Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development

08-Jun-2015

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INNOVATION
COMMITTEE ON DIGITAL ECONOMY POLICY

DSTI/ICCP/REG(2013)9/FINAL
Unclassified

Working Party on Security and Privacy in the Digital Economy

GUIDANCE FOR IMPROVING THE COMPARABILITY OF STATISTICS PRODUCED BY COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTs)

JT03378078

English - Or. English

FOREWORD

This document presents guidance for improving the international comparability of statistics produced by Computer Security Incident Response Teams (CSIRTs). The project – undertaken in co-operation with the Asia-Pacific Economic Co-operation (APEC) Information and Telecommunications Working Group (TEL) – emerged from the findings of a 2012 OECD report on *Improving the Evidence Base for Information Security and Privacy Policies* (OECD, 2012b), which identified an opportunity to work with CSIRTs to improve their statistics and to develop better statistical indicators for digital security risk. The 2011 *OECD Recommendation on Principles for Internet Policy Making* provides further impetus for this work in its call for stakeholders to "develop capacities to bring publicly available, reliable data into the policy-making process" (OECD, 2011), such as data accessible to CSIRTs.

An undertaking such as this requires a multidisciplinary perspective. A key characteristic of the project, therefore, was the mix of three different areas of expertise:

- Computer emergency and incident response: the CSIRT community was a key partner on the project.

- Digital security policy making: the project was initiated at the OECD Committee on Digital Economy Policy (CDEP) Working Party on Security and Privacy in the Digital Economy (SPDE) and the APEC Telecommunications and Information Working Group (TEL) Security and Prosperity Steering Group (SPSG) agreed to participate.

- Internationally comparable statistics for better policies: the OECD is the international forum for developing internationally recognised statistical guidance. Examples in other areas include the *OECD Guide to Measuring the Information Society*, the *OECD Patent Statistics Manual*, the *OECD Oslo Manual* (on measuring innovation) and the *OECD Frascati Manual* (on measuring research and development).

An initial description of the CSIRT statistics project was presented at the 33rd meeting of the OECD SPDE in October 2012 and further developed at its 34th and 35th meetings in April and December 2013. At the 36th meeting in June 2014, delegates discussed a preliminary analysis of results from a feasibility study aiming to test whether CSIRTs could report data about their constituencies, the size of their networks, numbers of users within their purview, organisational capacity and specific types of incidents. The statistical guidance was finally approved by SPDE delegates at its 37th meeting in December 2014 and declassified by its parent body, the CDEP, in May 2015.

This document is the culmination of over two years of research and engagement with the incident response, digital security ("cybersecurity") policy and statistical communities. It includes insights drawn from interviews with CSIRT experts and in-depth discussions at various international cybersecurity events.

In the initial stages of the project, the Secretariat carried out 12 interviews with experts from CSIRTs and the digital community. The interviews covered a range of topics, including the factors that affect the creation, use and diffusion of CSIRT statistics, the kinds of data CSIRTs use to create statistics and the various sources of bias that limit the international comparability of CSIRT statistics. In addition to these interviews, the Secretariat undertook several exchanges with representatives of CSIRTs covering the project's aims and objectives, garnering input on the feasibility of the project, potential challenges and the best way forward for the development of statistical guidance and statistical indicators. As part of the

engagement efforts, presentations were made at several meetings and conferences over the course of the project. Annex A summarises these outreach activities.

This guidance also builds on findings from a feasibility study of draft statistical indicators carried out in 2014. There were 24 completed responses to the study overall, from 20 national CSIRTs based in OECD member countries, four CSIRTs from Asia Pacific Computer Emergency Response Team (APCERT) economies (three of which are also OECD members), and three national CSIRTs from other regions. Annex B lists the CSIRTs that participated in the feasibility study.

This voluntary guidance has been written in conjunction with – and for use by – CSIRTs with national responsibilities (i.e. national CSIRTs) from both OECD members *and* non-members. It is intended as a guide that CSIRTs from a wide range of countries/economies can use to make their statistics more comparable. Its ultimate objective is to improve the evidence base for informing digital security policy making.

It is important to underline that this document represents the first stage to improve the international comparability of CSIRT statistics. Further work is needed to proceed with the actual collection of the data and to further develop this guidance with a view to overcome various challenges indicated throughout the document, and possibly others that large scale statistical data collection is likely to reveal. It will therefore be important, as such data becomes available, to interpret it with appropriate caution. In addition, a list of CSIRT statistical indicators meriting further consideration, exploration and development in the future is provided in Annex D.

The Secretariat would like to express its deep gratitude to all the experts and CSIRT representatives who participated in this project and listed in Annex C. It would like to thank the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) for its financial support and, in particular, Yurie Ito for championing this work since its inception. The Secretariat would also like to thank the Korea Internet & Security Agency (KISA) for its support of the project.

The report was prepared by Aaron Martin and Terrence Park under the supervision of Laurent Bernat (OECD Secretariat).

Following the 37th meeting of the OECD Working Party on Security and Privacy in the Digital Economy in December 2014, representatives of the Japan Computer Emergency Response Team Coordination Center, Korea Internet Security Center, and United States Computer Emergency Readiness Team expressed a joint commitment to implementing the CSIRT statistical guidance presented in this document, building on its findings to improve the holistic measurement of digital security risk and carrying forward work in this area.

Concretely, these organisations agree to testing a subset of the statistical indicators detailed in the guidance for presentation and discussion at the Annual Meeting of CSIRTs with National Responsibility at the FIRST Conference to take place in Berlin, Germany in June 2015 and the APCERT Annual General Meeting in Kuala Lumpur, Malaysia in September 2015, among other events. They will continue the development and improvement of the CSIRT statistical guidance, identifying best practices, with a longer-term and broader view of enriching the evidence base for international policy making in this area.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Computer Security Incident Response Teams (CSIRTs) play an essential role in digital security risk management ("cybersecurity") and occupy a position of trust in the digital environment. Their main responsibility is to prevent, handle and mitigate computer security incidents with the aim of protecting their constituencies and assisting the community with the management of cybersecurity risks.

Policy makers are increasingly interested in reliable, trustworthy information about current and historical cybersecurity trends and the effectiveness of digital security risk management measures ("security measures"). Due to CSIRTs' unique role in the digital ecosystem, there is mounting interest in CSIRT-produced statistics to inform policy making in the area of cybersecurity.

Many CSIRTs already generate statistics based on their daily activities. These statistics are focused primarily on incidents and their mitigation. CSIRTs may also collect data or potentially have access to data that could be used to generate statistics on other relevant aspects of cybersecurity. However, such statistics is rarely comparable across national contexts, which is a limitation to their use for better informing policy making processes. Enhancing the quality and international comparability of these existing and potentially new statistics raises many challenges, which this guidance seeks to address.

This document explores a broad range of areas for cybersecurity statistics before focusing on two aspects for which better measurement and the ability to compare statistics could inform policy making: *i)* CSIRT capacity and resourcing to effectively mitigate security incidents and *ii)* the security incidents that CSIRTs handle. It develops policy and operational guidance for improving statistics related to both components.

Statistical indicators are specifically developed for CSIRT capacity: CSIRT budget, skills, personnel and formal co-operation. All incident response teams, no matter their size or maturity, will possess data required for these statistics, thus making them more suitable for international comparison.

The guidance explains a number of conceptual, methodological, practical and technological challenges facing CSIRTs in the creation of comparable statistics on incidents, and makes suggestions on how to address these challenges. This is an area that will require ongoing co-operation among CSIRTs, as well as among the incident response, statistical and policy communities.

The document also discusses various ways of normalising incident-related statistics to account for differences in network size, before concluding with final reflections regarding the dissemination and adoption of the guidance.

SECTION 1: BACKGROUND, OBJECTIVES & SCOPE OF THE GUIDANCE

Introduction

While definitions of "cybersecurity" vary, one way of understanding the concept is in terms of the management of digital security[1] risk. Such risk is the effect on economic and social objectives of the uncertainty related to activities in the digital environment. This risk results from intentional or unintentional threats exploiting vulnerabilities and causing incidents, which disrupt the confidentiality, availability and/or integrity of the data, systems, networks and activities relying on the digital environment. Cybersecurity risk management is therefore about assessing and treating this risk.

Thus threats, vulnerabilities and incidents are risk factors, i.e. causes that influence risk. When they multiply, digital security risk increases. Policy makers are more and more focusing their attention on cybersecurity risk and the development of appropriate risk management policies and frameworks. The 2012 OECD report on *Cybersecurity Policy Making at a Turning Point* found that cybersecurity is becoming a national policy priority for many countries/economies. The analysis revealed a "fundamental evolution in government policy making whereby cybersecurity is elevated among government priorities" (2012a: 17).

Evidence base for cybersecurity policy making

Effective policy making requires sound evidence. A solid evidence base helps policy makers to *i)* identify where policy interventions are warranted, *ii)* design better policies while limiting unintended consequences and *iii)* assess the effectiveness, benefits and costs of existing and proposed policies (OECD 2012b: 8).

In the area of cybersecurity policy making there is a wide range of existing data, statistics and statistical indicators, which are mainly qualitative in nature. The 2012 OECD report on *Improving the Evidence Base for Information Security and Privacy Policies* surveyed this landscape, noting the strengths and weaknesses of each source of data or statistics. It also identified an opportunity to work with Computer Security Incident Response Teams (CSIRTs) to improve the international comparability of the statistics they produce. By virtue of their unique position in the cybersecurity ecosystem, CSIRTs are widely considered a highly trustworthy source of data.

Incident response

Incident response is a fundamental part of cybersecurity risk management. Recognising this fact, the 2002 *OECD Guidelines for the Security of Information Systems and Networks* ("Security Guidelines") include a Response principle: "Recognising the interconnectivity of information systems and networks and the potential for rapid and widespread damage, participants should act in a timely and co-operative manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective co-operation to prevent, detect and respond to security incidents. Where permissible, this may involve cross-border information sharing and co-operation."[2]

1 . This document uses the expressions "digital security risk" and "cybersecurity risk" interchangeably.

2 . The OECD Security Guidelines are currently being revised. This revision is expected to be finalised in 2015.

CSIRTs institutionalise incident response. These teams perform, co-ordinate and support the response to security incidents within a defined constituency. Policy makers are increasingly recognising the essential role that CSIRTs play in facilitating information sharing and international cybersecurity co-operation. As a result, various international and regional bodies have called on their members to establish CSIRTs, including the African Union[3] and European Union[4]; while others like the Organization of American States (2004) and United Nations *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*[5] have recommended increased interaction and collaboration among security incident response teams.

International co-operation

The Response principle of the OECD Security Guidelines emphasises the co-operative nature of security incident response and the need for international co-operation in many instances. The spirit of this principle is reflected in numerous high-level policy statements and commitments at national, regional and international levels. For example, the United States *International Strategy for Cyberspace*[6], the Association of Southeast Asian Nations (ASEAN) Regional Forum 2006 *Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space* and the International Telecommunication Union *Resolution 130*[7], all emphasise the importance of international co-operation in incident response.

