Characteristics of Cyber Incident Response Teams in the World and Recommendations for Turkey

Y. E. Karabulut, G. Boylu, E.U. Küçüksille and M.A. Yalçınkaya

***Abstract*— Today, in countries across the world, operations such as the digitalization of critical infrastructure and public services, through the use of computer networks, has revealed the security problems of cyber space. Used for the transferring and storing of highly critical data, any weaknesses and vulnerabilities located on these computer systems have the potential to cause tangible and intangible costs and losses on the country concerned. With the concept of cyber security growing in importance globally, countries have developed strategies, launched awareness-raising activities, and organized campaigns to have maximum information security level. In what is an ongoing process, it has been revealed that countries are finding it necessary to create computer security incident response teams, in order to protect their national cyber security. Cyber incident response teams are for the early identification of threats to national security that may occur in cyberspace, and to reduce the effects of any attack that may be encountered. In this study, we examined in detail the policies being implemented for the creation of cyber incident response teams and the qualifications team members should have. In addition, the cyber incident response teams created in developed countries around the World, and the properties and activities of these teams, are investigated. The study is concluded by examining the development of cyber incident response teams in Turkey, and presenting recommendations for Turkey.**

Index Terms— **CSIRT, Incident response teams, Information security, Strategy of national security.**

I. Introduction

The transition to digital infrastructures being conducted in various countries, with the aim of providing better and faster solutions for their organizations and institutions, as well as improved services for society, has led to the emergence of the concept of cyber-security.

Y. E. Karabulut, is with the, Computer Engineering Department, Süleyman Demirel University, Isparta, Turkey, (e-mail: emrkarabulut@gmail.com).

G. Boylu, is with the, Computer Engineering Department, Süleyman Demirel University, Isparta, Turkey, (e-mail: gulistan.boylu@gmail.com).

E. U. Küçüksille, is with the, Computer Engineering Department, Süleyman Demirel University, Isparta, Turkey, (e-mail: ecirkucuksille@sdu.edu.tr).

M. A. Yalçınkaya, is with the, Computer Engineering Department, Süleyman Demirel University, Isparta, Turkey, (e-mail: mehmetyalcinkaya@sdu.edu.tr).

Discussions on this new concept have also drawn attention to the protection of these critical infrastructures against potential threats, as well as the ability to respond to attacks. Many countries, in parallel to increasingly digitalizing their critical infrastructure, have also begun to draw and publish cyber-security strategies and action plans, taking concrete steps towards restructuring their organizations and forming cyber incident response teams - one of the most critical aspects of these strategies and plans.

Around the world, cyber intervention teams are defined either as computer security incident response teams (CSIRTs) or computer emergency response teams (CERTs). Teams at cyber incident response centers focus on identifying threats to national security within the cyber environment; on reducing the impact of potential attacks; and on responding to actual attacks. Many countries have already formulated their own national cyber-security strategy, announcing their action plans and establishing their own cyber incident response centers.

In the following sections of this study, we discuss the activities and tasks of cyber incident response centers, evaluate how cyber incident response teams are formed and what their skills should be based on examples from around the world. In this context, we will highlight what is being done and should be done in Turkey.

II. Cyber Incident Response Teams

Cyber incident response teams (CIRTs) are institutional and sectorial organizations established to rapidly identify threats and potential attacks in the cyber environment, and to develop and share measures for solving the problems caused by these attacks. The goal of these teams is thus to provide cyber response skills to institutions and organizations. CIRTs are classified into three groups: national teams, institutional teams, and sectorial teams.

National CIRTs are tasked with leading the formation of institutional response teams, and with providing support to both institutional and sectorial cyber incident response teams. Institutional CIRTs, on the other hand, are tasked with the formation of sectorial cyber incident response teams. To ensure a holistic approach to security, as well as rapid response and organization, the national, institutional and sectorial cyber incident response teams all work in coordination with one another [1].

