Global Cyber Security Capacity Centre

Computer Security Incident Response Teams (CSIRTs) An Overview

Maria Bada
Global Cyber Security Capacity Centre,
University of Oxford

Sadie Creese
Global Cyber Security Capacity Centre,
University of Oxford

Michael Goldsmith
Global Cyber Security Capacity Centre,
University of Oxford

Chris Mitchell
Global Cyber Security Capacity Centre,
Royal Holloway, University of London

Elizabeth Phillips
Oxford University's Centre for Doctoral Training (CDT)
Worcester College

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

May 2014

Contents

Abstract 4
1 Introduction 5
1.1 Scope and purpose 5
1.2 Structure of the paper 5
1.3 Audience 5
2 CSIRTs - An introduction 6
2.1 The role and purpose of CSIRTs 6
2.2 Terminology 6
2.3 Services provided by CSIRT teams 6
2.4 Categories of CSIRTs 7
2.5 Sectors of CSIRT operation 8
2.6 Building a new CSIRT 8
2.7 Determining the authority 9
3 Existing CSIRTs 10
3.1 National CSIRTs/CERTs 10
3.1.1 The UK CERT 10
3.1.2 The US-CERT 11
3.1.3 MyCERT Malaysia 12
3.2 Multinational European CSIRTs/CERTs 12
3.2.1 CERT EU 12
3.2.2 European Government CERTs Group (EGC) 12
3.3 CSIRT Cooperation and Coordination Organisations 13
3.3.1 FIRST – Forum of Incident Response and Security Teams 13
3.3.2 AP-CERT Asia Pacific Computer emergency Response Team 14
3.3.3 TERENA - Trans-European Research and Education Networking Association 14
3.3.4 TI Trusted Introducer 15
3.3.5 CEENet 15
3.3.6 NATO NCIRC TC 15
4 Case studies 16
4.1 Qatar 16
4.2 Tunisia 17
4.3 Kenya 18

4.4 Other Case studies 19
References 20

Computer Security Incident Response Teams (CSIRTs) An Overview

Maria Bada
Global Cyber Security Capacity Centre, University of Oxford, maria.bada@cs.ox.ac.uk

Sadie Creese
Global Cyber Security Capacity Centre, University of Oxford, sadie.creese@cs.ox.ac.uk

Michael Goldsmith
Global Cyber Security Capacity Centre, University of Oxford, michael.goldsmith@cs.ox.ac.uk

Chris Mitchell
Global Cyber Security Capacity Centre, Royal Holloway, University of London,
c.mitchell@rhul.ac.uk

Elizabeth Phillips
Oxford University's Centre for Doctoral Training (CDT), Worcester College
elizabeth.phillips@cybersecurity.ox.ac.uk

Abstract

Following the pioneering work at Carnegie-Mellon University in the US, national Computer Emergency Response Teams (CERTs) have been established worldwide to try to address the ever-growing threats to information systems and their use. The problem they are designed to address is clearly real and formidable, in mitigating the threats posed by cyber-criminals and state-sponsored cyber-attacks.

This paper is presenting the role and purpose of Computer Security Incident Response Teams (CSIRTs) the services they provide, and also various examples of existing national and multinational CSIRTs as well as organizations which foster the cooperation and coordination of CSIRTs are presented. The paper then presents case studies as examples of national CSIRTs.

1 Introduction

1.1 Scope and purpose

The purpose of this paper is to present the mission and services provided by Computer Security Incident Response Teams (CSIRTs) both at a National and Organizational level. The primary mission of a Computer Security Incident Response Team (CSIRT) is to help other organizations to handle incidents occurring in computer networks, as well as provide a wider set of services. Apart from their main mission, CSIRTs need to be able to adapt to a continuous changing environment and present the flexibility to deal any unexpected incident.

1.2 Structure of the paper

Section 2 of this paper describes the role and purpose of CSIRTs, the services they provide, as well as information on the different sectors of CSIRT cooperation and of building a new CSIRT.

Section 3, provides an overview of existing CSIRTs in National level, such as the UK CERT, the US CERT, the MyCERT from Malaysia, as well as Multinational European CSIRTs, such as CERT EU and the European Government CERTs Group (EGC). Also, in this section various organizations which foster the cooperation and coordination of CSIRTs are being presented. Examples are the Forum of Incident Response and Security Teams (FIRST), The Asia Pacific Computer Emergency Response Team (AP-CERT), The Task Force of Computer Security and Incident Response Teams (TERENA TF-CSIRT), The Trusted Introducer (IT), The Central and Eastern European Networking Association (CEENet) and The NATO Computer Incident Response Capability - Technical Centre (NATO NCIRC TC).

Section 4, presents case studies of countries who established their CERT. Each country follows different approach according to its sources and needs. Exapmles of Qatar, Tunisia and Kenya are described.

1.3 Audience

This paper is written primarily for Computer Security Incident Response Team (CSIRT) experts, Computer Emergency Response Team (CERT) experts, Chief Information Officers (CIOs), Senior Agency Information Security Officers (SAISOs) and Information System Security Officers (ISSOs). The measures presented can be used both within government and industry contexts.

