security such as implementation, effectiveness/efficiency, and impact. The authors established that these are not just measurement types but they are actually purposes or the drive for measuring information security. In another NIST publication, NIST Special Publication 800-61 Revision 1 [17] possible metrics were proposed: a) the number of incidents handled; b) time per incident; c) objective assessment of each incident; and d) subjective assessment of each incident. These metrics are very practical but suggest only a small portion of possible metrics and measurement types for measuring CSIRT.

A technical report from Carnegie Mellon's Software Engineering Institute [18] measured incident management based on common functions and processes within CSIRT work flow. Sritapan, et al. [19] developed a metrics framework for incident response to serve as an internal analysis, in order to support the incident reporting improvement and strengthen the security posture for an organisation' s mission.

The OECD report on Improving the Evidence Base for Information Security and Privacy Policies [20] indicates that many CSIRTs already generate statistics based on their daily activities, including statistics on the number of alerts and warnings issued or incidents handled.

The OECD report [21] presents the ability of CSIRTs to report data about their constituencies, the size of the networks and users under their responsibility, organisational capacity and incidents, as well as information on the quality of these responses.

ENISA [22] also released a report which, "*builds upon the current practice of CERTs with responsibilities for ICS networks, and also on the earlier work of ENISA on a baseline capabilities scheme for national/ governmental (n/g) CERTs*," without prescribing which entity should provide these services for the EU. The good practice guide divides ICS-CERC provisions into four categories: mandate capabilities; technical operational capabilities; organisational operational capabilities and co-operational capabilities.

IV. METHODOLOGY

A focus group was conducted, with participation of 15 experts working in both academia and industry. The research itself was conducted using an online survey and interviews, in two phases, a pilot phase and the main survey phase.

Questions asked during the interviews and online survey, solicit the personal knowledge and experience of participants regarding CSIRTs. Prior to taking part in the study, participants were required to read and sign a consent form that informed them of the project, its goals and how their information and feedback would be treated and used. All data were anonymised immediately following its collection, and information was treated as confidential. This project has been reviewed by, and received ethics clearance through, the University of Oxford Central University Research Ethics Committee (Ref No: SSD/CUREC1A/14-127, Annex C).

A. Pilot Phase

An online tool-survey was developed using Qualtrics [23]. During the pilot phase, the online survey consisted of 51 questions on various factors determining the effectiveness of CSIRTs, and participants were required to answer the questionnaire through a web link.

B. Main Research Phase

After the pilot phase, feedback from participants was collected, which resulted in the survey consisting of 19 questions. Furthermore, during this phase three interviews were conducted in order to gain a deeper insight on the experience of experts working for CSIRTs, and on the level of cybersecurity capacity of a nation, region or organisation.

C. Participants

The participants who took part in the study are experts within the existing CSIRT community, currently working in a CSIRT environment or who have done so in the past, or have been involved in the creation of a CSIRT. In total, 46 participants responded to the survey, from 27 different countries in Europe, Africa, the Americas, and Asia. Also, three experts working for CSIRTs in the UK and USA were interviewed.

 ISBN: 978-1-61208-605-7

V. RESULTS

This section presents the results from the research described above.

Regarding the type of the constituency the participants have worked for, the majority stated that their constituency was a government or a commercial organisation. Some participants stated that they have worked for the Internet Society, a non-governmental organisation, a research group, an academic organisation or a coordination centre.

A. Training

A very important aspect of measuring the effectiveness of a CSIRT is the training provided to its members. Our findings indicated that the training is provided for most experts working for a CSIRT. When considering the types of training provided to employees working for a CSIRT, the responses referred to training on operational, technical issues as well as on forensics and conducting CSIRT exercises.

Training on communication and legal issues is less commonly provided. Moreover, some participants mentioned other areas of training provided, such as tools for operationalising a CSIRT, threat intelligence resources, policies and procedures as well as TRANSITS courses. Usually, CSIRT programs are made up of qualified experts, but lack full-time staff. Most of the training provided focuses on operational, technical issues as well as on forensics and conducting CSIRT exercises [3]. Consistent training of CSIRT staff, as well as the continuous building of a network of experts who can provide advice and help, is necessary.

B. Type of services provided

Our findings indicate that most of the services provided are reactive, including incident handling, alerts and warnings, and vulnerability handing; although proactive services, such as security audit/assessments and dissemination, are also provided. Lastly, a significant volume of security quality management services are provided, such as awareness, education and training. Other noteworthy services provided, as indicated by the participants, include monitoring; the applicability of Audit Law and the protection of the critical infrastructure and situational awareness services.

C. Security incidents

According to our results, most frequent classes of security incident are: malicious code; unauthorised access; and spam. Less frequent incident types include: denial of service attacks; improper usage; scans/probes/attempted access; data breach; ransomware and destructive malware. Some other security incidents referred to by participants are website defacement; computers in botnet; phishing; and fraud attempts.

