Association for Information Systems
AIS Electronic Library (AISeL)

CONF-IRM 2016 Proceedings

International Conference on Information Resources Management (CONF-IRM)

2016

Prioritizing computer security incident response services for the South African National Research Network (SANReN)

Roderick Mooi
Nelson Mandela Metropolitan University, rmooi@csir.co.za

Reinhardt Botha
Nelson Mandela Metropolitan University, ReinhardtA.Botha@nmmu.ac.za

53. Prioritizing computer security incident response services for the South African National Research Network (SANReN)

Roderick Mooi
Nelson Mandela Metropolitan University
RMooi@csir.co.za

Reinhardt Botha
Nelson Mandela Metropolitan University
ReinhardtA.Botha@nmmu.ac.za

Abstract

The need for the South African (SA) National Research and Education Network (NREN) to establish a Computer Security Incident Response Team (CSIRT) was identified. CSIRTs offer a subset of all possible security services based on the environment and needs of the customers. Selecting this subset has its challenges as the view of the customer may differ from the provider and knowing which services will have the most impact (or be most beneficial) is difficult. In order to address the problem, this paper aims to propose an informed selection and prioritization of initial services for the SA NREN CSIRT, an academic sector CSIRT in South Africa. In order to do this, the first two stages of the IT Infrastructure Library (ITIL) service portfolio management process are used: *defining* the services based on authoritative CSIRT literature and *analyzing* them for value proposition and prioritization. A survey was used to obtain the viewpoint of the prospective customer base. The services are then selected based on the revelation of the SA NREN CSIRT as a coordinating CSIRT as well as the survey results. The primary contribution is providing a list of services for the CSIRT in the context of the SA NREN environment that can be used to develop a services portfolio. This study is useful to anyone wishing to select services for a new CSIRT or wanting to revise a CSIRT services portfolio.

Keywords

CSIRT, CERT, security operations center, information security, incident response, services, ITIL service portfolio management.

1. Introduction

The concept of a Computer Security Incident Response Team (CSIRT) is well known in the information security domain as: "*an organization or team that provides services and support to a defined constituency for preventing, handling, and responding to computer security incidents*" (Alberts, Dorofee, Killcrece, Ruefle & Zajicek, 2004, p. 2). These incidents include all kinds of malicious activity on a network and PC level, ranging from Denial of Service (DoS) attacks and hacking attempts to malware and compromised systems. A CSIRT attempts to isolate, mitigate the effects of, disable and assist with recovery from these incidents (Killcrece, Kossakowski, Ruefle & Zajicek, 2003a). Secondary responsibilities may include incident prevention, advisory dissemination and security consultancy services in order to minimize risk and reduce actual incidents. The exact services provided depend on the needs of the constituency (customer base)

and the available resources (finances and staff) (ENISA, 2006). It is useful to observe that similar services can be provided by Security Operations Centers (SOCs) (Zimmerman, 2014).

CSIRTs have recently received renewed interest for novel areas of application like cloud computing (with its unique information security challenges) (Ab Rahman & Choo, 2015) and in developing countries (Ellefsen & von Solms, 2012; Wara & Singh, 2015) catching up with the Internet bandwagon.

A National Research and Education Network (NREN) provides backbone network infrastructure, access connectivity and specialized services to the academic and research institutions of a country. This includes high-bandwidth links for science and research, commodity Internet connectivity, network support and maintenance, and related services. An NREN can be seen as a specialized Internet Service Provider (ISP) for the research and education community of a country or region (GÉANT Association, 2010, para. 8). The South African National Research Network (SANReN) competency area together with the Tertiary Education and Research Network of South Africa (TENET) constitute the South African (SA) NREN. The SANReN project team design and build the network while the TENET team operate it. Both parties are involved in the development and provisioning of value-added services on top of the network (Petruccione et al., 2013). As of 28 February 2015, 204 higher education and research sites were connected to SANReN providing multi-gigabit Internet access with individual site bandwidth averaging at 2.82 Gbps (Staphorst, 2015). The number of connected sites continues to grow, covering nearly one million users at public universities, science councils and national research facilities throughout South Africa.