2 CSIRTs - An introduction

This section presents the role and purpose of CSIRTs, the services they provide and the various sectors they can operate in. Moreover, the basic principles of building a new effective CSIRT, as well as the importance of the parameters within which the CSIRT will be able to act, are being presented.

In order to be able to tackle any type of cybersecurity incident we need the capacity to be available at least in some organizational form, in particular a CSIRT. These are single organizations that present information to end users as well as organizations with the country.

2.1 The role and purpose of CSIRTs

The name **Computer Emergency Response Team** is the historic designation for the first team (CERT/CC)[1] at Carnegie Mellon University (CMU). CERT is now a registered service mark of Carnegie Mellon University that is licensed to other teams around the world. Some teams took on the more generic name of **CSIRT** (Computer Security Incident Response Team) to point out the task of handling computer security incidents instead of other tech support work.

2.2 Terminology

CERT stands for Computer Emergency Response Team. Various abbreviations for the same sort of terms exist:

- CERT or CERT/CC (Computer Emergency Response Team / Coordination Centre)
- CSIRT (Computer Security Incident Response Team)
- IRT (Incident Response Team)
- CIRT (Computer Incident Response Team)
- SERT (Security Emergency Response Team)
- WARPs (Warning Advice and Reporting Points)

At the moment both terms (CERT and CSIRT) are used synonymously. In this document the term CSIRT will be used.

The history of CSIRTs is linked to the existence of malware, especially computer worms and viruses. Whenever a new technology arrives, its misuse is not long in following. The first worm in the IBM VNET was covered up. Shortly after, a worm hit the Internet on 3 November 1988, when the so-called Morris Worm paralysed a good percentage of it. This led to the formation of the CERT/CC at Carnegie Mellon University under a U.S. Government contract. With the massive growth in the use of information and communications technologies over the subsequent years, the now-generic term "CSIRT" refers to an essential part of most large organisations' structures.

2.3 Services provided by CSIRT teams

CSIRT teams provide various services such as reactive as well as proactive. Also, part of their purpose is Artifact handling as and security quality management. These services need to be realistic and reflect the financial, labour and technical resources available to a nation. A more analytical list of the CSIRT services is presented below (Table 1).

A CSIRT needs to act as a focal point for incident reporting and to be easily reached by users. A CSIRT has three essential attributes a) a central location in relation to its constituency b) an educational

[1] http://www.cert.org/

role with regard to computer security c) an incident handling role (Javaid, 2013). The accumulated experience of the personnel in a CSIRT is crucial, both in terms of responding to incidents and of educating others.

The European Commission[2] has presented also the requirements and tasks of a Computer emergency Response Team (CERT). ENISA[3] also released a November 2013 a report titled *Good practice guide for CERTs in the area of Industrial Control Systems - Computer Emergency Response Capabilities considerations for ICS*. This report, "*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 practices guide divides ICS-CERC provisions into four categories: mandate capabilities, technical operational capabilities, organisational operational capabilities, and co-operational capabilities.

Table 1. Services provided by CSIRTs

Reactive Services	Proactive Services	Artifact Handling	Security Quality Management
Alerts and Warnings Incident Handling Incident Analysis Incident Analysis Incident Response Support Incident Response Coordination Incident Response on Site Vulnerability Handling Vulnerability Analysis Vulnerability Response Vulnerability Response Coordination	Announcements Technology Watch Security Audits or Assessments Configuration and Maintenance of Security Development of Security Tools Intrusion Detection Services Security Related Information Dissemination	Artifact Analysis Artifact Response Artifact Response Coordination	Risk analysis Business Continuity and Disaster Recovery Security Consulting Awareness Building Education/Training Product Evaluation or Certification

CSIRT Services list from CERT/CC[4]

2.4 Categories of CSIRTs

General categories of CSIRTs include[5]:

- *Internal or organizational CSIRTs* - provide incident handling services to their parent organization (e.g. a university).
- *National CSIRTs* – coordinate and facilitate the handling of incidents for a particular country, or economy.

[2] European Commission, 2013 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:EN:PDF

[3] ENISA, Good practice guide for CERTs in the area of Industrial Control Systems - Computer Emergency Response Capabilities considerations for ICS, December 2013. 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

[4] CSIRT Services list from CERT/CC: http://www.cert.org/csirts/services.html

[5] Creating and Managing Computer Security Incident Handling Teams (CSIRTs), CERT Training and Education Networked Systems Survivability Software Engineering Institute Carnegie Mellon University, 2008. http://www.first.org/conference/2008/papers/killcrece-georgia-slides.pdf

- *Analysis Centers* – focus on synthesizing data from various sources to determine trends and patterns in incident activity. This information can then be used to help predict future activity or provide early warning when current activity matches a set of previously determined characteristics.
- *Vendor Teams* – coordinate with organizations who report and track vulnerabilities.
- *Incident Response Providers* – provide incident handling services as a product to other organizations. These are sometimes referred to as Managed Security Service Providers (MSSPs).

Various global and regional organizations devoted to incident management collaboration and coordination have been created. This includes organizations such as the:

- Forum of Incident Response and Security Teams http://www.first.org/

2.5 Sectors of CSIRT operation

There can be more than one CSIRT in a country serving the interest of various constituencies for example the academic, banking sectors, the commercial sector, CIP/CIIP Sector, governmental/national sector, military, energy sector, financial sector and within organisation.