In 2013, the UN *Group of Governmental Experts* recommended enhanced information sharing and co-operation in security incident response as a confidence building measure: "Enhanced sharing of information among States on ICT security incidents, involving the more effective use of existing channels or the development of appropriate new channels and mechanisms to receive, collect, analyse and share information related to ICT incidents, for timely response, recovery and mitigation actions. States should consider exchanging information on national points of contact, in order to expand and improve existing channels of communication for crisis management, and supporting the development of early warning mechanisms" (GGE, 2013: 9).

Role of CSIRTs in improving the evidence base

With this increased recognition of the essential role that CSIRTs play in cybersecurity risk management comes increased expectations about the extent of their responsibilities, particularly from policy makers whose appetite for reliable, trustworthy information about current and historical trends and

3. "State Parties shall encourage the establishment of institutions that exchange information on cyber threats and vulnerability assessment such as the Computer Emergency Response Team (CERT) or the Computer Security Incident Response Teams (CSIRTs)" (AU, 2014: 29)

4. "Each Member State shall set up a Computer Emergency Response Team (hereinafter: "CERT") responsible for handling incidents and risks according to a well-defined process…" (EU, 2013: 21)

5. "States should consider the development of practical confidence-building measures to help increase transparency, predictability and cooperation, including… exchanges of information and communication between national Computer Emergency Response Teams (CERTs) bilaterally, within CERT communities, and in other forums, to support dialogue at political and policy levels." (GGE, 2013: 9)

6. "No one nation can have full insight into the world's networks; we have an obligation to share our insights about our own networks and collaborate with others when events might threaten us all. As we continue to build and enhance our own response capabilities, we will work with other countries to expand the international networks that support greater global situational awareness and incident response—including between government and industry." (White House, 2011: 19)

7. "…coordinated national, regional and international action is required for prevention, preparation, response and recovery from computer security incidents…" (ITU, 2010: 1)

the effectiveness of measures is growing. There is mounting interest in CSIRT statistics among policy makers, but it is important that such statistics are of sufficiently high quality and internationally comparable if they are to inform decision making. Along these lines, the 2014 Internet Governance Forum (IGF) Best Practice Forum on Establishing and Supporting CSIRTs for Internet Security emphasised, as one of the unresolved issues where further multistakeholder co-operation is needed, that "the CSIRT community needs to continue working with policy makers and the statistical community to improve the quality and international comparability" of their statistics (2014: 16).

The 2012 OECD report on *Improving the Evidence Base for Information Security and Privacy Policies* found that many CSIRTs already generate statistics based on their daily activities, particularly statistics on the number of incidents handled. Such statistics are usually published in quarterly or annual reports. They may also be shared with other CSIRTs at organised events.

CSIRTs also collect data or potentially have access to data that could be used to generate statistics on other relevant phenomena. However, ensuring the quality and international comparability of these statistics raises many challenges, which this guidance seeks to address.

Factors influencing the scope of the guidance

Cybersecurity risk management is a complex area. Organising the measurement of such complexity is extremely challenging. This guidance approaches this challenge by placing national CSIRTs at the locus of measurement. The decision to focus on CSIRTs, their activities and what they can measure has both positive and negative implications.

It would be useful if CSIRTs could generate robust statistics on all dimensions of cybersecurity risk management, but this is not possible. For one, there are practical barriers that prevent CSIRTs from being able to collect and interpret all the desirable existing data. Considering the longer-term objective of comprehensively measuring cybersecurity risks, this guidance addresses only a subset of that effort. It is important to understand the kinds of data that are at the disposal of CSIRTs and whether and how these data can be used to inform policy making.

Dimensions of cybersecurity risk management

Taking a broad view, five dimensions of cybersecurity risk management were explored over the course of the project.[8] In general terms, the relevant policy questions for these dimensions can be described as follows:

- *Capacity*: The ability to manage and mitigate cybersecurity risk. There are different levels to consider: What is a country/economy's overall level of cybersecurity capacity? What is the capacity of the national CSIRT to fulfil its mission? What can policy makers and other stakeholders do to increase capacity?

- *Risk conditions*: What threats and weaknesses exist in the digital environment that can be exploited to increase security risk both within and outside the digital environment? What is the relative severity of different risk conditions? What security measures are effective at reducing digital security risk?

8 . See *Improving the Evidence Base for Information Security and Privacy Policies* (2012: 13-14) for a broader analytical framework for classifying risk-related data and statistics.

- *Incidents*: What security incidents afflict a country/economy and the organisations and users therein? What is the relative severity of different incidents? What incident response measures have proven effective in mitigating the impact of security incidents?

- *Impacts*: What are the financial, economic, social and other impacts of security incidents? How can the costs of these impacts be reduced?

- *Awareness*: What is the level of awareness of cybersecurity risks among the user population? How does awareness affect behaviour? How can awareness and/or behaviour be improved to better manage risk?

There are at least two aspects to consider along each dimension:

- What can CSIRTs measure?

- Is it of value to policy making?

There are some aspects of cybersecurity risk management that CSIRTs can measure easily and publish statistics on, but which may provide little value to policy making. Conversely, statistics related to other aspects of cybersecurity risk management may be very valuable from a policy perspective, but are phenomena for which CSIRTs lack access to good data.

Take the dimension of risk conditions, for example. CSIRTs have access to data on the number of alerts, warnings and advisories issued to constituents during a certain period. As CERT/CC explains: "This service involves disseminating information that describes an intruder attack, security vulnerability, intrusion alert, computer virus, or hoax, and providing any short-term recommended course of action for dealing with the resulting problem. The alert, warning, or advisory is sent as a reaction to the current problem to notify constituents of the activity and to provide guidance for protecting their systems or recovering any systems that were affected. Information may be created by the CSIRT or may be redistributed from vendors, other CSIRTs or security experts, or other parts of the constituency."[9] This is an important service and CSIRTs could publish statistics based on these data. However, these statistics would have limited value. For one, a simple count of the number of alerts, warnings and advisories issued to constituents would not convey information about the relative severity of the potential attack, vulnerability, etc. Nor would these statistics indicate how many constituents actually acted on this information.

There may be other ways of approximating the level of risk in the digital environment. However, the data needed to produce these statistics are often not immediately available to CSIRTs, as the data are usually held by third parties (i.e. not CSIRTs or their constituents). Thus, while it is recognised that there would be tremendous value in developing statistical indicators of risk conditions, it does not appear that CSIRTs are currently well-positioned or well-equipped to collect and interpret the relevant data.

It would also be highly useful to develop statistical indicators of the impacts of security incidents, especially for the purposes of informing policy making in this area. However, there is no indication that CSIRTs have direct access to the type of data from the impacted organisations that could inform statistics on the impacts of the security incidents they handle.

1. Likewise, governments widely recognise the importance of user education, skills development and awareness raising in improving overall cybersecurity risk management (OECD, 2002). However, not

9 . www.cert.org/incident-management/services.cfm?#alerts

every CSIRT engages in these activities. In some cases, the activities may be handled by the CSIRT's sponsor or other parts of the government (e.g. the ministries of communications or education). Therefore, reporting robust statistics on these issues would require an effort that extends beyond CSIRTs.

While the development of CSIRT statistical guidance on measuring risk conditions, impacts and awareness is currently out of scope, future work to develop the evidence base for cybersecurity policy making could explore how best to measure and develop internationally comparable statistics on these important dimensions.

Scope of the guidance

This guidance therefore mainly focuses on two dimensions of cybersecurity risk management that lend themselves to CSIRT statistics: capacity (section 5) and incidents (section 6).

The document also contains guidance for CSIRTs on measuring the size of networks within their constituencies in order to improve (i.e. by normalising) the statistics on capacity and incidents (section 7).

The focus of the guidance is on CSIRTs with national responsibility. Where the term "CSIRT" is used in this guidance, it refers to CSIRTs with national responsibility unless otherwise explicitly noted. However, much of the guidance is applicable to any type of CSIRT.

Box 1. Structure of the guidance

The guidance starts with a discussion on general aspects of the work of Computer Security Incident Response Teams (CSIRTs) (section 2).

It continues with a methodological discussion on data, statistics and statistical indicators, and explains the kinds of data available to CSIRTs that could be used for statistical purposes (section 3).

A brief discussion on some of the key stakeholders for CSIRT statistics and the anticipated main uses of these statistics follows (section 4).

Statistical indicators for CSIRT capacity are then put forward (section 5).

This is followed by an extended discussion on the conceptual, methodological, practical and technological challenges facing CSIRTs in the creation of high-quality, internationally comparable incident-related statistics, as well as guidance on how to address these challenges (section 6).

Points on how to measure networks for statistical purposes aim to improve the normalisation of incident statistics (section 7).

Finally, the concluding section highlights outstanding concerns regarding the organisation and co-ordination of CSIRT statistics (section 8).

Because improving CSIRT statistics requires an effort by both policy makers and CSIRTs themselves, this guidance is mainly targeted at these two audiences. In particular, sections 1-4 are mainly addressed to policy makers, whereas sections 5-7 are largely aimed at CSIRTs. As section 8 addresses outstanding concerns about the organisation and co-ordination of CSIRTs' statistical efforts, it is important for both policy makers and CSIRTs. However, there is value for both policy makers and CSIRTs in all the sections.

Relationship between the guidance and other international efforts

This document provides voluntary guidance to CSIRTs on how to improve the quality and international comparability of their statistics. It does not seek to replace current standards for incident handing or information exchange.

There are several existing standardisation initiatives for incident handling and information exchange. First is the Internet Engineering Task Force's (IETF) Incident Object Description Exchange Format (IODEF) standard[10], which has been extended to facilitate the exchange of enriched cybersecurity information among security experts at organisations and to facilitate their operations.[11] Additional IETF work to improve information sharing among security incidents is ongoing in the Management Incident Lightweight Exchange (MILE) Working Group. Second is the International Telecommunication Union's (ITU) Cybersecurity Information Exchange (CYBEX) framework[12].

A third effort is a standardisation initiative being led by the United States Department of Homeland Security (DHS) and involves three specifications: the Trusted Automated eXchange of Indicator Information (TAXII), the Structured Threat Information eXpression (STIX) and the Cyber Observable eXpression (CybOX). TAXII defines a set of services and message exchanges that enable the sharing of actionable cybersecurity threat information. STIX aims to develop a standardised, structured language to represent cybersecurity threat information. CybOX is a standardised schema for specifiying, capturing, characterising and communicationg events or stateful properties that are observable in all system and network operations.[13] The OECD CSIRT statistical guidance is intended to be fully complimentary with these standards.

At least three existing taxonomies for incidents have been identified. One was developed by the Latvian CERT NIC.LV and another by TS-CERT (Telia CERT/CC), which was popularised by the European CSIRT Network (eCSIRT.net). Both of these taxonomies are explained in depth in the ENISA *Good Practice Guide for Incident Management* (2010: 58-63). A third widely known and utilised taxonomy is the incident classification scheme from National Institute of Standards and Technologies (NIST) *Computer Security Incident Handling Guide* (2012).

Increased efforts should be made by the CSIRT community to ensure the adoption of common standards and shared taxonomies for incident handling. The use of standardised definitions and incident classification schemes would do a lot to facilitate better internationally comparable statistics, specifically for incident-related statistics. In particular, newly established CSIRTs should be encouraged to adopt and use recognised standards and common taxonomies. This topic will be discussed in depth in section 6.