From an ITIL perspective, SANReN and TENET are regarded as external service providers to the beneficiaries and customers of the NREN (Cannon, 2011, p. 83). As part of its mandate to develop new services for NREN beneficiaries, the SANReN competency area has been investigating the establishment of a CSIRT for the SA NREN. The remainder of this paper reports on how the SANReN team has proceeded to define the specific CSIRT services that should be offered, commencing with a delineation of the research. Thereafter the survey approach and results are presented followed by the selection of services in Section 7.

2. Delineating the Research

Successfully providing CSIRT services requires an holistic approach. This section focuses on how the services themselves can be selected by presenting the research problem, objectives and approach used in this paper.

2.1 Research Problem and Objective

The size of the SANReN makes it particularly vulnerable to malicious activity; including attacks on the data and infrastructure. In addition, intellectual property at connected universities and science councils is a valuable target for malicious actors. The threat of malicious activity including data theft, Denial of Service (DoS) attacks and virus outbreaks is very real and handling incidents on this scale will require a collaborative effort.

As a means of addressing this problem, it is proposed that an academic sector CSIRT (Killcrece et al., 2003a) be established to protect the NREN infrastructure and provide information security-

related services to the NREN customers and beneficiaries. One of the considerations is which CSIRT services to provide. The objective of this paper is therefore to expound on the literature study and survey process followed in order to determine which SA NREN CSIRT services should be provided.

The approach used to achieve this objective is influenced by the manner in which people from industry select services. Considering that a CSIRT can be seen as a team providing specialized IT services to defined customers (the constituency) (West-Brown et al., 2003), the IT Infrastructure Library (ITIL®), as a framework for IT service management, is certainly applicable. Thus, an ITIL-based approach was selected to provide structure to the study.

2.2 ITIL Service Portfolio Management Approach

According to ITIL, it is critical for a service provider to ensure that they deliver value to the consumer of the service (Cannon, 2011, p. 38). Furthermore, the value of a service lies in the perception of the customer and not the provider (Cannon, 2011, p. 55). Although a CSIRT as a whole can be seen as a service provided to a constituency, there are also a range of sub-services that can be provided. These services are external, customer-facing services (Cannon, 2011, p. 52). In order to facilitate the decision of which sub-services should be provided by the SA NREN CSIRT, a survey was constructed and distributed to the future CSIRT constituency. The questions have an emphasis on determining the current situation and service requirements of the CSIRT's potential customers thus enabling one to gauge the respondent's requirements (Cannon, 2011, p. 88) and perception of the value of each service (Cannon, 2011, pp. 56–57).

The ITIL service portfolio management process is used to define the CSIRT activities in terms of services. There are four phases in this process: define, analyze, approve and charter (Cannon, 2011, p. 180). In this paper the first two phases are executed in part. Firstly, generic CSIRT services are defined according to authoritative CSIRT literature in Section 4. Secondly, the value proposition and prioritization of services for the SA NREN CSIRT is achieved in Section 7 following the survey outcomes. The methodology used to execute this process is described in the next section.

3. Methodology

Previous studies identified core CSIRT literature from ScienceDirect, Scopus, SpringerLink, IEEEXplore and Google Scholar based on a pattern of authoritative sources from respected authors (Mooi & Botha, in press). The primary sources were then selected as the most relevant publications from the associated institutions. A subset of this literature provides information on CSIRT services, as revealed in Table 1, following the form of a concept matrix (Webster & Watson, 2002).

Source	Service information	Institution	Description
Smith (1994)	X	AusCERT[i]	This article briefly mentions CSIRT services.
Brownlee & Guttman (1998)	XX	AUCK, SUN[ii]	An early list and description of services is provided in this best practice RFC – including real-time (reactive) and non-real-time (proactive) services – incident response (triage, coordination and resolution) and proactive activities (provisioning of information, security tools, education and training, product

