Prerequisites for building a computer security incident response capability

Roderick Mooi*† and Reinhardt A. Botha†
*Meraka Institute, Council for Scientific and Industrial Research
†Center for Research in Information and Computer Security, School of ICT, Nelson Mandela Metropolitan University
Email: RMooi@csir.co.za, ReinhardtA.Botha@nmmu.ac.za

***Abstract*—There are a number of considerations before one can commence with establishing a Computer Security Incident Response Team (CSIRT). This paper presents the results of a structured literature review investigating the business requirements for establishing a CSIRT. That is, the paper identifies those things that must be in place prior to commencing with the actual establishment process. These include characterising the CSIRT environment, funding, constituency, authority and legal considerations. Firstly, we identified authoritative CSIRT literature. Thereafter we identified salient aspects using a concept matrix. The study enumerates five areas of primary business requirements. Finally, a holistic view of the business requirements is provided by summarising the decisions required in each area.**

***Index Terms*—incident response, security team, CSIRT, CERT, establishing requirements.**

I. Introduction

Popular IT news sites [1], [2], security-related conferences [3], [4] and talks of global cyber-war [5], [6] evidence the reality of the information security landscape today. 2014 marked a year of particular significance with Distributed Reflective Denial of Service (DRDoS) attacks on the rise[1] followed by the revealing of critical vulnerabilities in core libraries of systems connected to the Internet. Names like "Heartbleed" (OpenSSL vulnerability), "Shellshock" (Bash vulnerability), and the exploitation of these vulnerabilities,[2,3] show just how fragile this ecosystem really is.

Hacking, virus outbreaks and denial of service attacks are primary examples of computer or *information security incidents*. Formally, an information security incident is defined as

> *"a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security"* [7, p. 3].

The Internet community has adapted to recognise and deal with these incidents. Policies and procedures not only define *normal* operations but should include mechanisms to act on infringement. Ultimately, all mechanisms involve *people* in some sort of team structure and collaboration: individuals cannot fight alone. Therefore, the establishment of a team responsible for incident handling is the preferred approach to establishing an *incident response capability* [8, p. 1].

A Computer Security Incident Response Team (CSIRT) is defined as

> *"an organization or team that provides services and support to a defined constituency for preventing, handling, and responding to computer security incidents"* [9, p. 1].

A CSIRT is a group of information security experts primarily responsible for handling security incidents in an IT environment. These 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. Secondary responsibilities may include incident prevention, advisory dissemination and security consultancy services in order to minimise 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) [10].

The team can be formalised or called together on an ad hoc basis as needed [11]. In addition, a CSIRT can coordinate incident response activities between groups or organisations [8] and even facilitate education and training [12].

II. Research problem

[13] present a number of challenges faced through the authors' experience of establishing a national CSIRT in a developing country. These challenges include: an unclear mandate or mission, lack of management support, finding investments, selecting a revenue model, and interacting with the constituency and external parties. A lack of funding, management support and a clearly defined mission and authority were confirmed as challenges by [11] in a survey among CSIRTs.

A mechanism is needed to address these challenges. There are a plethora of guidelines and processes to follow when setting out to establish a CSIRT, though where to start is not clear. A lot of advice is provided about what aspects to consider without a consistent method or process to follow ensuring that the most important of these *requirements* for establishing a CSIRT are catered for.

[1] https://www.us-cert.gov/ncas/alerts/TA14-017A
[2] http://www.fireeye.com/blog/technical/2014/09/shellshock-in-the-wild.html
[3] https://www.mandiant.com/blog/attackers-exploit-heartbleed-openssl-vulnerability-circumvent-multifactor-authentication-vpns/

This paper therefore presents the first part of a solution to this problem of *where does one start when aiming to establish a CSIRT?* More specifically, this paper examines the business requirements, i.e. the objectives within the organisation [14, p. 61], needed prior to building a CSIRT.