These CSIRTs are focussed on and provide services and support to their defined constituency for the prevention of, handling, and response to cybersecurity incidents. However it is also possible for a country to designate an entity as a national CSIRT to serve a principle entity serving Government or government-related organisations.

2.6 Building a new CSIRT

In order to create an effective CSIRT, Carnegie Mellon University (CMC, J Haller, 2011) believe that there are four core principles all CSIRTs must have:

- **Technical Excellence:** The National CSIRT/CERT should have the most up to date resources and advice and in order to maintain this advantage, the advice they give must be sound which requires high levels of technical excellence. This may lead to the CSIRT only being initially with a small number of good quality capabilities rather than lots of poor quality capabilities.
- **Trust:** If the organizations and end users do not explicitly trust the CSIRT then they will be unable to share data with the CSIRT and will not be able to use all the facilities on offer. The trust is crucial for partner organisations and the organisations themselves would want confirmation that the CSIRT can handle sensitive information responsibly.
- **Resource Efficiency:** The CSIRT must be constantly adapting by analysing potential new threats and their potential impact. This will then help to steer the allocation of funding sources to test, which treats and incidents are truly of interest to the CSIRT.
- **Cooperation:** The CSIRT should cooperate as fully as possible (taking into account the sensitivity of some of their clients' data) with national stakeholders, government and other National CSIRTs/CERTs so that the knowledge can be shared and they can collaborate on complex problems.

Before the real work begins, it is crucial to identify key partners and Sponsors to ensure the financial security of the CSIRT. After this has been established, it is then necessary to determine any limiting factors such as time commitment, skill level of staff and the physical infrastructure available[6].

[6] Grobler Marthie and Bryk Harri, 2010. http://icsa.cs.up.ac.za/issa/2010/Proceedings/Full/17_Paper.pdf

2.7 Determining the authority

Depending on the purpose of the CSIRT and its sponsor, the CSIRT may be capable of prescribing or mandating particular actions after cyber-attacks and may be able to enforce other security measures. However, in some instances government approval/advice may be required first before conducting any action.

The parameters within which the CSIRT will be able to act will depend on the specific nation's laws, cultures and customs. The precise nature of the CSIRT may determine the level of cooperation and sharing of sensitive data as some organizations may be reluctant to disclose information if they believe the CSIRT to be too self-governing.

3 Existing CSIRTs

There are a large number of CSIRTs in existence, in many different countries. Every country has different CSIRT capabilities as well as a different level of maturity to dispose. African countries such as Kenya, Mauritius, South Africa and Tunisia have National CSIRTs/CERTs to present. Moreover, many countries in the rest of the world have already built CSIRTs.

This section provides an overview of existing CSIRTs/CERTs at a National level, such as the UK CERT, the US CERT, the MyCERT from Malaysia, as well as Multinational European CERTs, such as CERT EU and the European Government CERTs Group (EGC). Also, in this section various organizations which foster the cooperation and coordination of CERTs are being presented. Examples are the Forum of Incident Response and Security Teams (FIRST), The Asia Pacific Computer Emergency Response Team (AP-CERT), The Task Force of Computer Security and Incident Response Teams (TERENA TF-CSIRT), The Trusted Introducer (IT), The Central and Eastern European Networking Association (CEENet) and The NATO Computer Incident Response Capability - Technical Centre (NATO NCIRC TC).

3.1 National CSIRTs/CERTs

3.1.1 The UK CERT

UK's National Computer Emergency Response Team (CERT-UK)[7] works closely with industry, government and academia to enhance UK cyber resilience. CERT-UK has four main responsibilities that flow from the UK's Cyber Security Strategy[8]:

- National Cyber Security Incident Management.
- Support to Critical National Infrastructure companies to handle cyber security incidents.
- Promoting cyber security situational awareness across industry, academia, and the public sector.
- Providing the single international point of contact for co-ordination and collaboration between national CERTs.

CERT-UK falls under the Communications-Electronics Security Group (CESG)[9], the UK Government's National Technical Authority for Information Assurance. Their Incident Response Guidelines[10], provide clear details to individuals and companies as to what falls within the scope of GovCertUK and what is beyond its control. An important part of their mission is to educate everyday users by producing interesting posters and clear information packs[11] for organizations and end users.

In order to reinforce the idea of simplicity for the users there are only four categories for reporting incidents, namely:

- **A**. Concerned Targeted Attack must be reported to GovCertUK. Incidents that are concerted, repeating, targeted and causing harm to confidentiality, integrity or availability of ICT systems or data.
- **B.** Targeted Attack must be reported to GovCertUK. Incidents that are repeating, targeted and causing harm to confidentiality, integrity or availability of ICT systems or data.

[7] CERT UK https://www.cert.gov.uk/

[8] UK's Cyber Security Strategy https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

[9] CESG https://www.cesg.gov.uk

[10] GovCertUK Incident Response Guidelines, http://www.cesg.gov.uk/publications/Documents/incident_response_guidelines.pdf

[11] GovCertUK Information packs http://www.cesg.gov.uk/awarenesstraining/PET/Pages/index.aspx

- **C.** Non-Targeted GovCertUK is to be tipped. Incidents that are general and non-targeted or incidents where the IT teams suspect suspicious behaviour.
- **D.** Other reporting GovCertUK is to be tipped. Cryptographic events such as loss of laptop/media, protective marking breaches etc.