Although security experts claim that they can identify security incidents within hours, it typically takes about a month to work through the entire process of incident investigation, service restoration and verification. The identification of a security incident is only a small part of the overall process of handling that incident. Investment is critical for effective cyber incident response programs. Also, a crucial aspect is that usually management is largely unaware of cybersecurity threats [24].

D. Cooperation and Trust

International cooperation is widely regarded as an integral part of the activities of national CSIRTs, and several countries have already established operational networks through which they exchange information and good practice. Most countries cooperate at the regional (e.g., European TF-CSIRT and EGC, APCERT) or global level (e.g., FIRST). ENISA [22], while discussing the subject of the effectiveness of CSIRTs, addressed the topic of multi various cooperation between CSIRTs. From our research, we found that cooperation is strongest at a national level, less evident in the context of cooperation between EU member States, and at its lowest level for cooperation at an international level.

As trust is not inherent, CSIRTs can go about establishing a first bond of trust in three ways: necessity, opportunity [25] and through trusted introducers. As indicated at the latest paper of the Global Public Policy Institute (GPPi) [24], *'Necessity drives cooperation, and if cooperation leads to a positive outcome it builds trust'*.

E. Metrics

In this section, we present results of our findings regarding possible ways of measuring the effectiveness of CSIRTs. The metrics identified from our research and suggested by stakeholders could be categorised in six categories: a) impact measures; b) incident response quality; c) incident prevention; d) situational awareness capability; e) measures on general capability of CSIRTs; f) outreach mission.

a) Impact measures: These measures are used in order to assess the impact of a CSIRT's mission. Examples of these measures are: 1) the volume of information output by the CSIRT (advisories, bulletins, reports) or 2) the amount of information reported to constituency about computer security issues or ongoing activity.

b) Incident Response Quality: Examples of measuring incident response quality are: 1) digital forensics capability; 2) well-defined processes with identified steps, stakeholders and escalation lists; 3) the number of high impact incidents measured in dollars or damage; 4) re-occurring incidents that were already handled; 5) the speed of initial response to an event; 6) the speed of identification of incident nature / attack characteristics (estimated time); ability to achieve normal work flow through attack status in face of incidents (indication of skills/adequate capabilities); 7) stakeholder level of awareness (communications ability); 8) percentage of security incidents that were managed in accordance with established policies, procedures, and processes (Incident Management Procedures) [26], [27]; 9) percentage of incidents reported within required time frame per applicable incident category [15]; 10) percentage of successful attacks handled in accordance with policy, defined procedures, and in-place processes in a disciplined repeatable, predictable manner (this assumes that well-defined processes for

incident management exist) [24]; 11) ability to cooperate with other CSIRT teams in support of investigations and prosecutions (the latter requiring the evidence capability) [3], [4].

c) Incident prevention: Examples of measuring incident prevention quality are metrics such as: 1) the number of vulnerability exploits for organisations and/or individuals in the target audience for the CSIRT; 2) the percentage of security incidents that exploited existing vulnerabilities with known solutions, patches, or workarounds and 3) the mean times between incidents (high performers have long mean times).

d) Situational Awareness Capability: This capability can me measured by looking at: 1) access to threat and attack data feeds; 2) the synthesis of data feeds into single data model (indicator of fusion capability); 3) the support for threat and attack intelligence capability; 4) the translation into information for distribution to stakeholder community; 5) the translation into actionable information for incident response; 6) the integration of feedback into refinement of architectures and best practices; 7) the involvement in disaster recovery planning [28].

e) Measures on general capability of CSIRTs: As mentioned above there are other capabilities which define the effectiveness of a CSIRT. These are: 1) the existence of enough funding [29]; 2) the existence or possible access to specialised legal and PR experts among staff members [14]; 3) the existence or possible access to specialised personnel in reverse engineering or digital forensics; 4) the security posture of the organisation; 5) the effectiveness of a Government to support a CSIRT policy; 6) the existence of a portal on CSIRTs; 7) the number of staff members with [X] years of incident handling experience.

f) Outreach Mission: Metrics such as: 1) the promotion of stakeholder awareness on existing national CSIRTs and their responsibilities and 2) training in specialised technical aspects [3] are also identified as crucial factors regarding the effectiveness of CSIRTs.

g) Other Measures: The current research has also identified other essential qualities that could reinforce the effectiveness of a CSIRT. These are: a) the collaboration with law enforcement agencies; b) capacity-building programmes; c) public-private partnerships; d) career tracks for all staff members; e) establishment of national regional and international centres for a coordinated response in real time and training CSIRT; and f) the presence of pre-established channels of communication prior to actual incident responses.

Awareness and education is also a central and ongoing process for a CSIRT. Therefore, the improvement of awareness of CSIRTs in target audience is crucial. This might be done by various ways, such as via web sites, conferences and white papers.