III. Methodology

Standards, recommended practices, guidelines and the like provide useful recommendations for establishing a CSIRT or similar team. The best current practice for the Internet community is documented in RFC 2350 — Expectations for Computer Security Incident Response [15]. SANS 27002 [16] is an ISO-based implementation that covers information security techniques and provides valuable insight to consider when establishing an incident response team and its associated services. The National Institute of Standards and Technology (NIST) provide a guide [17] for handling computer security incidents including incident response team structures, collaboration and services. Finally, two recognised authorities providing guidelines for use when establishing a CSIRT are the Software Engineering Institute at Carnegie Mellon University (CMU-SEI) [8], [18] and the European Network and Information Security Agency (ENISA) [10], [12].

A *comprehensive study of the relevant literature* was performed utilising a concept matrix for categorisation [19] as the foundation for this research. The primary requirements and specific decisions required prior to establishing a CSIRT were then identified and isolated.

This section introduces the primary literature and presents the resulting concept matrix.

A. Primary literature sources

A comprehensive search was performed with the objective of determining the primary sources of literature relevant to CSIRT establishment. The search concepts were therefore selected as:

1) CSIRT or CERT ("incident response team","computer emergency response/readiness team") and
2) establish (create, start, found).

Searches were conducted on ScienceDirect, Scopus, SpringerLink and IEEEXplore using these terms. To ensure that no important publications were missed, Google Scholar was searched using the terms *CSIRT OR CERT OR "Incident Response Team" OR "Computer Emergency Response Team" establish*. To reduce the volume of returned publications, the results were filtered for relevance based on the title followed by the abstract or summary text. Then, as recommended by [19], the processes of going backwards and forwards through citations was utilised to ensure that the final set was as complete as possible. Finally, when no significant new concepts emerged, the primary source of each concept was identified and the search terminated [19, p. xvi].

Reading through the material revealed a pattern of authoritative sources from respected authors. It was found that the main institutions affiliated with these sources include the Software Engineering Institute of Carnegie Mellon University (CMU-SEI) [8], [9], [11], [18] (who established the first CERT in 1988[4]), the European Network and Information Security Agency (ENISA) [10], [12] and the National Institute of Standards and Technology (NIST) [17]. The latest publications from these institutions, filtered for relevance to the business requirements, were selected as the primary sources for this study[5]. Other related sources include the Australian Computer Emergency Response Team (AusCERT) [20] and the University of Auckland (AUCK) with Sun Microsystems (SUN) [15]. The rest of this section presents a brief summary of these sources ordered as in table I. It is important to observe that although there are only a few primary sources here the volume of material is quite large as these articles and reports range from 37 [20] to 291 [11] pages with an average of 141 pages between them (total 1271 pages).

1) Forming an incident response team [20] (AusCERT): Based on the author's experience of building the Australian Security Emergency Response Team (SERT), this paper looks at what it takes to form and maintain an incident response team. Topics include the constituency, policies, information, equipment and tools as well as partner relationships and interactions [20, p. 1].

2) Handbook for Computer Security Incident Response Teams (CSIRTs) [18] (CMU-SEI): Providing guidance on building and running a CSIRT, this handbook has a particular focus on the incident handling service [18, p. xv]. In addition, a basic CSIRT framework is provided covering the mission, constituency, organisational placing and relationships of the CSIRT to other teams. Detailed descriptions of CSIRT services, policies and team operations (including staffing issues) are supplied.

3) Organizational models for Computer Security Incident Response Teams (CSIRTs) [8] (CMU-SEI): This handbook provides guidance on selecting the correct model for an organisation's incident response capabilities. The primary focus is on the organisational model and operational structure of the team. Common CSIRT models with their attributes, respective advantages and disadvantages and typical service offerings are discussed.

4) A step-by-step approach on how to set up a CSIRT [10] (ENISA): This document, provided by the European Network and Information Security Agency (ENISA), covers business management, processes and technical aspects of CSIRT establishment. It provides a definition of a CSIRT, a description of services that can be provided as well as a process to follow for getting started [10, p. 4].

5) State of the practice of Computer Security Incident Response Teams (CSIRTs) [11] (CMU-SEI): A comprehensive survey forms the basis of this technical report intended to present the status quo of CSIRTs across the globe [11, p. xii].

[4] http://www.cert.org/about/

[5] Although some of these references may appear "dated" the foundations are still applicable and provide good academic value particularly due to the authoritative nature of the sources. The most recent references were utilised where possible.