III. THE FORMATION OF CYBER INCIDENT RESPONSE TEAMS

When forming cyber incident response teams, it is important to define the teams' parameters. From the outset, procedures should be formed and policies defined, so that the teams can readily adapt to the dynamic nature of cyberspace while also being able to respond rapidly to cyber threats.

The general organizational and operational framework of CIRTs should be fully delineated. In this context, the scope of a CIRT, the institutions and organization with which it will cooperate and communicate, its aims and objectives, and the existing risks, should all be clearly laid out. It is necessary to define the elements, methods, and infrastructure of communication, while also developing a system that will prevent loss of time in emergencies and exceptional situations.

When forming CIRTs, the existing national, institutional and sectorial communication and information networks should also be evaluated and taken into consideration. In addition to responding to cyber threats and events, CIRTs are also tasked with informing the public and raising awareness. Being newly established, CIRTs should come up with a strategy for fulfilling this requirement.

The mission statement of a CIRT should clearly outline their aims and objectives. Aspects, such as how the team will respond to emergencies and exceptional situations, as well as the areas and description of the team's reactions and reflexes, should all be clearly explained. The mission statement of a CIRT is also important for defining the scope of the team's services, and for further improving the team's quality.

In addition to the mission statement, the intra-team hierarchy and the assignment of tasks should also be determined. Clearly describing the financial resources of a CIRT will also help prevent chaos and confusion during emergencies, or when steps are being to further expand the team. The purpose, the roles assumed within the country, and the areas of activities of CIRTs should all be clearly defined and announced to the public.

IV. THE COMPETENCIES OF CYBER-SECURITY TEAMS

The operational expectation of CIRTs is for them to avert cyber-attacks, and to prevent potential attacks by reinforcing the vulnerable points where attacks may occur.

The critical service infrastructure (such as power, electronic communications, finance) of CIRTs should allow them to monitor digital systems, and to resolve cyber security-related issues and weaknesses, by predicting the possible damages that might be caused by cyber-attacks.

Thus, CIRTs should possess certain skills and competencies, and as such, consist of individuals specializing in areas such as vulnerability analysis, log management, cyber response information security management [2].

A. Vulnerability Analysis

Vulnerability analysis includes the structuring and monitoring of security activities, the execution of penetration tests, and the gathering of information on the techniques used in cyber-attacks. Within the scope of vulnerability analysis, CRTs focus on identifying major system vulnerabilities and risks before actual attacks take place, while also taking measures and coordinating activities concerning these vulnerabilities and risks.

B. Log Management

Log Management includes the ability to identify attacks and to effectively track and interpret records and trails left on a system, as well as centralized security monitoring and incident management. Enabling national and institutional CIRT personnel to track system records and raise awareness of systems and threats can also be considered, within the scope of Log Management.

C. Response to Cyber Events

This competency involves the formation of an effective institutional CIRT establishment and team member selection by national CIRT personnel, as well as a firm grasp of the details pertaining to information system forensic analyses, network forensic analyses, protection methods against Distributed Denial of Service (DDOS) attacks and information technology law. This competency provides CIRTs with the necessary management and coordination skills for dealing with cyber incidents and attacks. Furthermore, this competency also covers the proper implementation and execution of the measures and methods for preserving digital evidence.

D. Information Security Management

Information security management is an important skill for cultivating an understanding of cyber-security processes, and raising cyber-security awareness, both at an institutional and public level. Increasing the awareness of institutional and sectorial CIRT personnel, on information security management, enables them to execute rapid and coordinated incident management during negative incidents and cyber-attacks.

V. INCIDENT RESPONSE TEAMS INTERNATIONALLY

In many countries, CIRTs can be found as either Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs).

The launch of the first CIRTs in Turkey began towards the end of 2013, and was soon followed by the formation of the sub-teams (i.e. institutional and sectorial teams). The structure and organization of CIRTs tends to vary, depending on the social and governance structures of the different countries. In many countries, national CIRTs have additional teams and institutions working under them.