			evaluation, site security auditing and consulting).
West-Brown et al. (2003)	XXX	CMU-SEI[iii]	This handbook provides an updated list of all CSIRT services and categories as well as detailed descriptions of each service. (The original list was presented in the first edition of the handbook.)
Killcrece et al. (2003a)	XXX	CMU-SEI	Focusing on CSIRT organizational models, this report contains the same list and descriptions as West-Brown et al. (2003). A mapping of services to organizational models plus a summary of all models with core and extended services is also provided.
Killcrece et al. (2003b)	X	CMU-SEI	A state of the practice CSIRT survey. This report lists the services with brief descriptions of the each service category. It further reports on the services provided by survey participant institution.
Alberts et al. (2004)	X	CMU-SEI	This report on CSIRT processes provides an essential list of CSIRT services as well as the description of a coordinating CSIRT.
ENISA (2006)	XX	ENISA[iv]	This guide (in its Appendix 2) repeats the list and descriptions from West-Brown et al. (2003).
ENISA (2010)	X	ENISA	A minimal listing of services from CERT-CC[v] plus a list of extended services including forensics and vulnerability handling is made available in this guide. It refers to ENISA (2006) for services detail.
Cichonski, Millar, Grance, & Scarfone (2012)	XX	NIST[vi]	This report of recommendations lists the incident response process and examples of other services (with a short description) such as intrusion detection, advisory distribution, education and awareness, and information sharing.

[i] Australian Computer Emergency Response Team
[ii] University of Auckland (AUCK) with Sun Microsystems (SUN)
[iii] Software Engineering Institute of Carnegie Mellon University
[iv] European Union Agency for Network and Information Security
[v] The CERT coordination center
[vi] National Institute of Standards and Technology

Table 1: Literature concept matrix for CSIRT services

From the concept matrix, the two primary sources for CSIRT services were identified based on the quantity of services-related material: the Handbook for Computer Security Incident Response Teams (CSIRTs) (West-Brown et al., 2003) and Organizational models for Computer Security Incident Response Teams (CSIRTs) (Killcrece et al., 2003a) both from the Carnegie Mellon Software Engineering Institute (CMU-SEI). The Handbook for Computer Security Incident Response Teams provides guidance on building and running a CSIRT with a particular focus on the incident handling service (West-Brown et al., 2003, p. xv). In addition, a basic CSIRT framework is provided covering the mission, constituency, organizational placing and relationships of the CSIRT to other teams. Detailed descriptions of CSIRT services, policies and team operations (including staffing issues) are supplied. Organizational models for Computer Security Incident Response Teams (CSIRTs) (Killcrece et al., 2003a) provides guidance on selecting the correct model for an organization's incident response capabilities. The primary focus is on the organizational model and operational structure of the team. Common CSIRT models with their attributes, respective advantages and disadvantages and typical service offerings are discussed. The other sources provide inputs as indicated in the table. A study of

these sources revealed a common list of services and descriptions that developed over time. This "standard" list and descriptions, also available on the web[1], are utilized in this paper with the *objective of establishing a baseline of CSIRT services*.

Surveys are an excellent method for obtaining facts and opinions (Hofstee, 2006, p. 122). Therefore a *survey* was selected as the research method towards achieving the objective of determining which services the SA NREN CSIRT should provide. In 2012 an exploratory survey was distributed to SANReN beneficiary institutions. This survey revealed a definite interest in CSIRT services but also some deficiencies in understanding within the community. It was therefore decided to perform a more in-depth literature study, host a workshop where the service details could be explained to and discussed with the constituency and then ask the attendees to complete a redesigned survey. This second survey was developed based on the information obtained through the literature study, compiled in Word and physically distributed and completed at a workshop as explained next.

In May 2015, SANReN and TENET hosted a workshop with NREN beneficiary institutions to explore the establishment of an SA NREN CSIRT[2]. One of the workshop objectives was to explain the possible services that could be provided and to determine which services should have priority from the perspective of the participants. Attendees were educated on the possible services through presentations and discussions. A questionnaire was then handed out to the attendees for completion with the request that each institution respond only once. The completed surveys (feedback) were physically collected and the results were captured in Excel for analysis and graphing. The next section provides background on CSIRT services prior to describing the SA NREN environment (Section 5) and presenting the results of the survey (Section 6). Thereafter, the selection of services for the SA NREN CSIRT based on the survey results and literature is described in Section 7.