The term ''reported'' means that a formal report needs to be submitted and ''tipped'' that GovCertUK need to be informed but no formal report is required. The informal method of tipping off GovCertUK encourages companies to seek advice and inform GovCertUK even if they are unsure as it is not time consuming and they can still get advice and guidance, which improves the trust between GovCertUK and the organization or user.

When an incident is reported and GovCertUK advices action needs to be taken, a step-by-step guide indicating how to resolve the situation is sent directly to the victim along with a summary of the incident containing the most important information should the organization want to conduct its own investigations at a later date.

The UK CERT not only analyse and handle incidents, but also actively welcome samples of malicious code so that it can help improve their understanding and stress that a formal report need not be completed with the code. Moreover, GovCertUK stress that no ''blacklist'' of companies is maintained and if a report leads to further action then no blacklisting will happen either. The transparent nature of GovCertUK allows the organizations to trust their actions and the users feel happy to report an incident.

3.1.2 The US-CERT

US-CERT[12] is a partnership between the Department of Homeland Security and the public and private sectors. It was established to protect the nation's Internet infrastructure and coordinate defence against and responses to cyber-attacks across the nation. US-CERT was established in order to improve computer security preparedness and respond to cyber-attacks in the United States. In addition, US-CERT also provides a way for citizens, businesses and other institutions to communicate and coordinate directly with the United States government about cyber security.

In a similar way to GovCertUK, they also produce a large number of self-help guides, which are publicly available. These publications range from instructions as to how to secure your computer from spyware to disposing of devices safely and anything in between.

Their advice refers to both home and business users and include basic cloud security, home network security and information to help them understand denial of service attacks and how to avoid social engineering and phishing attacks. Government users are directed into specific alerts and bulletins relevant to the current situation as well as tools, programs and guidance about the reporting of incidents whereas Control System Users see more targeted information regarding the latest software update alerts, recommended practices, training and assessment tools for the organization.

This targeted information ensures that home users are not bombarded with irrelevant information whereas technically aware Control System Users are given more detail in their information with regards to the technical skills and best practises needed to protect most cybersecurity attacks.

[12] US-CERT https://www.us-cert.gov/about-us

3.1.3 MyCERT Malaysia

MyCERT[13] is the Malaysian CERT and works closely with the CERT coordination center and the partners below:

- Asia Pacific Computer emergency Response Team (AP-CERT)
- Organization of the Islamic Conference-Computer-Emergency Response Team[14] (OIC-CERT)
- The Honeynet Project[15]
- Forum for Incident Response and Security Teams (FIRST)
- The Anti-Phishing Working Group[16] (APWG)

MyCERT's primary mission is to address the computer security concerns of internet users and its vision is to reduce the probability of successful attacks and lower the risk of consequential damage. MyCERT appreciates the importance of local end users but has a narrower range of facilities.

3.2 Multinational European CSIRTs/CERTs

3.2.1 CERT EU

CERT EU is a permanent Computer Emergency Response Team (CERT-EU)[17] for the EU institutions, agencies and bodies. The team is made up of IT security experts from the main EU Institutions (European Commission, General Secretariat of the Council, European Parliament, Committee of the Regions, Economic and Social Committee). It cooperates closely with other CERTs in the Member States and beyond as well as with specialised IT security companies.

CERT-EU's mission is to support the European Institutions to protect themselves against intentional and malicious attacks that would hamper the integrity of their IT assets and harm the interests of the EU. The scope of CERT-EU's activities covers prevention, detection, response and recovery. CERT-EU operates according to the following key values:

- Highest standards of ethical integrity
- High degree of service orientation and operational readiness
- Effective responsiveness in case of incidents and emergencies and maximum commitment to resolve the issues
- Building on, and complementing the existing capabilities in the constituents
- Facilitating the exchange of good practices between constituents and with peers
- Fostering a culture of openness within a protected environment, operating on a need to know basis

CERT-EU gradually extends its services, on the basis of the requirements of its constituency and takes into account the available competencies, resources and partnerships.

3.2.2 European Government CERTs Group (EGC)

Within the EU some of the countries with successful CSIRTs have joined together to form the European Government CERTs Group (EGC).[18] The EGC exists to informally associate the CERTs across

[13] MyCERT http://www.mycert.org.my/en/
[14] OIC-CERT http://www.oic-cert.net/v1/index.html
[15] The Honeynet Project http://www.honeynet.org/about
[16] APWG http://www.antiphishing.org/
[17] CERT EU http://cert.europa.eu/cert/
[18] The European Government CERTs Group http://www.egc-group.org/

Europe. This group encourages the collaboration between nation CERTs which increases each country's individual knowledge. The group tries to:

- Jointly develop measures to deal with large-scale or regional network security incidents
- Facilitate information sharing and technology exchange relating to IT security incidents and malicious code threats and vulnerabilities
- Identify areas of specialist knowledge and expertise that could be shared within the group
- Identify areas of collaborative research and development on subjects of mutual interest
- Communicate common views with other initiatives and organizations.