A. *United Kingdom*

The United Kingdom's (UK's) national CIRT began its operations in March 2014 under the name CERT-UK. Infrastructure activities for the CERT-UK began soon after the publication of the national cyber-security strategy in 2011 by the British Government, and the institution became active and operational in 2014. In the UK, the CERT has been assigned with four main tasks:

- National cyber-security incident management,
- Support to companies and institutions providing national critical infrastructure services.
- Conducting activities for promoting and raising awareness on cyber-security at an academic and sectorial level,
- Contacting the cyber incident response teams of other countries to ensure coordination and cooperation.

Furthermore, within CERT, a Cyber Security Information Sharing Partnership (CiSP) team has also been established. The purpose of this team is to ensure that all institutions and sectors are kept aware of cyber-security-related developments through a cyber-security information-sharing partnership, while also informing the participants about vulnerabilities, and raising their overall knowledge on the subject. CiSP is a joint project of the British government and industry. The CiSP project endeavors to develop a holistic cyber-security approach in the UK, and share real-time information on cyber-attack news, methods and vulnerabilities with institutions and commercial sectors by closely adhering to confidentiality [3].

B. *Germany*

The German cyber incident response team was established by the German government under the name of CERT-BUND (German abbreviation: BSI). Referred to as the Federal Office of Information Security, the BSI is tasked with promoting digital and communication security for the German government, and its areas of responsibility and specialization includes:

- Protection of critical infrastructures (energy, communications, transportation) against cyber-attacks,
- Internet security,
- Setting measures against and identifying wiretapping activities.
- Developing security standards and certifications.
- Giving accreditation to security test laboratories.

BSI currently has over 600 personnel. It was established in 1986 with the information technology security authorization. The cyber incident response team was established in 2009, and the scope of BSI's authority and tasks was significantly broadened following the enactment of the most radical regulatory changes to date concerning its tasks and responsibilities [4].

C. *Japan*

The Japanese cyber incident response team is known as Japan Computer Emergency Response Team (JPCERT). JPCERT is tasked with promoting the critical infrastructure security of national GSM operators, state institutions and organizations, and of industrial organizations against cyber attacks. In addition, JPCER also led and coordinated the establishment of the first Asia-Pacific Cyber Incident Response Team, APCERT. This team is also responsible for ensuring coordination and cooperation with other national teams.

JPCERT organizes training activities on information security within the country, and also holds events, contests, and conferences for raising awareness on cyber incidents and information security. JPCERT acquired official status in 2003, becoming a non-profit organization working for the state [5].

D. *United States of America*

The American cyber incident response team is known as US-CERT. This organization's mission statement describes it as being tasked with ensuring the cyber security of the American people, that it enjoys a proactive management, and that its aim is to become the preeminent cyber incident response center in the world.

The official website of US-CERT contains information and documents on current information security vulnerabilities and cyber-attacks being carried out across the world, by posting such information and documents online, the United States (US) aims to inform and raise the awareness of its people about information security, and to create a source and reference on cyber security. This organization, also called the National Cyber Awareness System (NCAS), relays information and updates through electronic mail, allowing subscribers to receive the latest updates on cyber-space incidents by e-mail [6].

E. *Turkey*

The Cyber Security Institution of Turkey has developed, and shared with the public, a National Cyber Security Document of its first meeting. Following this, and the publication of the relevant regulations in the Turkish Official Gazette dated November 11, 2013, the National Cyber Incident Intervention (USOM) center was established. While this organization is called USOM in Turkey, it is internationally known as TR-CERT.

Following the foundation of USOM, Turkey's strategy document also considered the establishment of both institutional and sectorial Cyber Incident Response centers. The document envisages the formation of institutional CIRTs within Ministries, and in institutions and organizations affiliated with Ministries, and also emphasizes coordination and cooperation between these teams and USOM.

Sectorial CIRTs, on the other hand, will be established to promote measures for information, data, and system security, in companies providing industrial and critical infrastructure services. Sectorial CIRTs will be directly in contact with institutional CIRTs, while also engaging in information sharing and cooperation with USOM.