4. CSIRT Services

According to ITIL, "A service is a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks" (Cannon, 2011, p. 47). CSIRT services assist customers in conducting their business by facilitating a more secure IT environment. They are classified in three broad categories, namely reactive, proactive or security quality management services (Killcrece et al., 2003a).

As the primary CSIRT activity, reactive services involve actions taken to resolve or mitigate incidents as they occur (Alberts et al., 2004). They are triggered by events or requests requiring a "reaction" and thereby initiating the service process (Killcrece et al., 2003a, p. 13). Proactive services are aimed at preventing incidents from occurring in the first place by providing related announcements and information for preparing, protecting and securing systems (Killcrece et al., 2003a, p. 14), training and education, monitoring and sharing information (Alberts et al., 2004). Security quality management services have a broader focus and may be provided by the CSIRT

[1] http://www.cert.org/incident-management/services.cfm
[2] http://www.csir.co.za/news/2015/08/education_community.html

or another entity in an organization depending on the specific structure (Killcrece et al., 2003a, p. 14). A commonly accepted list of CSIRT services is provided in Table 2.

	Service
Reactive services	Alerts and warnings
	Incident handling – analysis, support, coordination
	Incident response on site
	Vulnerability handling
	Artifact handling
Proactive services	Announcements
	Technology watch
	Security audits or assessments
	Configuration and maintenance of security tools, applications and infrastructure
	Development of security tools
	Intrusion detection services
	Security-related information dissemination
Security quality management services	Risk analysis
	Business continuity and disaster recovery planning
	Security consulting
	Awareness building
	Education and training
	Product evaluation or certification

Table 2: CSIRT Services
Source: West-Brown et al. (2003)

Detailed descriptions of these services are beyond the scope of this paper but can be found in West-Brown et al. (2003) and Killcrece et al. (2003a). Most CSIRTs do not provide all of these services but rather a subset based on the type of CSIRT and the needs of the constituency (Killcrece et al., 2003a, p. 14). A CSIRT should therefore select a core service offering and grow that as the need arises and resources allow (Killcrece et al., 2003a, p. 24).

5. SA NREN Environment

In order to optimize the survey for the SA NREN CSIRT and determine the services requirements, we needed to understand the SA NREN environment. Following the guidance presented in Mooi & Botha (2015), the SA NREN CSIRT environment is defined as an academic sector CSIRT serving the whole country of the Republic of South Africa. An embedded organizational model – with SANReN, TENET or a combination of both as the hosting organization – is preferred. These decisions are reflected in Table 3.

Type of CSIRT	Academic (research and education)
Geographic area	National – Republic of South Africa
Organizational model	Embedded – SANReN / TENET / Both

Table 3: SA NREN CSIRT Environment

This environment further reveals the constituency as the research and education institutions of South Africa: universities, science councils and supporting organizations; an *external* constituency. Based on these deductions, the SA NREN CSIRT is classified as a *coordinating* CSIRT: the customers are from external organizations and the CSIRT focus would be on coordination (Killcrece et al., 2003a, p. 130).

In order to determine the required CSIRT services is it useful to determine the current state of affairs with respect to incident response in that environment. As described in Section 3, a survey was selected as the instrument to perform a needs analysis and identify beneficial CSIRT services from the perspective of the SA NREN community. The survey questions were constructed based on the core services for coordinating CSIRTs (Killcrece et al. 2003a, pp. 136–137). The incident, vulnerability and artifact coordination services were generalized to "handling" and an intrusion detection service option was included as this could be attractive to this specific constituency based on the nature of the environment[3]. The next section presents the results of the survey.

6. Survey Results and Discussion

The survey was distributed to the 25 institutions represented at the 2015 workshop to explore the establishment of a SA NREN CSIRT. Eighteen institutions (72%) completed the survey. Respondents were asked to rank the CSIRT services by value/importance: *a score of 1 meaning most important* and *11 meaning least important*. The combined responses from the 18 institutions resulted in the prioritization of services as per Table 4. As seen in the table, the top three services are: intrusion detection services, alerts and warnings, and incident handling/response. In the following section these results and their implications on services selection are discussed.