The findings are presented in detail with a summary of what CSIRTs require to be effective. This was complemented by a literature review which includes a basic framework of areas and factors to consider when developing an incident response capability [11, p. 84]. This information is helpful to both new and existing CSIRTs.

6) Good practice guide for incident management [12] (ENISA): Also by ENISA, this more recent guide provides practical information and good practices for managing network and information security incidents. This handbook is especially useful to developing CSIRTs in the establishment phase as it contains guidelines on structuring incident management and, in particular, the incident handling service [12, p. 4].

7) Expectations for computer security incident response [15] (AUCK, SUN): This best current practice Request for Comments (RFC) provides a general framework of what can reasonably be expected of a CSIRT and presents the important subjects that are of concern to the community. A template for CSIRTs is provided as an aid for implementing and communicating the recommendations. Although quite old, this RFC is still used as the basis for defining many CSIRTs. This is evidenced by the results returned of RFC 2350 descriptions when googling *cert OR csirt rfc 2350*, showing the relevance of RFC 2350 to this research[6].

8) Computer security incident handling guide [17] (NIST): This guide from the National Institute of Standards and Technology (NIST) provides recommendations for establishing a successful incident response capability. Incident handling in general is also featured with the primary focus on detecting, analysing, prioritising and handling incidents.

9) Defining incident management processes for CSIRTs: A work in progress [9] (CMU-SEI): This report takes a process-centric approach to identifying the resources and roles required for incident management. The process definitions are accompanied by workflow diagrams and descriptions. The resulting process maps provide a best-practice model outlining the requirements for a successful incident management capability in terms of the primary functions and tasks [9, p. 8].

B. Concept matrix

A concept matrix was used to synthesise the literature (as recommended by [19]). The concepts (or topics) emerged while reading the literature as natural groupings of CSIRT business requirements with the resulting matrix shown in table I. The number of ticks show our perceived strength/influence of the resource, that is, how much it has to say on a topic as reflected in the following sections.

As seen in the table, [20] (AusCERT) and [18] (CMU-SEI) were the most influential sources for this research, making contributions in all areas of the business requirements except for the environment. Two additional publications from CMU-SEI ([8], [11]) and the two from ENISA ([10], [12]) followed with the next highest inputs. In addition, [10] had the highest inputs towards the environmental requirements and [12] had the most to say regarding the constituency.

[6]Examples of the use of RFC2350 include: http://www.ren-isac.net/csirt/ and https://www.cert.at/about/rfc2350/rfc2350_en.html

TABLE I
BUSINESS REQUIREMENTS CONCEPT MATRIX

Source	Environment	Constituency	Authority	Funding	Legal
AusCERT [20]		✓	✓✓	✓✓	✓✓
CMU-SEI [18]		✓	✓✓	✓	✓✓
CMU-SEI [8]	✓✓	✓✓	✓✓		
ENISA [10]	✓✓✓	✓✓		✓✓	
CMU-SEI [11]			✓	✓✓	✓✓
ENISA [12]		✓✓✓			✓
AUCK, SUN [15]		✓✓	✓		✓
NIST [17]	✓	✓			
CMU-SEI [9]					✓

RFC 2350's [15] main contribution was also with the regards to the constituency. The final two sources, [17] and [9], provided inputs towards the environment, the constituency and legal considerations as shown.

IV. BUSINESS REQUIREMENTS FOR ESTABLISHING A CSIRT

Successfully providing CSIRT services requires an holistic approach. Smith [20, p. 32] argues that policies, procedures, equipment, premises, contacts and staff must be established before commencing operations even though it is likely that some of these may be missing or inadequate. To address this problem of ensuring that everything has been sufficiently considered, we need a place to start. The primary business requirements (or organisational inputs) that need to be considered when establishing a CSIRT are thus described in this section.

A. Environment

The CSIRT environment can be defined by the sector which will be served by the CSIRT as well as the geographic region of operations [17, p. 47]. Table II briefly describes the following types and sectors (or *business areas* [8, p. 3]): national, academic, CIP/CIIP, government, military, SME, commercial, internal, vendor and other CSIRTs.