Also, better communication, information sharing and cooperation between CSIRTs can lead to better performance. Therefore, by improving the means of communication to target audience through multiple communication channels can improve the effectiveness of CSIRTs [9], [30].

In order to enhance the flow of vulnerability information to CSIRTs and improve the use of information provided by CSIRTs trust is of vital importance. Improving trust in and between CSIRTs can ensure that (a) as much information is provided to CSIRTs as possible, and (b) take-up (action on) of information provided by a CSIRT is maximised.

Moreover, having a good legal framework and establishing collaboration with law enforcement agencies can enhance sharing of data. A possible approach might be to draft regulation and/or legislation to make organisations take action on CSIRT warnings and/or increase their liability so they feel obliged to take warnings seriously. Better enforcement of existing legislation (including data privacy legislation) could also enforce organisations to take privacy and security into consideration.

VI. CONCLUSION

Further research in this field would be highly desirable. Improving the effectiveness of CSIRTs is likely to be a long-term process. Experts working in CSIRTs need to share their knowledge and experience with a wider network of experts in order to enhance their capabilities.

As shown in this study, better communication, information sharing and cooperation between CSIRTs can lead to better performance. The suggested steps in order to improve the effectiveness of CSIRTs include, improvement of awareness of CSIRTs in target audience, improvement of the flow of vulnerability information to CSIRTs, improving use of information provided by CSIRTs, improving trust in CSIRTs to ensure that as much information is provided as possible, better enforcement of existing legislation and of course existence of enough resources.

Limitations and future research

Our research was subject to a number of limitations. First, our sample involved 46 participants, from 27 countries in Europe, Africa, the Americas and Asia. Although we tried to cover a broad range of countries at various levels of development, a larger sample would provide more accurate data. Second, the majority of participants have current or previous experience in national CSIRTs and less in organisational CSIRTs. This can partly be explained by the nature of the experts that were contacted. Future research might usefully explore the effectiveness of CSIRTs in the private sector.

REFERENCES

[1] Computer Emergency Response Team, CERT. [Online]. Available: http://www.cert.org/ [Accessed 5 June 2017].

[2] Organisation for Economic Co-operation and Development (OECD): “Studies in Risk Management, Norway Information Security”, 2006. [Online]. Available from: http://www.oecd.org/norway/36100106.pdf [Accessed 24 June 2017].

[3] European Network and Information Security Agency (ENISA): “Deployment of Baseline Capabilities of National/ Governmental CERTs”, 2012. [Online]. Available: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/deployment-baseline-capabilities-nationalgovernmental-certs [Accessed 10 June 2017].

[4] S. Bradshaw, "Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity", Centre for International Governance Innovation and Chatham House, Paper Series: No. 23 – December 2015. [Online]. Available: https://www.cigionline.org/sites/default/files/gcig_no23web_0.pdf [Accessed 9 June 2017].

[5] National Institute of Standards and Technology (NIST): "Special Publication 800-55 Revision 1, Performance Measurement Guide for Information Security", E. Chew, M. Swanson, K. Stine, N. Bartol, A. Brown, and W. Robinson, July 2008. Available: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf [Accessed 10 June 2017].

[6] F. Wamala, "National Cybersecurity Strategy Guide", International Telecommunication Union (ITU), September 2011. [Online]. Available: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf [Accessed 30 May 2017].

[7] European Network and Information Security Agency (ENISA): "Incentives and Barriers to Information Sharing", 2010. [Online]. Available: https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing/ [Accessed 15 June 2017].

[8] Multinational Alliance for Collaborative Cyber Situational Awareness (MACCSA): "Information Sharing Framework (ISF), version 2.4", 20 November 2013. [Online]. Available: https://www.terena.org/mail-archives/refeds/pdfjJz1CRtYC4.pdf [Accessed 10 May 2017].

[9] Organisation for Economic Co-operation and Development (OECD): "The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries, Working Party on Information Security and Privacy", December 2005. [Online]. Available: http://www.oecd.org/internet/ieconomy/35884541.pdf [Accessed 2 May 2017].

[10] European Network and Information Security Agency (ENISA): "Detect, SHARE, Protect - Solutions for Improving Threat Data Exchange among CERTs", 2013. [Online]. Available: https://www.enisa.europa.eu/activities/cert/support/data-sharing [Accessed 4 May 2017].

[11] N. Brownlee and E. Guttman, "Expectations for Computer Security Incident Response. Best Current Practice", ISF, Network Working Group RFC 2350, June 1998. [Online]. Available: http://tools.ietf.org/html/draft-ietf-grip-framework-irt-04 [Accessed 24 June 2017].