The services ranking from the survey results provide useful inputs towards the SA NREN CSIRT services selection. To finalize the selection, some other factors need to be considered. This is because the customer's perception may differ from that of the provider and these perceptions need to be harmonized. For example, to illustrate with the overlap of services, providing alerts and warnings require information to communicate on either from a technology watch service or incident report (from the handling or intrusion detection services). The literature is also re-visited to identify the primary sources for this type of CSIRT – identified as a *coordinating CSIRT* based on the *environment* (see Section 5). The next section therefore describes the selection of core services based on these factors culminating in a final selection of services for the SA NREN CSIRT.

[3] It would be more cost effective to provide a central IDS service than for each institution to deploy their own solution. The SA NREN CSIRT will also have insight and tools not accessible to the community that can be utilized for intrusion detection.

Rank	Service	Combined score*
1	Intrusion detection services	52
2	Alerts and warnings	53
3	Incident handling/response	66
4	Vulnerability handling	72
5	Incident coordination	82
6	Announcements	83
7	Technology watch	86
8	Awareness building	89
9	Information dissemination	107
10	Education and training	109
11	Artifact handling	119

*combined by addition; lowest score = highest importance

Table 4: Survey Results: Services by importance

7. Selection of SA NREN CSIRT Services

Killcrece et al. (2003a, pp. 135–137) provide a summary of services offered for each type of CSIRT identified in the handbook. This information is used to supplement the survey findings and facilitate the selection of services for the SA NREN CSIRT as shown in Table 5. The combined decision column shows the final decision as a combination of the survey rank together with the services identified for coordinating CSIRTs. The selected services for the SA NREN are shown in **bold**.

To be called a CSIRT, the team must provide at least one of the incident handling services: incident analysis, response on site, support and/or coordination (West-Brown et al., 2003). For the SA NREN CSIRT, it makes sense that at least *incident response support and coordination* services are provided. Incident analysis could be offered in a limited fashion though is generally restricted to an advisory role for coordinating CSIRTs (Killcrece et al., 2003a).

Vulnerability and artifact response coordination would form part of the incident coordination service (as they are interdependent). Artifact handling is unlikely though as this is a coordinating CSIRT.

	Service	Survey rank*	Coordinating CSIRTs**	Combined decision
Reactive services	**Alerts and warnings**	2	Yes – core	YES – high ranking + core
	Incident handling	3 + 5 (coord.)	Yes – core	YES – high ranking + core
	Incident response on site	N/A [61% interest]	No – unusual	NO
	Vulnerability handling	4	Coordination only	YES – high ranking; coordination only
	Artifact handling	11	Coordination only	NO – low ranking
Proactive services	**Announcements**	6	Yes – core	YES – med. ranking + core
	Technology watch	7	Yes – core	YES – med. ranking + core
	Security audits or assessments	N/A [94% interest]	No – unusual	NO – despite high interest it is unusual for coordinating CSIRTs

	Security tools, applications and infrastructure	N/A [83% interest]	No – unusual	NO – unusual for coordinating CSIRTs
	Development of security tools	N/A	No – additional	NO –resource intensive + additional
	Intrusion detection	1	No – unusual	YES – although unusual it's the highest ranked for this constituency
	Information dissemination	9	Yes – core	YES – although low ranked it is integrated into the other services + core
Security quality management services	Risk analysis	N/A [83% interest]	No – additional	NO – additional for coordinating CSIRTs; consider later
	Business continuity and DR planning	N/A [61% interest]	No – additional	NO – additional for coordinating CSIRTs; consider later
	Security consulting	N/A [72% interest]	No – additional	NO – additional for coordinating CSIRTs; consider later
	Awareness building	8	Yes – core	YES – med. ranking + core
	Education and training	10	Yes – core	YES – can build on above + core
	Product evaluation or certification	N/A [55% interest]	No – additional	NO – low interest + additional

* lowest number = most important / highest rated. Interest was identified in a separate question.
** adapted from Killcrece et al. (2003a, pp. 136–137)

Table 5: CSIRT Services showing survey results and services for coordinating CSIRTs

Alerts and warnings include notifications of incidents, critical vulnerabilities or related matters (e.g. fixes or mitigation advice) (Killcrece et al., 2003a). "The alert, warning or advisory is sent as a reaction to the current incident state – to notify constituents of the activity and to provide guidance for protecting or recovering affected systems." (Cosmin Ciobanu et al., 2013, p. 4). For the SA NREN, examples from 2013-2015 include DDoS attacks, Heartbleed, Shellshock and the NTP vulnerability alerts.