The countries which build the European Government CERTs group are:

- Austria - GovCERT.AT
- Belgium - CERT.be
- Denmark - Danish GovCERT
- Finland - CERT-FI
- France - CERT-FR
- Germany - CERT-Bund
- Netherlands - NCSC-NL
- Norway - NorCERT
- Spain - CCN-CERT
- Sweden - CERT-SE
- Switzerland - GovCERT.ch
- United Kingdom - CSIRTUK
- United Kingdom - GovCertUK

3.3 CSIRT Cooperation and Coordination Organisations

Successful cooperation[19] among CSIRT or Abuse Teams located in different countries in many regions is a key factor for successful incident handling due to the global character of the Internet and security threat propagation.

But also many other CSIRT services are strongly dependent on collaboration with other teams from different parts of the world.

3.3.1 FIRST – Forum of Incident Response and Security Teams

The Forum of Incident Response and Security Teams[20] (FIRST), consists of a network of individual computer security incident response teams that work together voluntarily to deal with computer security problems and their prevention, to stimulate rapid reaction to incidents and promote information sharing among members of the community at large.
First's mission includes:

- FIRST develops and share of technical information, tools, methodologies, processes and best practices
- FIRST encourages and promotes the development of quality security products, policies & services
- FIRST develops and promulgates best computer security practices

[19] ENISA, 2006, CERT_cooperation_ENISA.pdf
[20] FIRST http://www.first.org/

- FIRST promotes the creation and expansion of Incident Response teams and membership from organizations from around the world
- FIRST members use their combined knowledge, skills and experience to promote a safer and more secure global electronic environment.

3.3.2 AP-CERT Asia Pacific Computer emergency Response Team[21]

AP-CERT is a coalition of CERTs from 13 economies across the Asia Pacific region. AP-CERT organises an annual meeting called APSIRC conference and the first conference was held in 2002, in Tokyo, Japan. The mission of AP-CERT is to improve the region's awareness and competency in relation to computer security incidents through:

- Enhancing Asia Pacific regional and international cooperation on information security.
- Jointly developing measures to deal with large-scale or regional network security incidents. Facilitating information sharing and technology exchange, including information security, computer virus and malicious code among its members.
- Promoting collaborative research and development on subjects of interest to its members.
- Assisting other CERTs and CSIRTS in the region to conduct efficient and effective computer emergency response.
- Providing inputs and/or recommendations to help address legal issues related to information security and emergency response across regional boundaries.

3.3.3 TERENA - Trans-European Research and Education Networking Association

The Trans-European Research and Education Networking Association[22] (TERENA), offers a forum to collaborate, innovate and share knowledge in order to foster the development of Internet technology, infrastructure and services to be used by the research and education community. TERENA works in close collaboration to TF-CSIRT, providing secretarial support.

3.3.3.1 TERENA TF-CSIRT Task Force of Computer Security and Incident Response Teams

Task Force of Computer Security and Incident Response Teams (TF-CSIRT) is a task force that promotes collaboration and coordination between CERTs in Europe and neighbouring regions, whilst liaising with relevant organisations at the global level and in other regions.

TF-CSIRT provides a forum where members of the CERT community can exchange experiences and knowledge in a trusted environment in order to improve cooperation and coordination. It maintains a system for registering and accrediting CERTs, as well as certifying service standards. The task force also develops and provides services for CERTs, promotes the use of common standards and procedures for handling security incidents, and coordinates joint initiatives where appropriate. This includes the training of CERT staff, and assisting in the establishment and development of new CERTs.

The task force further liaises with FIRST, ENISA, other regional CERT organisations, as well as defence and law enforcement agencies. Secretarial support for this task force is provided by TERENA with funding from the GN3 project.

[21] AP-CERT http://www.apcert.org/
[22] TERENA http://www.terena.org/

3.3.4 TI Trusted Introducer

Trusted Introducer (TI)[23], provides European CERTs with a public repository that lists all known European CERTs and explains about the TI's accreditation service. It facilitates trust by formally accrediting CERTs that are ready to take that step. Once accredited, a CERT can gain access to the restricted TI repository. There they can find details on fellow CERTs, readily downloadable contact lists and PGP-Key rings, secure discussion forum, automatic RIPE Database IRT-object registration and more.

3.3.5 CEENet

The Central and Eastern European Networking Association (CEENet)[24] is a regional cooperation in Central and Eastern Europe and includes some adjacent countries from Asia, has as goal to share computer networking knowledge between more and less developed members of the association. The primary mission of CEENet is to co-ordinate the international aspects of the academic, research and education networks in Central and Eastern Europe and in adjacent countries. Moreover, CEENet promotes and supports the technical and organizational collaboration between NRENs

3.3.6 NATO NCIRC TC

NATO Computer Incident Response Capability - Technical Centre (NCIRC TC)[25] is the Tier 2 of the NATO Computer Incident Response Capability (NCIRC). This site is maintained by NATO Information Assurance Technical Centre (NIATC) to provide operational CERT support to the NATO CIS community, including a) Incident Handling b) Vulnerability and Threat Information c) Vulnerability Assessment (online / on site) d) Consultancy Services (Scientific and Forensic) e) Online Data Collection and Monitoring (IDS, Antivirus, Firewalls) f) Online Support (auto updates, downloads, SOPs) and g) Offline incident analysis and security testing.