VI. SUGGESTIONS FOR TURKEY

The Turkish Cyber Incident Response Team USOM has closely followed the approach implemented by other countries, and has rapidly completed its organization accordingly. However, in addition to not yet being widely known by the public, at the present time USOM is also not assuming an active role. For this reason, public awareness raising activities should first be conduct to explain to the public what cyber space is, and to emphasize its importance for personal, company and national security.

One option in this context would be to form, just as it is the case in the UK and US, an external team that will conduct public awareness raising activities, define specific actions for raising awareness, and organize activities that are compatible with Turkey social fabric. Measures could also be taken to ensure continuous communication and exchange of opinions between this team and the larger public.

VII. CONCULUSION AND DISCUSSION

By examining a number of examples and organizations from around the world, this study investigated how cyber incident response centers or teams are formed, what their competencies should be, and the main methods and mechanisms they employ. In addition, the study evaluated the cyber incident response teams of developed countries such as the UK, the US and Japan, as well as the activities of these teams, and in this context, by taking into account current developments and studies, made suggestions on what steps also need to be taken in Turkey.

ACKNOWLEDGMENT

The study is selected from National Engineering Research Symposium 2015 (Ulusal Mühendislik Araştırmaları Sempozyumu) UMAS 2015 (Duzce University).

REFERENCES

[1] A. Sawicka, J. Gonzalez and Y. Qian, “Managing CSIRT Capacity as a Renewable Resource Management Challenge. An Experimental Study”. In: Proceedings of the 23rd System Dynamics Society Conference, Boston, MA, USA, July 2005, pp. 31.

[2] P. Pavel, "Adapting the ticket request system to the needs of CSIRT teams." WSEAS Transaction on Computers 8.9, 2009, pp. 1440-1450.

[3] SANS Institute InfoSec Reading Room, Computer Incident Response Team. 2001 (Accessed June 2015) http://www.sans.org/reading-room/whitepapers/incident/computer-incident-response-team-641

[4] J. Wiik, J. J. Gonzalez, P. I. Davidsen, and K. P. Kossakowski, Preserving a balanced CSIRT constituency. In Twenty Seventh International Conference of the System Dynamics Society July, at Albuquerque, NM, USA, 2009.

[5] Cyber Emergency Response Team UK Organization, (Accessed July 2015) http://www.cert.org/resilience/research/index.cfm

[6] Listing Of Worldwide CERT Organization, (Accessed August 2015) https://scadahacker.com/resources/cert.html

[7] JPCERT Coordination Center Incident Response, (Accessed August 2015) http://www.jpcert.or.jp/.

[8] US-CERT, United States Computer Emergency Readiness Team, (Accessed August 2015) https://www.us-cert.gov/

[9] Ulusal Siber Olaylara Müdahale Merkezi, (Accessed August 2015) https://www.usom.gov.tr/

BIOGRAPHIES

Yunus Emre KARABULUT was born in Sivas in Turkey. He received the B.Sc. Degree from Süleyman Demirel University, Turkey. Since 2015, he is currently M.Sc. student in Computer Engineering Department at Süleyman Demirel University. His current research interests are information security and search engine algorithms.

Gülistan BOYLU was born in Denizli in Turkey. He received the B.Sc. Degree from Süleyman Demirel University, Turkey. Since 2014, he is currently M.Sc. Student in Computer Engineering Department at Süleyman Demirel University. His current research interests are software engineering and software development.

Ecir Uğur KÜÇÜKSİLLE was born in Isparta, Turkey in 1976. He received the B.Sc. degree in Computer Systems Education form Gazi University, Turkey and M.Sc. degree in Department of Mechanical Education from Suleyman Demirel University. He obtained the Ph.D. degree in Numerical Methods in 2007 from Suleyman Demirel University, Turkey. His current research interests are information security and penetration tests.

Mehmet Ali YALÇINKAYA was born in Isparta in Turkey. He received the B.Sc. and M.Sc. Degrees from Süleyman Demirel University, Turkey. Since 2013, he has been with the Department of Computer Engineering at Süleyman Demirel University, Turkey as a Research Assistant. His current research interests are information security and penetration tests.