10 . www.ietf.org/rfc/rfc5070.txt

11 . https://tools.ietf.org/html/rfc7203

12 . www.itu.int/en/ITU-T/studygroups/com17/Pages/cybex.aspx

13 . https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

SECTION 2: ORGANISING COMPUTER SECURITY INCIDENT RESPONSE

Introduction

This section is largely intended for non-technical readers, including policy makers, who may be unfamiliar with Computer Security Incident Response Teams (CSIRTs). The operations of CSIRTs are not widely understood outside the technical community. However, CSIRTs play an important role in the environment in which people, organisations and governments operate and interact with technology. A discussion on the general aspects of the work, influence and goals of CSIRTs will enable a better understanding of the opportunities and challenges for improving relevant statistics in this area and of the kinds of decisions they support.

This section introduces the CSIRT concept, summarises the main forms of CSIRT co-operation, explains the organisation of CSIRTs with national responsibility, notes the international diversity of incident response teams and discusses the different CSIRT services and the incident handling workflow. It may be useful to countries/economies looking to develop their CSIRT capacity.

About CSIRTs

A CSIRT is an organisation that acts as a trusted point of contact for computer security incident response. Its main responsibility is to prevent, handle and mitigate computer security incidents with the aim of protecting its constituency – which refers to a CSIRT's customer base – and assisting the community with the management of cybersecurity risks. A CSIRT may provide a range of services to its constituents, such as issuing alerts and advisories on current and impending computer-related threats or collecting and gathering data to analyse incidents in order to provide constituents with solutions and response actions to reduce risks and minimise the expected damage. CSIRTs may also issue advisories on vulnerabilities and malware in the software and hardware running on their constituents' systems. Thereafter, constituents may promptly patch or update their systems to prevent infection or further damage.

The size of a CSIRT's constituency will vary. A CSIRT with national responsibility usually has nationwide coverage and co-ordinates with international partners where necessary, regardless of whether its own constituency is limited to the private or public sector. Some CSIRTs with national responsibility will have organisations from both the private and public sectors in their constituency. Some CSIRTs are based within enterprises, which are its sole constituency. In some cases, however, they may be extended beyond the enterprise. For example, several academic CSIRTs began their role with a general research purpose and to protect the domain of academia, but this remit was later expanded to include other domains, in some cases even extending to a national scope.

There are many historical variations of the term used to describe the entities responsible for the work of CSIRTs. The following abbreviations are currently used and there may be new variants in future. Despite the variations in name, the purpose of the entities designed for computer incident handling and mitigation has remained fairly constant.

- CERT© or CERT/CC (Computer Emergency Response Team/Coordination Centre)
- CERT (Computer Emergency Readiness Team)
- CSIRT (Computer Security Incident Response Team)

- CIRT (Computer Incident Response Team)
- SIRT (Security Incident Response Team)

Today, the term "CSIRT" is used more widely than "CERT". However, in practice the terms are used synonymously.

Co-operation among CSIRTs

There are different models of CSIRT organisation and internal interaction, as well as different models of co-operation among CSIRTs. The most common forms of co-operation include *i)* bilateral co-operation between CSIRTs, *ii)* associations comprised of multiple CSIRTs with common interests and goals and *iii)* co-operation among associations (ENISA, 2006: 10-11).

- Bilateral CSIRT co-operation is between two teams and is based on trust between the teams and/or their members. This model of co-operation is often stimulated by shared goals. Bilateral partners sometimes choose to formalise their relationship through a written agreement but such an agreement is not required for co-operation (ENISA, 2006: 10).
- Association frameworks may be set by a common geographical area, common sets of services, similar constituencies, sectors of operation, and so forth, and may go by different names: forum, task force, coalition, etc. Associations provide a long-term co-operation between interested parties, which benefits the building of trust (ENISA, 2006: 10-11).
- Co-operation among associations is based on the common goals of the organisations and is frequently realised through the exchange of experiences in security incident response (ENISA, 2006: 11).

CSIRTs with national responsibility

National CSIRTs have responsibility over a country or economy and can be found in most advanced and developing countries/economies. Their constituencies may include all networks in the country/economy, the general public, government networks, critical infrastructure or a combination thereof. According to CERT/CC, which hosts the annual meeting of national CSIRTs, at the time of writing there were 99 CSIRTs with national responsibility representing 88 countries/economies as well as the European Union.[14]

Generally speaking, it may be possible to classify national CSIRT constituencies as follows: *i*) national CSIRTs with responsibility for all sectors in a country/economy, *ii*) those that are responsible for all networks in a country/economy except those owned/operated by government or military, *iii*) those that are responsible only for networks in the public sector, government and/or critical infrastructure, and *iv*) those responsible for only private sector networks, particularly critical infrastructure. In practice, however, there are different varieties of national CSIRTs.

There are also a number of regional CSIRTs. These associations have been organised by CSIRTs themselves for the purpose of regional co-operation. For example, in Europe there is TF-CSIRT, a task force that promotes collaboration and co-ordination between European CSIRTs. The Asia-Pacific region has the Asia Pacific Computer Emergency Team (APCERT), which was inaugurated in 2003 for closer relationships and timely international incident handling among Asia-Pacific economies. The Forum of

14 . https://www.cert.org/incident-management/national-csirts/national-csirts.cfm

Incident Response and Security Teams (FIRST) is the only global organisation, which as of November 2014 had more than 309 member teams across 67 countries.

It is important to stress the diversity that characterises CSIRTs. Every CSIRT has its own mission, objectives, constituency and position within its organisation or country/economy, as well as historically shaped relationships with key partners and stakeholders such as Internet service providers. Likewise, every CSIRT has its own service types and definitions, policies and operational procedures.

A new CSIRT is likely to follow an existing model, often by adopting structures and activities that other, more advanced CSIRTs already have in place. However, a new CSIRT may soon realise that customisation is necessary, reflecting factors such as budget and human resources, technical capabilities, and so on. Still, despite these organisational differences, security incident handling and response are core to a CSIRT's tasks. Any organisation offering these core services can be considered a CSIRT.[15]

CSIRT services

CSIRT services can be categorised into two main types: reactive and proactive services.[16] Reactive services are tasks initially triggered by external events, for example reports originating from a source outside the CSIRT regarding compromised hosts, denial of service attacks, intrusions or attempted intrusions, phishing campaigns, web defacements, software and hardware vulnerabilities, etc. These services are generally regarded as a set of core services that a CSIRT facilitates as part of its basic functions. With these services operational, a CSIRT acts when notified, and then responds to mitigate incidents.

Proactive services include alerts and warnings on recent and impending cyber threats, intrusion detection services, security assessments, security tools development, setup and management of security tools and applications, etc. These services involve tasks that can be offered only when a CSIRT has determined that it has enough capacity and capability to do so. The introduction of such services often requires additional funding and resources. CSIRT service expansion is a proactive measure that enables cybersecurity risk management to follow technological innovation: as the threats evolve, so do the possible countermeasures.

As previously mentioned, the *raison d'être* of CSIRTs is incident handling and response. Therefore, to develop more comparable statistics across CSIRTs, it is necessary to understand the general workflow involved in incident handling.

Incident handling workflow

There are broadly four phases in a CSIRT's incident handling workflow.[17] The first phase involves receiving and assessing information about the incident, often referred to as the triage function. This is a step for information gathering and prioritising the incident that has been reported, requested or detected. CSIRTs often automate some of the steps in this function. A CSIRT will usually have a single point of

15 . CSIRTs may offer more services, including for example incident analysis, incident response co-ordination, detection and mitigation services, resolution and technical support, education, awareness-raising, etc.

16 . There may be more categories if the CSIRT's framework is based on extended capacity and it is determined to provide other services; for example, risk analysis, business continuity planning or disaster recovery planning, security consulting, evaluation, certification, etc.

17 . There may be more or fewer steps in the incident handling service, depending on the type of CSIRT, its characteristics, mission objectives, strategies, scale and funding.

contact to maintain efficient information collection processes and to avoid any conflicts possibly caused by multiple sources of input.

The second phase involves handling the incident. This step is the most time-consuming and resource-intensive. It can be divided into three or more sub-phases. The incident handling phase generally involves *i*) identifying and acquiring the necessary information to pass on the incident for analysis (where necessary), *ii*) the analysis itself, which may involve a computer or network forensics function, and *iii*) working with relevant stakeholders involved in the incident, which may include, for example, notifying, advising or instructing the compromised websites and their administrators, relevant Internet service providers, hosting companies of the affected websites, etc. In this phase, de-escalation or escalation activities may take place when *i*) the incident does not affect the CSIRT's own constituency, *ii*) CSIRTs use external resources and request help or seek co-operation from other parties on mitigation activities or *iii*) help or guidance is required by law enforcement entities. For efficient mitigation, a CSIRT tries to limit further damage resulting from the incident, i.e. containing or deterring the source of the presumed malicious activity, for which different methodologies may be used (including network, hardware or software approaches).

The third phase involves notifying the constituency about the threat or incident. This may be optional depending on the CSIRT's assessment, which is based on the results of the incident analysis, information received about potential hardware or software vulnerabilities, the status of the malware infection, how fast it can propagate and at what scale, the percentage of unpatched systems potentially affected by a particular malware or vulnerability, and so on.

The last phase involves removal and recovery, as well as a feedback function. Removal and recovery refer to restoring systems and data to a more secure, non-vulnerable or original state. This step may be optional. However, for a CSIRT with national responsibility or sufficient capability, it is an important function. Feedback is often treated as an extended CSIRT function, but for efficient mitigation it is recommended to communicate with relevant parties following an incident. Feedback is often driven or requested by external entities, such as media, government, etc., and can require significant time and resources, especially if a CSIRT has less capacity or weak partnerships with relevant stakeholders.

It is important to note that that after receipt of initial information about an incident, all other phases of activity may occur more or less in parallel, not necessarily sequentially one after the other.

SECTION 3: UNDERSTANDING CSIRT DATA, STATISTICS & STATISTICAL INDICATORS

Introduction

This section discusses, in general terms, what makes good data for statistics and the criteria for constructing robust statistical indicators[18]. It also explains the kinds of data available to CSIRTs that could be used for statistical purposes.

Distinguishing data, statistics and statistical indicators

Data, statistics and statistical indicators are three different concepts. For the current discussion, data can be understood as numerical information. CSIRTs' daily flow of activities generates large amounts of this information. To be useful, data must be organised, evaluated and analysed. This is the purpose of statistics. For example, data can be summed or averaged to provide a single measure (i.e. a statistic).

Statistics become statistical indicators when they can suggest the characteristics of a subject under scrutiny. Statistical indicators typically reflect some underlying theory associated with the subject to be measured, such as the distribution (e.g. normal or not) of its underlying population. As such, the theory is an explanation of relationships between phenomena.

For example, data from unemployment registers and labour force surveys are used to create statistics on the total number of unemployed workers and the total labour force. The unemployment rate is an economic indicator defined as a ratio between these two statistics because the theory suggests that the labour force is the relevant reference. Another theory could use another statistic such as the total number in the working-age population or total population, leading to another statistical indicator (OECD, 2012b).