[23] TI http://www.trusted-introducer.org/
[24] CEENET http://www.ceenet.org/
[25] NCIRC NATO http://www.ncirc.nato.int/

4 Case studies

In this section we look in greater details at three examples of national CSIRTs/CERTs. More specifically Qatar, Tunisia and Kenya CERTs are being presented. It is obvious that each country follows a different approach according to its sources and needs.

Through reviewing these examples we can get an idea of the scope of their activities, which in turn helps understand how one might assess their effectiveness.

4.1 Qatar

The Middle East and specifically ictQATAR (Supreme Council of Information Technology of Qatar) as the premier national body responsible for technology initiatives, recognised the role of ICT plays in the region and the need for a long term strategic partnership with CERT/CC. As such, they sponsored Qatar Computer Emergency Response Team (Q-CERT)[26] program and was the founding partner of the regional GCC-CERT initiative. It was initially influenced by the Council of Information and Communication Technology (ictQATAR), CERT/CC and Carnegie Mellon University's Software Engineering Institute.

Q-CERT's Vision is to be recognized as:

- A leader in Qatar and the region in promoting IT Security Standards, Practices, Products and Services to improve the security of critical IT infrastructure.
- A credible source of Cyber Security information.
- A trusted confidant partner in responding to Cyber Security incidents.
- A leader in building the CyberSecurity human capacities in State of Qatar.

They divided their work efforts into three main categories, namely ''Critical Infrastructure Protection'' ''Watch, Warning, Investigation and Response'' and ''Outreach, Awareness and Teaching''.

- **Critical Infrastructure Protection:** Their aim was to assist key national resources in identifying and addressing information security vulnerabilities and threats and provide new approaches for damage assessment and recovering operations from affected systems alongside other tasks.
- **Watch, Warning, Investigation and Response:** Their aim was to assist in creating new cybercrime and privacy laws and establish a national center for threat, vulnerability and security event data.
- **Outreach, Awareness and Teaching:** They aim to be able to act as a forum for national dialog on cyber security and increase the awareness and understanding of cyber security issues within public and private institutions across the public. A Curriculum in Information Security was created which included
    a) Creating a Computer Security Incident Response Team (CSIRT)
    b) Managing Computer Security Incident Response Teams
    c) Fundamentals of Incident Handling
    d) Advanced Incident Handling
    e) Information Security for Technical Staff
    f) Advanced Information Security for Technical Staff
    g) Computer Forensics for Technical Staff
    h) OCTAVE Training Workshop

[26] Q-CERT, http://www.qcert.org/

Their initial ideas have set down a long term sponsorship for the CERT which will enable continuity and the security of future research which will be alongside their increasing relationship with CERT/CC.

4.2 Tunisia

Tunisia [27] set up their CERT called CERT-TCC to have the national responsibility of acting to provide incident management services for:

- Government
- Public and Private Sector
- Home Users
- Professionals
- Banks

The CERT-TCC provides services free of charge to organizations and tries to ensure:

- A centralized coordination for IT security issues (Trusted Point of Contact)
- Centralized and specialized unit for incident response
- Technology and security watch
- Cyberspace monitoring
- The expertise to support and assist to quickly recover from security incidents
- Awareness of all categories of users

The CERT-TCC adopted a limited resources low cost approach and relied more on open sourced approaches. These approaches reduced the cost but had an effect on trust associated with the CERT due to open sourced handling of sensitive data.

Awareness is the main focal point of the CERT-TCC and their approach relies on the collaboration of national partners in order to provide free technical support to customers. They also provided attack simulations in order to assess the possible vulnerabilities of organizations. Tunisia, has established also a National Reaction Plan which is the formal plan which initiates the establishment of Coordination Crisis Cells across the country. This approach has been deployed with great success in 2004 for the African Football Cup and the Presidential Elections as well as during the Arab League in 2005.

The high skills of the employees in combination to the low running costs, made available a wide range of services including incident analysis, incident response coordination, penetration testing, virus handling and hotlines in addition to secondary services such as security policy development, forensic evidence collection and monitoring of network and system logs.

[27] Developing national CSIRT capabilities – A case study of Tunisian CERT http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/elmir-ansi-csirt-june-09.pdf

4.3 Kenya

There have been various initiatives to establish a national CERT[28] in Kenya. Kenya increasingly becomes more connected to and dependent on the internet and it was important to determine the risk exposure from not having a CERT.

The first such initiative was CERT-Kenya that was sponsored by the Kenya Network Information Centre (KENIC) and the Telecommunication Service Providers of Kenya (TESPOK). The objective of the CERT-Kenya was to assist members of the local internet community in implementing proactive measures to reduce the risks of computer security incidents and to assist the community in responding to such incidents when they occur. However CERT-Kenya is currently not functional.