[12] M. Messenger, "Why would I tell you? Perceived influences for disclosure decisions by senior professionals in inter organisation sharing forums", Unpublished Masters dissertation, University of London Birkbeck School of Management and Organisational Psychology, 2005.

[13] W. Johannes, J. Gonzalez, and K. P. Kossakowski, "Limits to Effectiveness in Computer Security Incident Response Teams", In 23rd International Conference of the System Dynamics Society, V. 11, Oxford, pp. 55-74, 2004. Available: http://scholarworks.lib.csusb.edu/ciima/vol11/iss3/5 [Accessed 24 May 2017].

[14] M. Nurul, Y. Zahri, A. Aswami, and N. Azlan, "CSIRT Management Workflow: Practical Guide for Critical Infrastructure Organizations", Proceedings of the 10th European Conference on Information Systems Management: ECISM 2016, Portugal September, pp.138-146, 2016.

[15] Organization of American States (OAS): "Best Practices for Establishing a National CSIRT", 2016. [Online]. Available: https://www.sites.oas.org/cyber/Documents/2016%20-%20Best%20Practices%20CSIRT.pdf [Accessed 2 May 2017].

[16] National Institute of Standards and Technology (NIST): "Special Publication 800-55 Revision 1", 2008. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf [Accessed 17 June 2017].

[17] National Institute of Standards and Technology (NIST): "Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide", Recommendations of the National Institute of Standards and Technology, P., Cichonski, T., Millar, and T.G.K., Scarfone, August 2012. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf [Accessed 24 June 2017].

[18] Software Engineering Institute (SEI): "Incident Management Capability Metrics Version 0.1", 2007. [Online]. Available: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8379 [Accessed 12 May 2017].

[19] V. Sritapan, S.W. Zhu, and C. E. Tapie Rohm Jr., "Developing a Metrics Framework for the Federal Government in Computer Security Incident Response", 2011. [Online]. Available: http://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1170&context=ciima [Accessed 16 June 2017].

[20] Organisation for Economic Co-operation and Development (OECD): "Improving the Evidence Base for Information Security and Privacy Policies: Understanding the Opportunities and Challenges related to Measuring Information Security, Privacy and the Protection of Children Online", OECD Digital Economy Papers, no. 214, OECD, 2012, Paris.

[21] Organisation for Economic Co-operation and Development (OECD): "Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy. Improving the International Comparability of Statistics Produced by Computer Security Incident Response Teams", 18 June 2014.

[22] European Network and Information Security Agency (ENISA): "Good practice guide for CERTs in the area of Industrial Control Systems - Computer Emergency Response Capabilities considerations for ICS", December 2013. [Online]. Available: http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/ics-cerc/good-practice-guide-for-certs-in-the-area-of-industrial-control-systems/at_download/fullReport [Accessed 5 June 2017].

[23] Qualtrics, http://www.qualtrics.com/

[24] I. Skierka, M. Hohmann, R. Morgus, and T. Maurer, "CSIRT Basics for Policy-Makers: The History, Types & Culture of Computer Security Incident Response Teams", Global Public Policy Institute (GPPi), April 29, 2015. [Online]. Available: http://www.digitaldebates.org/fileadmin/media/cyber/CSIRT_Basics_for_Policy-Makers_May_2015_WEB_09-15.pdf [Accessed 18 May 2017].

[25] K. Silicki and M. Maj, "Barriers to CSIRTs cooperation. Challenge in practice", the CLOSER Project, 20th FIRST Annual Conference, Vancouver, Canada, 2008.

[26] Carnegie Mellon University, "CERT's Podcasts: Security for Business Leaders", Show Notes, 2008. [Online]. Available: http://resources.sei.cmu.edu/asset_files/Podcast/2008_016_102_67465.pdf [Accessed 19 June 2017].

[27] CC. Chiu and KS. Lin, "Importance-Performance Analysis Based Evaluation Method for Security Incident Management Capability", In: Nguyen N., Tojo S., Nguyen L., Trawiński B. (eds) Intelligent Information and Database Systems, ACIIDS, pp. 180-194, 2017. Lecture Notes in Computer Science, vol 10192. Springer.

[28] T. Pahi, M. Leitner, and F. Skopik, "Analysis and Assessment of Situational Awareness Models for National Cyber Security Centers," In Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP), SCITEPRESS, pp. 334-345, 2017. ISBN 978-989-758-209-7. DOI: 10.5220/0006149703340345

[29] Ponemon Institute LLC, "Cyber Security Incident Response – Are we as prepared as we think?", January 2014. [Online]. Available: http://www.lancope.com/ponemon-incident-response/ [Accessed 19 June 2017].

[30] European Network and Information Security Agency (ENISA): "CERT cooperation and its further facilitation by relevant stakeholders", 2006. [Online]. Available: CERT_cooperation_ENISA.pdf [Accessed 11 June 2017]

 ISBN: 978-1-61208-605-7