Announcements are similar to alerts but less urgent and aimed at proactive measures to reduce possible future incidents with medium- to long-term impact. They include general IT security news, best practices, patch release information, hot topics, latest tools, etc. This information equips the constituency to protect systems and networks against new vulnerabilities before they can be exploited (West-Brown et al., 2003).

The *intrusion detection* service includes the deployment, monitoring and response to events reported by sensors on the network. For the SA NREN CSIRT this could include intrusion detection systems, honeypots, network telescopes and other sensors distributed on SANReN. Alerts and/or incident reports could be triggered by this service. To be effective, this service requires specialized tools or expertise (Killcrece et al., 2003a).

Awareness building, including best practices and precautions (West-Brown et al., 2003), can take place in various forms. Direct training can form part of the incident response process for an individual or group from the constituency. It could also be extended to workshops, tutorials, courses, etc. Topics for awareness building include guidelines for reporting incidents, approaches and processes for responding to incidents as well as useful tools and technologies. The exact

mechanisms and depth of service will be determined during implementation and could also evolve with time. This is seen as a fundamental service for the SA NREN CSIRT that could be supplemented by *education and* more in-depth *training* at a later date.

The *technology watch* service ``involves reading security mailing lists, security web sites, and current news and journal articles in the fields of science, technology, politics, and government to extract information relevant to the security of the constituent systems and networks" (West-Brown et al., 2003, p. 30). Topics can include technical developments and emerging technologies, security-related trends, hacker activities and even legal, social or political issues (Killcrece et al., 2003a). This description reveals the dependence of other services on this service.

Lastly, *security-related information dissemination* entails the development and publishing of security-related information (Killcrece et al., 2003a). “This service provides constituents with a comprehensive and easy-to-find collection of useful information that aids in improving security” (West-Brown et al., 2003, p. 32). This information can include outputs from the technology watch, incident handling and intrusion detection services in the form of alerts and warnings, announcements, a knowledge base (e.g. website/wiki), dashboards or even training materials (consult Killcrece et al. (2003a, p. 22) for additional examples).

The SA NREN service offering, as discussed in this section, is repeated in Table 6 in summary form for clarity.

Reactive services	Alerts and warnings
	Incident handling
	Vulnerability coordination only
Proactive services	Announcements
	Technology watch
	Intrusion detection services
	Information dissemination
Security quality management services	Awareness building
	Education and training

Table 6: Service offering for the SA NREN CSIRT

This offering is a subset of the services for coordinating CSIRTs with the addition of intrusion detection services based on the environment and survey results as described previously in this section.

This information facilitates the compilation of a services portfolio for the SA NREN CSIRT. During the establishment phase, the other areas of CSIRT requirements (staffing, tools, policies, etc.) can be developed accordingly (Mooi & Botha, in press). Once the CSIRT is operational, these services would be offered as described. As the CSIRT matures and the needs of the constituency develop, additional services can be provided for inclusion in the services pipeline thereby extending the services offering (for ideas consult Killcrece et al. (2003a, pp. 26–30)).

8. Conclusion

Following the identification of the need for an academic sector, coordinating CSIRT in South Africa, this paper described the process of selecting the initial services for the SA NREN CSIRT. Firstly, CSIRTs and the South African NREN environment were introduced. Thereafter the research problem (reducing the threat of malicious activity and coordinating incident response on the NREN) and objective (determining which CSIRT services should be provided) was described. The ITIL service portfolio management approach used to achieve this objective was presented next. This approach entails defining the services informed by authoritative CSIRT literature, the specific environment, as well as the perspective of the future constituency.