The Kenya Information and Communications Act CAP411A mandates the Communications Commission of Kenya (CCK) to develop a national cyber security management framework through the establishment of a national Computer Incident Response Team (CIRT). CCK setup the Kenya Computer Incident Response Team Cordination Center (KE-CIRT/CC)[29] whose mandate is to coordinate response and manage cyber security incidents nationally and to collaborate with relevant actors locally, regionally and internationally.

Its functions are as follows:

- Coordinating computer security incident response at the national level and acting as a national trusted point of contact
- Liaising with the local sector Computer Incident Response Teams (CIRTs), regional CIRTs, international CIRTs and other related organizations
- Gathering and disseminating technical information on computer security incidents, vulnerabilities, security fixes and other security information, as well as issuing alerts and warnings
- Carrying out research and analysis on computer security, related technologies and advising on new trends
- Facilitating the development of a national Public Key Infrastructure (PKI) and,
- Capacity building in information security and creating and maintaining awareness on cybersecurity-related activities, among others

The Industry Computer Security Incident Response Team (iCSIRT) is an initiative of Telecommunication Service Providers of Kenya (TESPOK). iCSIRT has been established to ensure network integrity and information security is maintained at the Kenya Internet Exchange Point (KIXP). Services currently offered by the iCSIRT include weekly reports on bad IPs reported on the member's networks, security bulletins, alerts and warnings and general security incident handling. The overall goal of the iCSIRT is to develop and promote the use of appropriate technology and systems management practices to resist attacks on networked systems, to limit damage and ensure continuity of critical services.

The East Africa Communications Organization (EACO) set up a Cybersecurity Taskforce. The vision of the taskforce is to build confidence and security in the use of cyberspace in the East Africa (EA)

[28] Mwende Njiraini, Establishing a National Computer Incident Response Team (CSIRT) in Africa: Kenyan case study, 2011, http://api.ning.com/files/CiKtTdA9zz-bW-rycYFYBYPsPW3M6MW83isAbwDQEvM7UoZt7B9oQ9xLbNk*fZbBJxfUnVWV7k6nkQYcmpAtpSNljYO-yGZT/EstablishingaNationalComputerSecurityIncidentResponseTeamCSIRTinAfricaAKenyanCaseStudy.pdf

[29] KE- CIRT/CC http://www.cck.go.ke/industry/information_security/ke-cirt-cc/

region while its mission is to enhance security of the cyberspace in the EA region through collaboration amongst all the stakeholders.

4.4 Other Case studies

Other countries have established CERTs effectively. A few examples can be viewed from the case studies below:

- Setting up a Governmental CERT - A case study of Spain's CCN-CERT
  http://www.first.org/conference/2007/papers/abad-carlos-slides.pdf
- A National Cyber Security Strategy, A case study of Arab emirates CERT
  http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/bazargan-national-strategy-aeCERT-doha-feb-08.pdf
- Vietnam Computer Emergency Response Team Case Studies
  http://www.cicc.or.jp/japanese/kouenkai/pdf_ppt/afit/7_Mr.%20Do%20Ngoc%20Duy%20Trac.pdf
- Sri Lankan Computer Emergency Response Team Case Studies
  http://www.slcert.gov.lk/case.html
- Digital Security Consulting Case Studies
  http://www.dsconsult.net/case-studies.php

References

AP-CERT, Asia Pacific Computer emergency Response Team, Retrieved from http://www.apcert.org/

APWG, The Anti-Phishing Working Group. Retrieved from http://www.antiphishing.org/

Arora, Ashish and Telang, Rahul and Xu, Hao, Optimal Policy for Software Vulnerability Disclosure, 2005. Retrieved from http://dx.doi.org/10.2139/ssrn.669023

CERT. Retrieved from http://www.cert.org/

CERT EU. Retrieved from http://cert.europa.eu/cert/

CERT UK. Retrieved from https://www.cert.gov.uk/

CSIRT Services list from CERT/CC. Retrieved from http://www.cert.org/csirts/services.html

ENISA, Good practice guide for CERTs in the area of Industrial Control Systems - Computer Emergency Response Capabilities considerations for ICS, December 2013. Retrieved from 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

ENISA CERT Inventory – Inventory of CERT teams and activities in Europe, Version 2.12b, January 2014. Retrieved from http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

ENISA, Step-by-Step Guide to Setting Up a CSIRT. Retrieved from: http://www.enisa.europe.eu/cert_guide/downloads/CSIRT_setting_up_guide_ENISA.pdf

European Commission (EC), Proposal for a Directive of the European Parliament and of the council concerning measures to ensure a high common level of network and information security across the Union, Brussels, 7.2.2013, COM (2013) 48 final. Retrieved from http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:EN:PDF

Forming an Incident Response Team http://www.auscert.org.au/render.html?it=2252&cid=1920

FIRST, Creating and Managing Computer Security Incident Handling Teams (CSIRTs), CERT Training and Education Networked Systems Survivability Software Engineering Institute Carnegie Mellon University, 2008. http://www.first.org/conference/2008/papers/killcrece-georgia-slides.pdf

FIRST, Forum of Incident Response and Security Teams. Retrieved from http://www.first.org/

GovCertUK Incident Response Guidelines. Retrieved from http://www.cesg.gov.uk/publications/Documents/incident_response_guidelines.pdf