In some cases, depending on the nature of the data, simple computation can provide statistical series that are sufficient to form a useful indicator on their own to inform policy making. However, in many cases the combination of different statistics will be necessary to create useful indicators.

It is possible to define criteria for constructing and selecting statistical indicators depending on whether they apply to policy, analytical soundness or measurability. Criteria may also be assessed in relation to factors such as transparency, scientific validity, relevance, robustness, sensitivity and the extent to which statistical indicators are linkable to each other. Not all criteria will be applicable to every statistical indicator. Each measurement situation has its own priorities for data collection and analysis (von Schirnding, 2002: 47-48).

Statistical indicators should be as precise as possible to maximise their usefulness. They should also be scientifically credible, unbiased and representative of the issue concerned. Additional features of good statistical indicators are consistency and comparability; moreover, they should be relatively unaffected by minor differences in methods and measurement techniques that may occur in the various contexts and settings in which data is collected (von Schirnding, 2002:48).

18 . The term "indicator" – while commonly used in the field of statistics – has specific connotations in the CSIRT community, namely an indicator of a security incident. This guidance therefore strives to use the term "statistical indicator" to avoid misunderstandings between the statistical and technical communities.

To ensure usefulness, statistical indicators should be readily understandable to policy makers, linked to clear decision-making goals and based on data that are either readily available or relatively easy and inexpensive to collect (von Schirnding, 2002: 48).

Understanding CSIRT data

Generally speaking, there are two kinds of data readily available to CSIRTs that could be used for statistical purposes: *i)* administrative data and *ii)* technical data.

Administrative data

Administrative data concern aspects of the CSIRT organisation itself – including, for example, data on the CSIRT's budget or human resources – and can be a good source of data for internationally comparable statistics regarding capacity issues.

Technical data

Technical data are the product of the incident-handling operations of CSIRTs as well as the activities of other actors in the cybersecurity ecosystem.

A further breakdown of the technical data that can be accessed by CSIRTs is possible: *i*) data that is generated by CSIRTs during the incident-handling process and *ii*) data collected from external sources that do not directly come from incident handling. It is important to understand the difference between the two and, in particular, the relevance for statistics.

- CSIRT-generated incident-related data: These are data that CSIRTs produce as part of the incident-handling process. These data may come from incident reports by constituents or may be shared by other CSIRTs. They may also come from internal sources (e.g. the CSIRT's own darknets, honeypots, spam traps, etc.). Importantly, these are data that any CSIRT will possess by virtue of being a CSIRT.

- External technical data: In addition to the data they generate through incident handling, CSIRTs may also collect or be able to access technical data from third-party organisations, i.e. not their constituents or other CSIRTs. These data come from sources such as anti-virus software providers or data providers specialising in cybersecurity research and analysis. Importantly, these data are not systematically incorporated into the incident-handing process. CSIRTs may use these data for different reasons, including to better understand the threat environment, to assess cybersecurity risk trends, etc. Many CSIRTs do not use these data in their work, especially less mature teams.

Where teams do rely on external data providers in their work, they do not always combine these data with the data generated through the incident handling process to produce incident statistics.

Those CSIRTs that do bring together internal and external data for statistical purposes face various challenges in doing so. These challenges include uncertainty regarding the original sources of the data (i.e. questions of provenance), the potential for double counting (data may appear in other feeds they receive, which would skew the statistics) and the need for complex methodologies to combine data from potentially disparate sources. There is a need for better technical guidance and basic, accessible research in this area.

While this document cannot resolve all of these challenges, it can guide CSIRTs on how best to organise the measurement of incidents to produce better internationally comparable statistics. Section 6 addresses these issues.

This project has strived to identify statistical indicators for which most, if not all, CSIRTs – no matter their size or maturity – should be capable of collecting data and producing statistics. To that end, the next section focuses on the key stakeholders and main uses of CSIRT statistics before turning to section 5, on the measurement of CSIRT capacity.

SECTION 4: KEY STAKEHOLDERS & MAIN USES OF CSIRT STATISTICS

Introduction

While there is a wide range of issues relating to cybersecurity risk management and incident response that are of concern to different stakeholder groups, as was noted in the introduction, CSIRT statistics cannot address all these issues. CSIRT statistics are limited in scope due to the nature of the work of institutionalised incident response. As discussed in the previous section, CSIRTs generally have access to data concerning the administration of the CSIRT organisation and incidents handled.

Moreover, the reality is that CSIRTs do not currently view the production of statistics as a core part of their mission. Teams are understandably more concerned with responding to incidents, thereby giving statistics a lesser priority. With that said, however, CSIRTs are increasingly recognising the need to show that they are accomplishing their mission and the role that statistics can play in demonstrating progress.

This section outlines some of the key stakeholders for CSIRT statistics and the anticipated main uses of these statistics. This discussion is not intended to be exhaustive, but aims rather to document some of the current uses of CSIRT statistics and to illustrate certain other possibilities.

Key stakeholders

CSIRT statistics will serve different purposes depending on the user. It is possible to organise those with a stake in CSIRT statistics into two main groups: *i)* stakeholders internal to the CSIRT community and *ii)* those external to the community.

Internal stakeholders

CSIRT management: the statistics produced by CSIRTs will be of immediate interest to the organisation's management. Statistics help to keep management informed of the team's activities, to analyse trends and to set priorities. They may also help to better organise the work of CSIRTs. For example, comparative statistics on levels of technical skills across CSIRTs may help to inform management decisions regarding new hires. Moreover, statistics may also help CSIRTs justify budget and requests for increased budget.

Other CSIRTs: CSIRT statistics may also prove useful to teams seeking to better understand the threats that other teams are facing, particularly if they can be confident that others are categorising incidents in comparable ways.

External stakeholders

Policy makers: If their quality can be assured, CSIRT statistics may also be helpful for informing policy making in the area of cybersecurity risk management. For example, comparative statistics regarding CSIRT budget may help policy makers allocate financial resources for incident response. Comprehensive statistics on the incidents affecting national constituencies may also be informative to policy making.

Global and regional development organisations: CSIRT statistics may help to inform cybersecurity global and regional capacity-building efforts.

Technical community: Organisations engaged in digital security risk management, including the technical community, would benefit from robust CSIRT statistics to inform, supplement and normalise

their own statistics and activities. In addition to informing the technical community's risk statistics, robust CSIRT statistics could also support standards development and related efforts.

Business community: Technology vendors and cybersecurity service providers can use CSIRT statistics to help ensure they are addressing the right problems. Other business actors can use CSIRT statistics to better understand cybersecurity risks level in different markets.

Academic and research communities: Academic and research organisations may also benefit from the public availability of internationally comparable statistics in the area of cybersecurity incident response.

The public: Last but not least, CSIRT statistics are a means of communicating with the public regarding trends in cybersecurity risk. The effective use of statistics can help to raise public awareness about cybersecurity threats. Statistics may also help those CSIRTs that are funded by taxpayers to fulfil reporting obligations.

SECTION 5: MEASURING CSIRT CAPACITY

Introduction

CSIRTs are often described as the fire brigades of the Internet – they are the first to react when security incidents occur online. In the offline world, decision makers as well as members of the public want to be able to access information on the resourcing of fire brigades and how well they manage and mitigate fire-related risks. Likewise, from a cybersecurity risk management perspective, there is utility in measuring the capacity of CSIRTs. CSIRT capacity can be broadly defined as the organisational capacity and resourcing to effectively mitigate security incidents. The measurement of CSIRT capacity provides an obvious starting point for the improvement of CSIRT statistics.

The data required for statistics about CSIRT capacity should be possessed by all teams, no matter their size or maturity. It is envisaged that a senior manager with access to data on administrative matters is best suited to provide data for the statistical indicators presented below.

The statistical indicators developed with experts pertaining to CSIRT capacity include annual budget, personnel, skills and formal co-operation. The feasibility study showed that these are statistical indicators for which CSIRTs can most reliably report comparable statistics. A discussion on the statistical indicators that were tested in the feasibility study but ultimately excluded in this guidance can be found at the end of the section.

Budget

The first statistical indicator related to CSIRT capacity is concerned with the CSIRT's annual budget. The objective of this indicator is to provide an economic measure of a government's priority to fund efforts to protect against security threats and to respond to security incidents. It assumes that greater CSIRT funding by government denotes greater policy priority.

Definition: Annual CSIRT budget as a percentage of overall annual government budget

All CSIRTs have data on their budget. However, many do not currently publish it. Generating statistics for this indicator would require CSIRTs to report their budget data. CSIRTs should strive to report data for the calendar year (i.e. January-December), where possible.

For this statistical indicator, CSIRTs should report:

- Their annual budget (in the local currency), which should include all expenditure for the year, including technology investments;
- The percentage of their budget funded by government;
- The overall annual government expenditure (also in the local currency) for the corresponding year, if it is known.[19]

19 . If the CSIRT does not know this figure, it may be available from third-party databases; in particular, aggregate government expenditure data according to Classification of the Functions of Government (COFOG) can be found in table 3.1 of the UN National Accounts: http://data.un.org/Explorer.aspx?d=SNA

In some cases, a CSIRT may not be allowed to publish the exact budget figure because it is included within the country's overall intelligence/defence budget. This may particularly be a concern for government CSIRTs that have been designated as national CSIRTs. These CSIRTs could instead report a best estimate.

In cases in which the responding CSIRT is not primarily or entirely funded by government, it may be necessary to reflect this fact when reporting the statistics, and adjust the normalisation accordingly.

This statistical indicator could be combined with other statistics (e.g. those related to particular incidents) to provide an indication regarding the adequacy of financial resources to mitigate risks, however further research may be required to gauge the efficacy of doing so.

As noted in section 1, the immediate scope of application of this statistical guidance is CSIRTs with national responsibility. In several countries/economies, there are multiple national CSIRTs in operation, usually with different constituencies. These teams very often do not co-operate to produce statistics. However, more complete national statistics would require increased co-operation between CSIRTs. If there are multiple national CSIRTs operating in a country/economy, it may be necessary for these teams to co-operate to combine their budget figures in order to report national statistics.

Future iterations of this guidance could explore how to break down the statistical indicator further along specific budget line items common to all CSIRTs (e.g. proactive services such as alerts and warnings, reactive services like incident response, staff costs, technology spend, etc.).

Personnel

The second statistical indicator related to capacity is concerned with CSIRT personnel. The objective of this indicator is to provide an organisational measure of a CSIRT – namely its human resources focused on security incident handling – as a percentage of the number of Internet users it serves at a national level.

Definition: Number of full-time equivalents (FTEs) employed for security incident handling and directly related tasks at the CSIRT per 100,000 Internet users in the country

All CSIRTs will have data on staff numbers, however some may not currently publish this data. Respondents will need to make a determination as regards the roles of CSIRT staff members.

For this statistical indicator, CSIRTs should report:

- The total number of FTEs employed by the CSIRT as of December 31st of the reporting year;
- The number of those FTEs who were employed for security incident handling and directly related tasks (i.e. excluding administrative and other support functions such as human resources, finance, etc.);
- The number of Internet users in the country (see section 7 for more information on these data).