Section 3 described how the literature study and survey method were used to collect the data for the paper. The next section introduced CSIRT services with a detailed description of the service categories and a list of all possible services. The SA NREN environment, as an important factor to consider when selecting services, was described next. In order to determine the constituency's perspective on which services should be provided, a survey was utilized and filled in by attendees of an SA NREN CSIRT workshop.

In Section 6 the survey results were presented followed by a brief discussion on how these results could be used to inform the selection of services complemented by literature advice and considering the environment. Lastly, the actual selection of the SA NREN CSIRT initial service offering is presented in Section 7. This result is a useful foundation for the development of the CSIRT services portfolio. The paper serves as an illustration of how CSIRT services can be selected and prioritized and is useful for anyone desiring to perform a similar exercise or maintain a CSIRT services portfolio.

References

Ab Rahman, N. H., & Choo, K.-K. R. (2015). A survey of information security incident handling in the cloud. *Computers & Security*, *49*, 45–69.

Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R., & Zajicek, M. (2004). *Defining Incident Management Processes for CSIRTs : A Work in Progress*.

Brownlee, N., & Guttman, E. (1998, June). Expectations for Computer Security Incident Response. *IETF*. IETF. Retrieved from http://www.ietf.org/rfc/rfc2350.txt

Cannon, D. (2011). *ITIL Service Strategy*. London: The Stationary Office (TSO).

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide - Recommendations of the National Institute of Standards and Technology*. *NIST Special Publication*.

Cosmin Ciobanu, Potter, M., Stikvoort, D., Maj, M., Chlebowski, T., Reijers, R., & Wollenberg, M. (2013). *Alerts, Warnings and Announcements: Best Practices Guide*. Retrieved from https://www.enisa.europa.eu/activities/cert/support/awa/at_download/fullReport

Ellefsen, I., & von Solms, S. (2012). Implementing Critical Information Infrastructure Protection Structures in Developing Countries. In *Critical Infrastructure Protection VI* (pp. 17–29). Springer.

ENISA. (2006). *A step-by-step approach on how to set up a CSIRT* (Vol. 1).

ENISA. (2010). *Good Practice Guide for Incident Management*. Retrieved from www.enisa.europa.eu/act/cert/support/guide2

GÉANT Association. (2010). Research and Education Networking FAQ - General. Retrieved January 5, 2016, from https://www.terena.org/activities/development-support/r+e-faq/general.html

Hofstee, E. (2006). *Constructing a Good Dissertation*. EPE.

Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003a). *Organizational Models for Computer Security Incident Response Teams (CSIRTs)*.

Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003b). *State of the Practice of Computer Security Incident Response Teams (CSIRTs)*.

Mooi, R., & Botha, R. A. (2015). Prerequisites for building a Computer Security Incident Response capability. In *Information Security for South Africa (ISSA), 2015* (pp. 1–8). http://doi.org/10.1109/ISSA.2015.7335057

Mooi, R., & Botha, R. A. (in press). A Management Model for Building a Computer Security Incident Response Capability. *African Research Journal*, *107*(2).

Petruccione, F., Hazelhurst, S., Høst, G., Lourens, A., McIntyre, C., & Moore, R. (2013). *National Integrated Cyberinfrastructure System: A framework for the establishment and maintenance of a sustainable NICIS*.

Smith, D. (1994). Forming an Incident Response Team. In *Proceedings of the FIRST Annual Conference* (pp. 1–37).

Staphorst, L. (2015). *SANReN Annual Progress Report for 2014/15*.

Wara, Y. M., & Singh, D. (2015). A Guide to Establishing Computer Security Incident Response Team (CSIRT) For National Research and Education Network (NREN). *African Journal of Computing & ICT*, *8*(2), 1–8.

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26*(2), xiii–xxiii.

West-Brown, M. J., Stikvoort, D., Kossakowski, K. P., Killcrece, G., Ruefle, R., & Zajicek, M. (2003). *Handbook for Computer Security Incident Response Teams (CSIRTs)* (2nd ed.). Carnegie Mellon Software Engineering Institute.

Zimmerman, C. (2014). *Ten Strategies of a World-Class Cybersecurity Operations Center*. The MITRE Corporation.