GovCertUK Information packs. Retrieved from http://www.cesg.gov.uk/awarenesstraining/PET/Pages/index.aspx

Grobler Marthie and Bryk Harri, Common Challenges Faced During the Establishment of a CSIRT, IEEE, 2010. Retrieved from http://icsa.cs.up.ac.za/issa/2010/Proceedings/Full/17_Paper.pdf

Internet Engineering Task Force (IETF), Site Security Handbook. http://www.ietf.org/rfc/rfc2196.txt

Internet Engineering Task Force (IETF), Expectations for Computer Security Incident Response. http://www.ietf.org/rfc/rfc2350.txt

Internet Engineering Task Force (IETF), Internet Security Glossary. http://www.ietf.org/rfc/rfc2828.txt

ITU, Developing national CSIRT capabilities – A case study of Tunisian CERT. Retrieved from http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/elmir-ansi-csirt-june-09.pdf

Q-CERT, Qatar Computer Emergency Response Team. Retrieved from http://www.qcert.org/

Javaid, Muhammad Adeel, Benchmarks for Setting Up CERT (September 10, 2013). Available at SSRN: http://dx.doi.org/10.2139/ssrn.2389061

Kang, Jerry, Information Privacy in Cyberspace Transactions. Stanford Law Review, Vol. 50, p. 1193, 1998. Available at SSRN: http://ssrn.com/abstract=631723

Kenya Computer Incident Response Team Coordination Centre (KE-CIRT CC). Retrieved from http://www.cck.go.ke/industry/information_security/ke-cirt-cc/

Mwende Njiraini, Establishing a National Computer Incident Response Team (CSIRT) in Africa: Kenyan case study, 2011. Retrieved from http://api.ning.com/files/CiKtTdA9zz-bW-rycYFYBYPsPW3M6MW83isAbwDQEvM7UoZt7B9oQ9xLbNk*fZbBJxfUnVWV7k6nkQYcmpAtpSNljYOyGZT/EstablishingaNationalComputerSecurityIncidentResponseTeamCSIRTinAfricaAKenyanCaseStudy.pdf

MyCERT Malaysia. Retrieved from http://www.mycert.org.my/en/

NATO Computer Incident Response Capability - Technical Centre (NCIRC TC). Retrieved from http://www.ncirc.nato.int/

NIST, Computer Security Incident Handling Guide, National Institute of Standards and Technology (NIST SP 800-61). http://www.csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

OIC-CERT, Organization of the Islamic Conference-Computer-Emergency Response Team. Retrieved from http://www.oic-cert.net/v1/index.html

Solove, Daniel J., A Taxonomy of Privacy. University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, January 2006; GWU Law School Public Law Research Paper No. 129. Available at SSRN: http://ssrn.com/abstract=667622

Spiekermann Sarah, Cranor Faith Lorrie, Engineering Privacy, *IEEE Transactions on Software Engineering, Vol. 35, Nr. 1, 2009.* Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1085333

Spiekermann, Sarah and Berendt, Bettina and Grossklags, Jens, E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior. Available at SSRN: http://ssrn.com/abstract=761107

Strandburg, Katherine J., Privacy, Rationality, and Temptation: A Theory of Willpower Norms. Rutgers Law Review, Vol. 57, No. 4, Spring 2005. Available at SSRN: http://ssrn.com/abstract=755284

TERENA, Trans-European Research and Education Networking Association. Retrieved from http://www.terena.org/

Terena, TF-CSIRT Guide to Setting up a CSIRT. http://www.terena.org/activities/tf-csirt/archive/acert7.html

Trim Peter and Youl Youm Heung, Korea-UK Collaboration in Cyber Security: From Issues and Challenges to Sustainable Partnership Report Submitted to the Korean Government and the UK Government, March, 2014, British Embassy Seoul: Republic of Korea. Retrieved from http://www.iaac.org.uk/ItemFiles/ReportTrimYoumCyberSecurityMarch14.pdf

Trusted Introducer,(TI). Retrieved from http://www.trusted-introducer.org/

Software Engineering Institute (SEI), Avoiding the Trial-by-Fire Approach to Security Incidents. http://www.sei.cmu.edu/news-at-sei/columns/security_matters/1999/mar/security_matters.htm

The European Governent CERTs Group. Retrieved from http://www.egc-group.org/

UK's Cyber Security Strategy. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

US-CERT. Retrieved from https://www.us-cert.gov/about-us

GOVCERT.NL CERT-IN-A-BOX. http://www.govcert.nl/render.html?it=69

The Central and Eastern European Networking Association (CEENET). Retrieved from http://www.ceenet.org/

Communications-Electronics Security Group, Retrieved from https://www.cesg.gov.uk

The Honeynet Project. Retrieved from http://www.honeynet.org/about

The Global Cyber Security Capacity Centre is funded by Commonwealth Office and hosted by the Oxford

Oxford Martin School, University of Oxford,
Old Indian Institute, 34 Broad Street, Oxford
OX1 3BD, United Kingdom

Tel: +44 (0)1865 287430 • Fax: +44 (0)1865 287435
Email: cybercapacity@oxfordmartin.ox.ac.uk • • www.oxfordmartin.ox.ac.uk