According to Eurostat[20], a full-time equivalent is a unit to measure employed persons in a way that makes them comparable although they may work a different number of hours per week. The unit is obtained by comparing an employee's average number of hours worked to the average number of hours of a full-time worker. A full-time person is therefore counted as one FTE, while a part-time worker gets a

20 . http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Glossary:Full-time_equivalent

score in proportion to the hours he or she works. For example, a part-time worker employed for 20 hours a week where full-time work consists of 40 hours, is counted as 0.5 FTE. The workforce of an enterprise, activity, or country etc. can then be added up and expressed as the number of full-time equivalents.

"Security incident handling and directly related tasks" refers to technical work aimed at treating and mitigating security incidents as well as other technical tasks that directly assist the work of incident handling.[21]

In some cases, a CSIRT may be based within a larger parent organisation that handles most, if not all, of the administrative tasks for the team. These differing organisational structures should be accounted for in the statistics, for example by noting if these administrative and/or support functions are based in-house (i.e. within the CSIRT) or not.

This statistical indicator could be combined with other statistics (e.g. those related to particular incidents) to show the adequacy of a CSIRT's human resources to mitigate risks.

In future, this statistical indicator could be expanded by measuring personnel engaged in other important non-administrative tasks, such as awareness raising, educational activities, international collaboration, etc., particularly as CSIRTs continue to mature and take on more responsibilities and activities.

If there are multiple national CSIRTs operating in a country/economy, it may be necessary for these teams to co-operate to combine their personnel figures for security incident handling in order to report national statistics.

Skills

The third statistical indicator related to capacity is concerned with skills. Like at most other organisations, not all CSIRT personnel do the same kinds of work. Some CSIRT employees possess specific skills that make their contribution to incident response and cybersecurity risk management especially valuable. This indicator intends to add sophistication to the statistics on personnel by ascertaining what percentage of staff possesses advanced technical skills, which are essential to effective security incident response.

Definition: Number of positions for security incident handling and directly related tasks *requiring advanced technical skills* as a percentage of the total CSIRT workforce.

The data required for this statistical indicator could be generated by a member of management within the CSIRT organisation.

For this statistical indicator, CSIRTs should report:

- The total number of positions for security incident handling and directly related tasks *requiring advanced technical skills*, as of December 31st of the reporting year.

21 . It is acknowledged that the term "security/incident handling", as it is used in this paper, is quite broad. As this guidance and these statistics are further refined, it may be worthwhile to break down the term further to explain the specific skills/services that encompass it.

As above, "security incident handling and directly related tasks" is defined as technical work aimed at treating and mitigating security incidents as well as other technical tasks that directly assist the work of incident handling.

Advanced technical skills are defined as skills and experience equivalent to an advanced university degree (masters or doctorate) in computer science, computer security or a similar technical subject, or 5 years or more[22] of relevant technical/operational experience.[23]

Indicia of technical skills include, but are not limited to, advanced knowledge of TCP/IP and experience in system administration, penetration testing, forensic analysis and vulnerability management.

Statistics for this indicator naturally link with CSIRT personnel statistics to arrive at statistics on technically skilled employees.

If there are multiple national CSIRTs operating in a country/economy, it may be necessary for these teams to co-operate to combine their figures regarding advanced technical skills in order to report national statistics.

Formal co-operation

The fourth statistical indicator related to capacity is concerned with co-operation between CSIRTs and partners. In particular, data sharing is a core component of what CSIRTs do, especially with other CSIRTs (as discussed above in section 2) when incidents have cross-border impacts. As ENISA notes, "the motivation for formalising co-operation may be the involvement of funds, fulfilling legal requirements or the exchange of sensitive data" (2006:11). This statistical indicator therefore provides insights into a CSIRT's capacity to work co-operatively with its partners by quantifying formalised data-sharing agreements.

Definition: Number of distinct entities with which the CSIRT actively shares data on a formal basis.

For this statistical indicator, the CSIRT should report:

- The total number of organisations with which it had a formal data-sharing agreement in place as of December 31st of the reporting year;
- The figure should exclude inactive relationships, i.e. entities with which a formal data-sharing relationship is in place but with which no data was shared during the reporting year;
- Where possible, CSIRTs should provide a breakdown according to the types of organisations with which they share data (see below).

According to the definition, formal agreements would include non-disclosure agreements, contracts, memoranda of understanding or comparable instruments that facilitate data sharing. In some cases, a

22 . Five years or more was selected as the criterion based on the United States Bureau of Labor Statistics Definitions for the Education and Training Classification System: www.bls.gov/emp/ep_education_tech.htm

23 . During the feasibility study, CSIRTs were asked to comment on what level(s) of IT security certification would be equivalent to "advanced technical skills", if any. Their responses were inconclusive. Future work to further develop this statistical indicator could re-explore whether certain IT security certifications qualify.

CSIRT's data-sharing relationships with partners may be mandated by regulation or treaty. Entities falling within such arrangements would be included in the statistics.

Typical entities with which CSIRTs share data include:

- Internet Service Providers (ISPs);
- Domestic private sector CSIRTs;
- Domestic public sector CSIRTs;
- Domain name registrars;
- Registries;
- Hosting service providers;
- Anti-virus software vendors;
- Law-enforcement agencies;
- Intelligence agencies
- National CSIRTs from other countries/economies; and
- Regional/international CSIRT forums.

Where a single regulation or legal requirement mandates data-sharing arrangements with multiple entities (e.g. all ISPs in a country/economy), each of these entities should be counted as long as the data-sharing relationship is active.

Respondents should exclude their primary constituents from the figures they report.

If properly documented, data on the number of formalised relationships with partners should be readily attainable and reportable. CSIRTs may maintain a database with information on the entities with which it engages, which would facilitate the reporting of data for this indicator.

This statistical indicator could be broadened to include both formal *and* informal data-sharing relationships with partners. Informal arrangements are based on personal or working relationships, for example. Objectively measuring the number of informal relationships, however, can be challenging. A distinction was made between formal and informal data sharing in the feasibility study in recognition of the fact that many important CSIRT relationships have not been formalised by written agreement. However, the responses were highly variable and hard to compare, so it was decided to exclude these from the guidance. In future, it may be worthwhile to return to the development of a statistical indicator for more informal forms of co-operation.

Excluded statistical indicators

A number of other statistical indicators were tested in the feasibility study but have been left out of this guidance. An "automation" indicator was tested to explore whether there might be a way to measure the automation of incident response as a component of CSIRT capacity. Greater automation is generally

assumed to improve CSIRT capacity. However, the responses received from CSIRTs were highly variable, and it does not appear that an indicator for automation could be defined precisely enough to elicit comparable statistics. Moreover, the degree of CSIRT automation will depend on the kind of incident that is being processed. More significant (i.e. severe) incidents may require more human interaction, and the complex nature of these incidents means that they are not always amenable to automation.

A second excluded indicator regards "requests for assistance" from constituents. The assumption was that requests from constituents for CSIRT assistance could be an indicator of constituent trust in the CSIRT and its ability to effectively help mitigate security incidents. In addition, understanding how frequently a CSIRT acts on a request for assistance could indicate CSIRT responsiveness. However, many respondents were unable to provide data for this indicator. Several do not distinguish the concept of "incident" from "request for assistance" in their ticketing and tracking systems.

A third excluded indicator regards the frequency with which CSIRTs proactively share incident information with specific constituents (i.e. "targeted mitigation"). In their responses to the feasibility study, CSIRTs were asked to include only instances in which the organisation proactively and specifically contacted a constituent regarding an incident, which would exclude general information distributed or posted through normal channels such as on a website or social media feed. As with statistics on requests for assistance, it was found that many CSIRTs do not precisely track instances of targeted mitigation. Some CSIRTs rely on automated systems for targeted mitigation, which can bias these statistics as the systems send information on a repeated basis until the problem is resolved.

Future work to further develop and refine statistical indicators for CSIRT capacity could explore how to improve these excluded indicators, as well as others, for incorporation into a future revision of this guidance. Annex D provides a list of CSIRT statistical indicators meriting further consideration, exploration and development in the future.

SECTION 6: IMPROVING CYBERSECURITY INCIDENT STATISTICS

Introduction

A cybersecurity incident can be understood as "any real or suspected adverse event in relation to the security of computer systems or computer networks", or as an "act of violating an explicit or implied security policy".[24] Such events or acts occur regularly and it is the job of CSIRTs to respond to security incidents and mitigate them as necessary.

In doing so, CSIRTs generate large amounts of data, which can be used to produce statistics about the incidents affecting their constituencies. In fact, most CSIRTs already produce some statistics based on data about the security incidents they handle. Incident statistics are the most common kind of CSIRT statistics, and help teams to set priorities and to analyse trends in the incidents affecting their constituents. In some cases, these statistics may provide an increased capacity for situational awareness. However, there are certain limitations to the quality and international comparability of CSIRTs' incident-related statistics.

To start, the concept of "incident" is itself very broad. A basic aggregate statistic concerning the number of incidents handled by a CSIRT in a given period reveals nothing about the specific kinds of security events that were encountered, which is important information. The severity of different kinds of incidents can vary greatly. For example, the impacts of a simple website defacement are likely less severe than those of a prolonged distributed denial of service (DDoS) attack, yet both are treated the same in aggregate statistics on incidents.

To improve the value of incident statistics, it may be better to focus on specific *categories* of incidents, for example "phishing" or "malware". Many CSIRTs publish statistics along such categories. The problem, however, is that these categories also have shortcomings. For example, malware-related incidents may take on very different forms: devices infected with malware, servers propagating malware binaries[25], servers redirecting users to malware hosted elsewhere, etc. These different kinds of incidents represent different security risks to the digital environment. Unless CSIRTs capture such levels of detail about the incidents in their incident handling systems, this information may be lost in the resulting statistics.

In recognition of the need to capture and report more precise information regarding specific kinds of security events, the feasibility study sought to test whether CSIRTs could provide data for statistics on *subcategories* of incidents. In other words, instead of asking CSIRTs to provide data on the overall number of incidents handled, or even according to general incident categories such as "phishing" or "malware", the study referred to more specific aspects with narrowly crafted definitions:

- Phishing websites hosted within the CSIRT's constituency
- Denial of service attacks targeting the CSIRT's constituency
- Websites hosted within the CSIRT's constituency identified as defaced
- Servers within the CSIRT's constituency hosting malware

24 . www.cert.org/incident-management/csirt-development/csirt-faq.cfm

25 . Binary malware is an executable file, usually downloaded from the Internet, that delivers malware.

- Servers within the CSIRT's constituency directing to malware hosted elsewhere

- Servers within the CSIRT's constituency identified as botnet "command and control servers", used to co-ordinate the actions of computers infected by a bot

Despite the fact that most of the CSIRTs participating in the feasibility study were able to provide some data along the aspects listed above, upon a closer inspection of the responses it became clear that there were considerable discrepancies. That is, even though these incident subcategories were precisely defined (e.g. "phishing websites hosted within the CSIRT's constituency" as opposed to simply "phishing incidents"), most CSIRTs were unable to report accurate figures in a systematic fashion. This points to fundamental challenges regarding how CSIRTs currently collect and analyse incident data for statistical purposes, which this section seeks to address. The decision was thus taken to provide general guidance for improving CSIRT statistics in this document, and not to specify incident-related indicators. Resolving the challenges facing CSIRTs in the production of incident statistics will pave the way for statistical indicators.

This section therefore explains the current conceptual, methodological, practical and technological challenges facing CSIRTs in the creation of high-quality, internationally comparable incident-related statistics. In doing so, it offers guidance on how to address these challenges.

Conceptual challenges

There are basic conceptual challenges which, if resolved, would go some way to improving CSIRTs' capacity to produce more comparable incident statistics. First, it is often noted that the CSIRT community lacks consensus on the operational definitions of key terms fundamental to security incident response, including definitions for concepts such as "incident", "breach" or "compromise". Without a shared understanding of these terms, which are the building blocks for other aspects of security incident response, it will be difficult to collectively improve CSIRT statistics. The community should therefore work together to develop a common vocabulary of basic terms.

Second, beyond shared definitions of basic security concepts, another challenge involves the development and – more importantly – the adoption of common incident taxonomies to structure, systematise and regularise the incident handling process and, in turn, the production of incident-related statistics. While some common incident taxonomies already exist (as first noted in section 1), for historical reasons they are not universally used by CSIRTs. Those teams that have adopted existing taxonomies usually modify them in-house to reflect changes in the threat environment, which can reduce their longer-term value for organising data about incidents to produce comparable statistics.

To rectify this, a community-wide effort may be required to undertake the development of both *i)* a shared incident taxonomy to be adopted by as many CSIRTs as possible and *ii)* a process for systematically updating the taxonomy, as required, to account for important changes in the threat environment. This effort should be as open and inclusive as possible, involving a wide range of CSIRTs representing different geographic regions and sectors. While this guidance may call for such an initiative and specify some of its requirements, the effort itself must emerge from within the CSIRT community. It must also be driven by and owned by the community. A forum such as FIRST is in a strong position to facilitate such an effort.

If it is to facilitate better incident statistics, a shared incident taxonomy should satisfy a number of requirements, including but not limited to the following:

- The taxonomy should achieve a common, clear and unambiguous language for describing incidents;

- It should represent an accurate picture of the entire cybersecurity risk landscape, and be revised as the environment changes significantly;

- Its incident categories should be mutually exclusive and, with subcategories, should be as exhaustive as possible;

- It should be detailed enough to reflect important differences across and within incident categories and subcategories, but flexible enough to be operationally valuable;

- It should not substantially increase the complexity of – or the time required for – incident handing; and

- It must be designed with a view to generating statistics.

It is notable that many newer CSIRTs which were engaged over the course of this project expressed that one of the main challenges they faced in terms of producing robust statistics was the categorisation of incidents. They were largely unaware of the existing incident taxonomies. These teams would benefit enormously from an effort to develop and disseminate a shared incident taxonomy.

Finally, it may be advisable to engage third-party producers of incident-related data in the process to develop a shared incident taxonomy. CSIRTs are major consumers of these data services. Involving such organisations in the development of the incident taxonomy would increase the tool's value.

Methodological challenges

Once common definitions and shared incident taxonomies are agreed, it would be important to establish certain methodological criteria. There are different aspects to consider.

In some cases, incident reports may include information about what could be interpreted as more than one incident. For example, a constituent or third party may submit a report to the CSIRT with multiple IP addresses and/or domain names, all of which appear to share the same phishing content. The question arises: is this a single or multiple incident(s)? Some CSIRTs may treat the report as a single incident because the malicious content appears to be the same across all the websites, whereas other teams may count each IP address/domain name as a separate incident. These methodological discrepancies lead to inconsistent statistics. It would be very beneficial for the community to develop rules for recording incidents from reports across the range of categories and subcategories in the incident taxonomy.

Likewise, common counting rules ought to be established. These are urgently needed to distinguish instances of what could be the same incident. This is best illustrated through an example. A distributed denial of service (DDoS) attack may last for several hours, if not days, perhaps with periodic lulls in the attack. Is this a single or multiple incident(s)? To further complicate matters, by definition, DDoS attacks will involve multiple machines in the attack. They may also target more than one website or server. It is not always clear to CSIRTs how to account for these complex kinds of events in their statistics. Common counting rules for incidents would certainly strengthen the quality of CSIRT statistics.

Another complex methodological aspect regards the potential for double counting when data is received from multiple sources. CSIRTs should be aware of this problem, understand how it biases incident statistics and work together to identify ways to prevent it.

Improving statistical consistency

One way to improve statistical consistency is through team exercises. The ENISA *Good Practice Guide for Incident Management* (2010) recommends that CSIRTs take the following steps to ensure consistent incident statistics (see Box 2).

Box 2. Three steps to get consistent statistics

1) Gather your team together. Hand out a set of 10 different incident reports. Ask everybody to classify them according to your taxonomy.

2) Discuss the results to step one. Point out incidents which were easy for the team to understand and address. Point out those that were classified differently and discuss the reasons. Reach an agreement on future cases.

3) Repeat steps one and two periodically (e.g. quarterly) as well as every time new kinds of threats appear and you feel that these threats are not unambiguous in terms of their classification.

Source : ENISA Good Practice Guide for Incident Management (2010)

It may also be advisable for teams from different CSIRTs to engage in similar exercises at annual conferences and CSIRT events, at regional and international level. For example, the Annual Meeting of CSIRTs with National Responsibility would provide a good venue for teams to practice incident classification and to discuss and compare results to ensure greater consistency across teams. Increased participation in the FIRST Metrics SIG would also go a long way to improving CSIRT methodologies for incident statistics.

Practical challenges

The challenges inhibiting the production of high-quality incident statistics are not just conceptual or methodological. There are also several underlying practical challenges, which are arguably more difficult to resolve without a concerted effort among CSIRTs, their constituencies and other stakeholders.

The under-reporting of incidents by constituents is a major challenge for comprehensive incident statistics. If CSIRTs are not aware of the incidents that have affected members of their constituency, they clearly cannot include this information in the statistics they report. While there may be rare circumstances in which a constituent justifiably cannot or chooses not to report an incident to the CSIRT, more robust statistics would greatly benefit from as many incidents being reported as feasible. Reporting could take place even if CSIRT assistance is not needed to mitigate the incident. The reporting of all incidents to CSIRTs would greatly improve the comprehensiveness of statistics on incidents.

However, encouraging constituents to report incidents regularly to CSIRTs is not trivial, and may require incentives such as, for example, the sharing of intelligence about new threats. In some jurisdictions, governments are introducing new laws, policies and rules that mandate the reporting of significant security incidents by certain types of organisations – including providers of critical infrastructure – to a national authority. Depending on the country/economy, this authority may be the national CSIRT. Such policy measures may improve the overall reporting of incidents and the quality of incident statistics.

CSIRTs should aspire to include data on all reported and detected incidents in their incident statistics. This may seem obvious, but over the course of this project it was discovered that CSIRTs may exclude

from their statistics incidents affecting their constituents which the CSIRT did not directly handle.[26] Incorporating these incidents in the overall statistics may require CSIRTs to develop new processes and to assess any possible legal implications.

Further addressing the comprehensiveness of CSIRT incident statistics, teams should be encouraged to leverage more data sources in their incident handling and mitigation work. There are various data providers that can enhance CSIRTs' visibility of the incidents occurring on the networks of their constituents. These data feeds are often provided at no cost to national CSIRTs. While adding new data feeds may increase the overall numbers of incidents a CSIRT is expected to handle, in addition to increasing their incident statistics, the primary aim should be to achieve the highest visibility possible of the incidents occurring on its constituency's networks.

However, when adding new feeds teams should aspire to understand the provenance of the data to ensure its quality and to determine whether these data may appear in other feeds they receive, in order to prevent double counting.

The actual systems used by CSIRTs to handle, track and mitigate incidents may also need to be updated to produce better, more granular statistics. These systems should reflect a common incident taxonomy, like the one described above. They should be able to generate statistics according to the categories and subcategories of incidents within the taxonomy. As noted, reporting statistics at certain levels of granularity proved difficult for CSIRTs that participated in the feasibility study. Improved software tools should help to alleviate this problem.

A longer-term ambition could be to designate national CSIRTs as a clearinghouse for in-country incident statistics. National CSIRTs would collect data from all CSIRTs – private, public, academic, etc. – working within the country/economy. This would allow the national CSIRT to publish more comprehensive national incident statistics based on a common incident taxonomy.

As has been noted throughout this guidance, in countries/economies in which more than one national CSIRT operates, these teams would need to devise a mechanism by which to collaborate to produce national statistics regarding incidents.

Infrastructural challenges

Finally, certain factors related to the infrastructure of the Internet and other digital networks arguably present the most difficult challenges to accurately measuring security incidents. While it is impossible to resolve these challenges, a greater appreciation of them would help CSIRTs as they prepare and publish incident-related statistics.

Network topology affects a CSIRT's visibility of incidents in different ways. The main issue concerns determining, with some degree of certainty, how many distinct devices are operating on the networks for which a CSIRT is responsible. Two different effects are worth considering.

The widespread use of Network Address Translation (NAT) may obscure CSIRTs' visibility of their constituency's networks. A NAT device maps all IP addresses behind it to a single, globally unique IP address, making it difficult to know how many devices are operating behind the NAT device. In particular, the continued deployment of carrier grade NAT devices may significantly reduce CSIRTs' visibility of

26 . For example, incidents reported through CERT-UK's Cyber-security Information Sharing Partnership (CiSP) are currently excluded from CERT-UK's incident statistics because the incidents are handled by the community on CiSP as opposed to CERT-UK staff (CERT-UK, 2014: 7).

security incidents. This decreased visibility would result in the undercounting of incidents affecting devices behind NAT devices.

Another form of address-sharing technology, Dynamic Host Configuration Protocol (DHCP) address leasing, relies on intermittent connectivity whereby an IP address is given back to the resource pool when the connection is broken (OECD, 2014: 17). This may result in the over-counting of incidents through IP address reassignment, as a single affected host could appear more than once in incident reports (JPCERT/CC, 2014: 20).

The increased adoption of Internet-connected mobile devices, as well as the deployment of the "Internet of Things", will only add more complexity to these concerns. CSIRTs should be aware of how ongoing changes to the Internet infrastructure may impact on their capacity to detect and accurately distinguish security incidents.

SECTION 7: MEASURING NETWORKS FOR STATISTICAL PURPOSES

Introduction

Incident statistics can be very challenging to compare without an understanding of the size of the affected networks. For example, the fact that country *X*'s national CSIRT identified *n* malware-infected devices in a given year, while country *Y*'s CSIRT identified *m* during the same year, does not provide any information about the relative size of the networks in countries *X* and *Y*. Yet this is important information. Adjusting incident statistics to account for network size is a process referred to as statistical normalisation. Normalisation is essential to making statistics cross-comparable.

It is impossible to quantify the exact size of the networks that CSIRTs oversee. The perfect measurement of networks presents considerable methodological and technical challenges.[27] However, it is possible to approximate values for the size of these networks, which for statistical purposes ought to be sufficient. Throughout this project, various network-related statistics were considered as candidates for normalising statistics on incidents. Specifically, the feasibility study tested whether CSIRTs were able to provide data on various facets of their networks. During the analysis some possibilities were discarded, e.g. data on the number of autonomous systems.[28]

The statistical concepts presented in this section can be used to normalise incident-related statistics.[29] It is important to note that none of these should be treated as the "best" indicator of network size. Each has its strengths and weaknesses, which should be carefully considered. Though, certain of the proposed network statistics may be more appropriate than others for normalising specific incident statistics. It would be intuitive to normalise statistics regarding phishing websites, for example, with ccTLD statistics, as both pertain to web domains.

Internet users as an indicator of network size

One of the most obvious ways of approximating the size of a computer network is by counting the number of users. Fortunately, there are existing datasets with these statistics at the national level. The ITU, for example, estimates national Internet usage based on household surveys and subscription data.[30]

These data are available for nearly all countries/economies and are readily accessible online. Assuming that a national CSIRT's constituency covers an entire country/economy, the use of this data to normalise incident statistics is fairly straightforward. However, in countries/economies in which multiple national CSIRTs operate, these figures are less useful without first determining a CSIRT's share of the overall number of users. However, as has been discussed, teams could work together to combine their

27 . Chapter 5 of the *OECD Communications Outlook* explores various ways of measuring the Internet (OECD, 2013).

28 . An autonomous system is a network controlled by a single entity such as a large company, university or Internet service provider. Such a network is called autonomous because it can determine the routing of its traffic independently from any other network. Every autonomous system is assigned a unique number known as an ASN. While data on the number of autonomous systems are publicly available, these may not be very indicative of network size because there can be both very small and very large autonomous systems.

29 . Note that, for annual statistics, a mean would need to be calculated for each of the proposed network statistics to account for network growth from the beginning to the end of the reporting year.

30 . www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

incident statistics to produce national statistics, in which case using a national Internet usage statistic would be appropriate for normalisation.

Another potential limitation to using Internet user statistics as an indicator of network size is that they do not account for the fact that consumers increasingly connect to the Internet with multiple devices. Unfortunately, global statistics on the number of Internet-connected devices do not currently exist.

Internet subscriptions as an indicator of network size

Related to statistics on Internet usage are those on Internet subscriptions. Subscription statistics provide a good measure of the extent of a country/economy's adoption of the Internet. In particular, two types of subscription statistics are noteworthy: *i)* fixed broadband subscriptions and *ii*) wireless broadband subscriptions.

The OECD Broadband Subscriptions Criteria[31] are as follows:

- **Fixed (wired) broadband penetration indicator**

  a) DSL

  i) Includes all DSL lines offering Internet connectivity which are capable of download speeds of at least 256 kbit/s.

  ii) The DSL line is excluded if it is not used for Internet connectivity (e.g. leased lines).

  b) Cable

  i) Includes all cable modem subscriptions at download speeds greater than 256 kbit/s.

  c) Fibre

  i) Includes all fibre-to-the-premises (e.g. house, apartment) subscriptions at download speeds greater than 256 kbit/s.

  ii) Includes all fibre-to-the-building subscriptions (e.g. apartment LAN) using fibre-to-the-building but Ethernet to end-users. Note that this counts only the number of actual subscriptions to the provider, not end users.

  d) Other wired

  i) Broadband over powerline: Includes all broadband over powerline subscriptions with download speeds greater than 256 kbit/s.

  ii) Leased lines: Includes only circuits with Internet connectivity (only connections with speeds faster than 256 kbit/s to end users).

- **Wireless broadband penetration indicator**

  a) Satellite

  i) Includes all subscriptions with advertised download speeds of at least 256 kbit/s.

  b) Terrestrial fixed wireless

31 . www.oecd.org/sti/broadband/oecdbroadbandsubscribercriteria2010.htm

i) Includes all subscriptions with advertised download speeds of at least 256 kbit/s.

c) Terrestrial mobile wireless

i) Standard mobile subscriptions (only included with active use): Includes mobile subscriptions which advertise data speeds of 256 kbit/s or greater and which have been used to make an Internet data connection via IP in the previous 3 months. To be counted, the subscription must allow access to the greater Internet via HTTP and must have been used to make a data connection using the Internet Protocol in the previous three months. Standard SMS and MMS messaging do not count as an active Internet data connection even if they are delivered via IP.

ii) Mobile: Dedicated data subscriptions: Subscriptions to dedicated data services over a mobile network which are purchased separately from voice services either as a stand-alone service (modem/dongle) or as an add-on data package to voice services which requires an additional subscription. All dedicated mobile data subscriptions with recurring subscription fees are included as "active data subscriptions" regardless of actual use. Pre-paid mobile broadband plans require active use if there is no monthly subscription.

iii) Does not include

(1) Wi-Fi, except for the rare cases when Wi-Fi is used as the transport technology for a fixed wireless Internet service provider. The lines supporting Wi-Fi hotspots are already counted once in the fixed-broadband subscriptions methodology.

Data on fixed and wireless broadband subscriptions for OECD countries can be found on the OECD Broadband Portal.[32] In the future these data will be reported using speed tiers (OECD, 2015). The ITU also has a repository, which includes datasets on fixed (wired) broadband subscriptions for most of the world.[33]

Allocated IP addresses as an indicator of network size

The Internet Protocol (IP) is a communications protocol responsible for transporting data from a host to its destination across the Internet. IP uses a numeric addressing system and routes messages based on IP addresses, which specify the locations of the source and destination nodes. Every device connected to the Internet, whether a desktop computer, tablet or mobile device and so on, needs an IP address in order to communicate with other devices. Two versions of IP addressing are in use: IP version 4 (IPv4) and IP version 6 (IPv6) (OECD, 2013: 144).

While imperfect, allocated IPv4 address statistics can be used to approximate the size of a CSIRT's constituency's networks. There are different ways of arriving at the number of allocated IP addresses by network. These data are publically available from the five Regional Internet Registries: *i)* African Network Information Centre (AfriNIC) for Africa[34], *ii)* American Registry for Internet Numbers (ARIN) for the United States, Canada, several parts of the Caribbean region and Antarctica[35], *iii)* Asia-Pacific Network Information Centre (APNIC) for Asia, Australia, New Zealand and neighbouring countries[36], *iv)* Latin America and Caribbean Network Information Centre (LACNIC) for Latin America and parts of the

32 . www.oecd.org/sti/broadband/oecdbroadbandportal.htm

33 . www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

34 . ftp://ftp.afrinic.net/pub/stats/afrinic

35 . ftp://ftp.arin.net/pub/stats/arin

36 . ftp://ftp.apnic.net/public/stats/apnic/

Caribbean region[37] and *v)* Réseaux IP Européens Network Coordination Centre (RIPE NCC) for Europe, Russia, the Middle East and Central Asia[38].

There are, however, some limitations to this approach. First, not all allocated IPv4 addresses are in use, which introduces some bias. Second, the increased use of network technologies such as Network Address Translation as the remaining stock of IPv4 addresses is exhausted (OECD, 2014) means that large numbers of devices may be sharing the same public IPv4 address (i.e. that of the NAT device), which yet again introduces bias. Third, devices connecting via IPv6 would be excluded.

IPv6 adoption remains low and, for the time being, it would not be advisable to rely on these statistics to normalise incident data.

Country code top-level domains as an indicator of network size

A country code top-level domain (ccTLD) is an Internet top-level domain generally used or reserved for a country, sovereign state or dependent territory. Each country/economy appoints a manager of its ccTLD and sets the rules for allocating domains. ccTLD registrations provide an useful country-level statistic that can be used to normalise incident statistics.

These data can be requested from network information centres within the CSIRT's jurisdiction. They are also available from various third-party providers online.

The use of ccTLDs would provide a good but partial indication of country-level network size as these data exclude other top-level domains, in particular the generic TLDs (.com, .net, etc.). Another potential weakness regards the popularity of vanity web pages that use ccTLD names, which would skew the numbers for certain countries. These potentially biasing factors should be kept in mind when considering the use of these data for normalisation.

Innovations in network measurement

The CSIRT community should explore emerging innovative techniques for measuring the networks of the Internet. It will be important that the data from these techniques are reliable and as universal as possible and, ideally, available from public sources using harmonised and transparent methodologies. For example, advertising networks may have more accurate data on the number of users across networks but this data is often regarded as commercial or proprietary.

37 . ftp://ftp.lacnic.net/pub/stats/lacnic/

38 . ftp://ftp.ripe.net/ripe/stats

SECTION 8: CONCLUDING COMMENTS

The early sections of this statistical guidance *i)* explained the organisation and work of CSIRTs, *ii)* discussed the kinds of data accessible to CSIRTs and the status quo of the statistics CSIRTs produce and *iii)* identified the key anticipated stakeholders and uses for improved CSIRT statistics. Those sections were largely intended for policy-making audiences.

The focus of the guidance then shifted to CSIRTs themselves and in particular on *iv)* developing statistical indicators for CSIRT capacity, *v)* addressing the challenges CSIRTs currently face in the creation of high-quality, internationally comparable incident-related statistics and *vi)* discussing ways of measuring the networks of the Internet for statistical purposes in order to support better normalisation. These sections intended to guide and instruct CSIRTs on how to improve the quality of the statistics they produce.

This final section briefly highlights outstanding concerns related to the organisation and co-ordination of CSIRT statistics.

Outstanding concerns

To begin, for any guidance to be effective it must be widely adopted. Policy makers have a role to play by actively encouraging national CSIRTs to make use of the guidance presented in this document and to work with other CSIRTs to achieve its recommendations.

CSIRTs also have a role to play in facilitating dissemination. For example, organised panels at key events (FIRST, APCERT, TERENA, etc.) would help to raise the community's awareness of the guidance and its objectives, and to encourage widespread adoption.

Once the guidance is disseminated and adopted, it may be necessary to provide CSIRTs with resources to achieve the statistical aims. CSIRTs may require additional expertise and technologies for data collection and statistical analysis. Specialised training could also be required. These expenditures may require investment by government and/or other stakeholders.

This guidance places national CSIRTs at the locus of measurement. However, it leaves unanswered the question of which organisation would serve as the hub for collecting data and/or statistics from reporting CSIRTs. There are different points to consider:

- Such an organisation may be unnecessary insofar as CSIRTs publish statistics in their annual reports or through their websites.

- However, a dedicated organisational effort could drastically improve the outcomes. This effort could be undertaken by an already-established and trusted organisation, e.g. FIRST, CERT/CC or regional bodies such as APCERT, TERENA, AfricaCERT, OAS, the Organization of the Islamic Conference, etc.

- Alternatively, a new body or platform could be established to facilitate and manage this effort.

- Decisions would need to be taken as regards the scope of this organisation's responsibilities. For example, would individual CSIRTs or the hub be responsible for vetting the quality of data/statistics? Who owns the data/statistics?

Another outstanding concern regards a potential relationship between CSIRTs and national statistical offices (NSOs). It may be beneficial to make NSOs responsible for providing some degree of oversight, for example by tasking them with quality control or statistical training of certain members of CSIRTs.

These and other practical considerations should be discussed and decided on by both policy makers and CSIRTs as this guidance is finalised and disseminated.

GLOSSARY

AfricaCERT	Africa Computer Emergency Response Team
AfriNIC	African Network Information Centre
APCERT	Asia Pacific Computer Emergency Response Team
APEC	Asia-Pacific Economic Co-operation
APNIC	Asia-Pacific Network Information Centre
ARIN	American Registry for Internet Numbers
ASEAN	Association of Southeast Asian Nations
ASN	Autonomous system number
AU	African Union
ccTLD	Country code top-level domain
CERT	Computer Emergency Response Team
CERT/CC	CERT Coordination Center
CERT-UK	Computer Emergency Response Team United Kingdom
CIRT	Computer Incident Response Team
CiSP	Cyber-security Information Sharing Partnership
COFOG	Classification of the Functions of Government
CSIRT	Computer Security Incident Response Team
CYBEX	Cybersecurity Information Exchange
CybOX	Cyber Observable eXpression
DHCP	Dynamic Host Configuration Protocol
DHS	United States Department of Homeland Security
DDoS	Distributed Denial of Service
DSL	Digital subscriber line
ENISA	European Union Agency for Network and Information Security
EU	European Union
FIRST	Forum of Incident Response and Security Teams
FTE	Full-time equivalent
GGE	Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IODEF	Incident Object Description Exchange Format
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center
IGF	Internet Governance Forum
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
ITU	International Telecommunication Union
KISA	Korea Internet & Security Agency
LACNIC	Latin America and Caribbean Network Information Centre
MILE	Management Incident Lightweight Exchange
MMS	Multimedia Messaging Service
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
NSO	National Statistics Office
OAS	Organization of American States

OECD	Organisation for Economic Co-operation and Development
OIC	Organization of the Islamic Conference
RIPE NCC	Réseaux IP Européens Network Coordination Centre
SIG	Special Interest Group
SIRT	Security Incident Response Team
SMS	Short Message Service
SPDE	Working Party on Security and Privacy in the Digital Economy
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated eXchange of Indicator Information
TLD	Top-level domain
TERENA	Trans-European Research and Education Networking Association

REFERENCES

AU (2014), African Union Convention on Cyber Security and Personal Data Protection, African Union.

ASEAN Regional Forum (2006), *Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space*, Association of Southeast Asian Countries, Kuala Lumpur.

CERT-UK (2014), *Quarterly Report: April-June 2014*, UK National Computer Emergency Response Team.

ENISA (2006), *CERT Cooperation and its Further Facilitation by Relevant Stakeholders*, European Union Agency for Network and Information Security.

ENISA (2010), *Good Practice Guide for Incident Management*, European Union Agency for Network and Information Security.

EU (2013), *Proposal for a Directive of the European Parliament and of the Council concerning Measure to Ensure a High Common Level of Network and Information Security across the Union*, European Union.

GGE (2013), *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98, United Nations General Assembly.

IGF (2014), *Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams for Internet Security*, Internet Governance Forum.

ITU (2010), *Strengthening the Role of ITU in Building Confidence and Security in the Use of Information and Communication Technologies*, Resolution 130, the Plenipotentiary Conference of the International Telecommunication Union, Guadalajara.

JPCERT/CC (2014), *Cyber Green Research Paper*, Japan Computer Emergency Response Team Coordination Center.

NIST (2012), *Computer Security Incident Handling Guide*, National Institute of Standards and Technology, Special Publication 800-61, Revision 2, Gaithersburg, MD, USA.

OAS (2004), *Framework for Establishing an Inter-American CSIRT Watch and Warning Network*, Organization of American States, Montevideo, Uruguay.

OECD (2002), *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, Organisation for Economic Co-operation and Development, Paris.

OECD (2011), *Recommendation of the Council on Principles for Internet Policy Making*, Organisation for Economic Co-operation and Development, Paris.

OECD (2012a), *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies For The Internet Economy*, OECD Digital Economy Papers, no. 211, OECD Publishing, Paris.

OECD (2012b), *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 Publishing, Paris.

OECD (2013), *OECD Communications Outlook 2013*, OECD, Paris.

OECD (2014), *The Internet in Transition: The State of the Transition to IPv6 in Today's Internet and Measures to Support the Continued Use of IPv4*, OECD Digital Economy Papers, no. 234, OECD Publishing, Paris.

OECD (2015), *OECD Digital Economy Outlook 2015*, OECD, Paris.

von Schirnding, Y. (2002), *Health in Sustainable Development Planning: The Role of Indicators*, World Health Organization, Geneva.

White House (2011), *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, Washington, DC, USA.

ANNEX A: PROJECT ENGAGEMENT ACTIVITIES

- April 2012: the project was presented at a workshop on CSIRTs at the APEC TEL 45 meeting in Vietnam, where it received strong interest from APCERT and US-CERT. It was also presented to the APEC TEL SPSG, which agreed to co-operate with the OECD and the CSIRT community in carrying out the project.

- June 2012: the project was presented to the APCERT Steering Committee, which expressed its support for collaboration with OECD and APEC TEL. The same month, a presentation was made at the Annual Meeting of CSIRTs with National Responsibility, back-to-back with the 24th Annual FIRST Conference in Malta. An invitation to the Metrics Special Interest Group (SIG) of FIRST was extended to OECD.

- February 2013: a webinar outlining the project's aims and objectives was delivered to the FIRST Metrics SIG.

- March 2013: the project was presented to the APCERT 2013 Conference in Brisbane, Australia (via teleconference).

- June 2013: a presentation was made at the International Watch and Warning Network (IWWN) meeting in Zurich, Switzerland. The same month, the Secretariat attended the 25th Annual FIRST Conference in Bangkok, Thailand to present an update on the project to the FIRST Metrics SIG and to engage in discussions and interviews with representatives of national CSIRTs regarding how they create, use and compare statistics.

- September 2013: a project update was given at the APEC TEL SPSG meeting in Honolulu, Hawaii. The same month, the APCERT Steering Committee meeting in Yogyakarta, Indonesia was updated on the project.

- October 2013: a presentation on the project was made at the Internet Governance Forum in Bali, Indonesia. Later that month, it was presented to the Latin America and Caribbean Network Information Centre (LACNIC) and Latin American and Caribbean Network Operators Group (LACNOG) joint meeting in Curaçao.

- November 2013: the Secretariat was invited to present at the Inaugural Cyber Security Capacity Centre Conference at Oxford University, United Kingdom.

- March 2014: the Secretariat was invited to participate in the APCERT AGM and Conference. This provided a strategic opportunity to update APCERT members on the project, raising the Asia-Pacific CSIRT community's awareness of the progress to date. It also allowed the Secretariat to learn more about the realities of CSIRTs operating in the region, including the potential role for statistics to support policy making. At the meeting an important strategic contact was made with AfricaCERT, which was an invited guest of the conference. AfricaCERT facilitates incident response capabilities among African countries and provides capacity building, access to best practices, tools and trusted communication at the continental level.

- June 2014: the Secretariat attended the 26th Annual FIRST Conference in Boston, Massachusetts to participate on a panel on "Developing Cybersecurity Risk Indicators", as well as to give an update to the Metrics SIG.

- September/October 2014: the APEC TEL SPSG was updated on the project's progress at the 50th APEC TEL conference, hosted in Brisbane, Australia.

ANNEX B: FEASIBILITY STUDY PARTICIPANTS

The national CSIRTs that responded to the feasibility study questionnaire are:

- CCIRC, Canadian Cyber Incident Response Centre
- CCN-CERT, Computer Emergency Response Team of the National Cryptologic Center (Spain)
- CERT Australia, Computer Emergency Response Team Australia
- CERT.at, CERT Austria
- CERT.be, Federal Cyber Emergency Team (Belgium)
- CERT.br, Computer Emergency Response Team Brazil
- CERT.LV, IT Security Incident Response Institution of the Republic of Latvia
- CERT.PL, CERT Polska (Poland)
- CERT.PT, Serviço de Resposta a Incidents de Segurança (Portugal)
- CERT-MX, Centro Especializado en Respuesta Tecnologica de Mexico
- CIRCL, Computer Incident Response Center Luxembourg
- CSIRT.SK, Computer Security Incident Response Team Slovakia
- EG-CERT, Egyptian Computer Emergency Readiness Team
- GovCERT.ch, Computer Emergency Response Team of the Swiss Government
- GovCERT.CZ, Government CERT of the Czech Republic
- GOVCERT.LU, Ministère d'État - CERT Gouvernemental (Luxembourg)
- INTECO-CERT, National Institute of Communication Technologies IT Incident Response Team (Spain)
- JPCERT/CC, Japan Computer Emergency Response Team Coordination Center
- KrCERT/CC, Korea Internet Security Center
- SI-CERT, Slovenian Computer Emergency Response Team
- SWITCH-CERT (Switzerland)
- TWNCERT, Taiwan National Computer Emergency Response Team
- TZ-CERT, Tanzania Computer Emergency Response Team
- US-CERT, United States Computer Emergency Readiness Team

ANNEX C: EXPERT PARTICIPANTS

The experts who participated in the project are:

- Kenneth Bendelier
- Peter Cassidy
- Andrea Dufkova
- Sara García Bécares
- Marcos Gómez Hidalgo
- Sherif Hashem
- Michael Hausding
- Christine Hoepers
- Chris Horsley
- Jean Robert Hountomey
- Yurie Ito
- L. Aaron Kaplan
- Baiba Kaskina
- Piotr Kijewski
- Nathan Klassen
- Klaus-Peter Kossakowski
- Thomas Millar
- Michael Murray
- Jose Nazario
- Shari Pfleeger
- Greg Rattray
- Klaus Steding-Jessen
- Don Stikvoort
- Héctor René Suárez
- Maarten Van Horenbeeck
- Adli Wahid
- Bisyron Wahyudi
- Ewan Ward
- Du Yuejin

ANNEX D: AREAS FOR FUTURE CSIRT MEASUREMENT

This annex aims to feed future reflection on statistical indicators within the scope of the work on CSIRT measurement. Ideas for additional indicators include:

Capacity

- Training: the frequency with which incident response-related training is conducted within CSIRTs
- Preparedness: the frequency of "cyber exercises" conducted by CSIRTs as an indicator of preparedness
- Informal co-operation, as opposed to formal co-operation (as previously mentioned in Section 5)

Risk Conditions

- Unwanted network traffic: defined as the portion of unwanted traffic – for example, malicious attack traffic, spam, etc. – as a percentage of overall network traffic. This could be understood by the equation $\frac{\text{attack traffic}}{\text{all traffic}}$ for any country/economy, region or globally.
- Infected hosts: defined as the number of hosts infected by some vector (malware, for example) as a percentage of the number of all identified hosts. This could be understood through the equation $\frac{\text{number of infected hosts}}{\text{total number of hosts}}$ per country/economy, region or globally.
- Vulnerable hosts: defined as the number of hosts identified as being susceptible to a particular vulnerability as a percentage of all hosts known to provide that service. This could be understood through the equation $\frac{\text{number of vulnerable hosts}}{\text{total number of hosts}}$ per country/economy, region or globally.

Incidents

- Identification: The percentage of reported cybersecurity incidents for which the cause of the incident was identified
- Response time: Mean time spent on incident response (per incident)
- Number and type of recurring incidents
- Detection trends for notable malware families