As noted by [10, p. 10], a team may serve more than one sector, with subsequent impact on the scope of the constituency. How these different types of CSIRTs typically fit into the CSIRT hierarchy can be seen in fig. 1. As shown, an individual CSIRT can belong to any (or even more than one) sector. It is important to understand where the CSIRT fits into the national hierarchy and identify the sector early on so that contact can be made with potential partners and coordinators.

The existing organisational structure of the hosting organisation (if any) is regarded as part of the environment. The

TABLE II
CSIRT SECTORS AND TYPES (BASED ON [10, PP. 8–10])

Sector	Serving
Academic	Research and education organisations
CIP/CIIP	Critical Information and/or Infrastructure Protection (energy, transportation, critical ICT infrastructure, etc.)
Government	Government agencies (and sometimes citizens)
Military	Military departments
SME	Small and medium enterprises or special interest groups (usually self organised)
Type	**Serving**
National	Whole country (usually in a coordinating/intermediary role)
Commercial	Commercial services to paying clients
Internal	Hosting organisation only
Vendor	Specific hardware or software vendor (also called a Product Security Incident Response Team (PSIRT))
Other	Any type or sector not fitting into the above

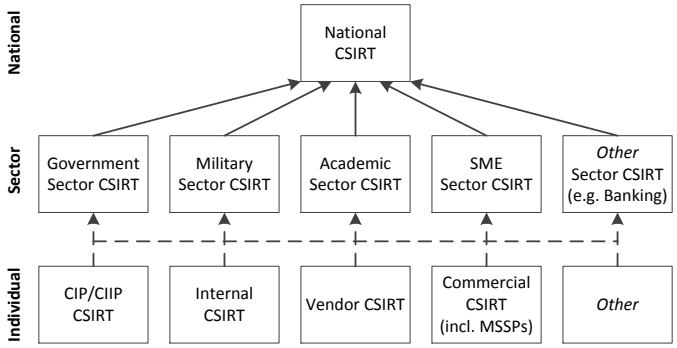

Fig. 1. National CSIRT hierarchy — types and sectors

organisational requirements will determine whether the CSIRT will be established as an independent entity, embedded in an existing organisation, distributed between campuses and/or consist of volunteers from the community [10, pp. 21–24].

Thus, the environment comprises the CSIRT sector, geographic area and organisational structure. The environment reveals the constituency and provides input to the CSIRT team model and services.

Some questions and implications related to the organisational environment include the following:

- Will the CSIRT be established as an independent entity with its own management and employees?

This leads to what is known as the *independent* model. This model requires the most human resources as the CSIRT needs to be fully staffed including administrative roles such as an office manager as well as an accountant, legal consultant and communications officer [10, p. 21].

- Will it be embedded within an existing organisation?

The *embedded* model caters for the re-use of existing resources which can be shared with the CSIRT team; it is also useful for scenarios where the CSIRT workload is uncertain (i.e. staff can be temporarily assigned to the CSIRT) [10, p. 22]. This lowers overheads and also allows the team to focus on CSIRT activities with a supportive base.

- Will it be distributed between independent campuses?

Referred to as the *campus* model, this structure is used mostly by research and education CSIRTs with a core team coordinating various university or campus internal teams [10]. As argued by [10, p. 23], operating the CSIRT in a distributed campus model (rotating core services between campus teams) results in lower costs of operation for the central team. Possible challenges with this approach include the level of authority and a conflict of interest for campus staff with other responsibilities.

- Will it consist of volunteers from the community?

The *voluntary* model represents an informal group of people with an interest in information security working together for the common good (sharing advice, recommendations, etc.) [10, p. 24]. As the commitment of the participants is crucial to successful operations, this model is risky for environments where participants have other obligations or priorities meaning that security-related work could "fall through the cracks". It can therefore be labelled a best-effort or ad-hoc approach and is generally not regarded as a formal CSIRT model [8].

The answers to the above questions will influence the decisions made in the following sections.

B. Constituency

The constituency is defined as:

> *"the group of users, sites, networks or organisations served by the team"* [15, p. 17].

The constituency must be defined clearly and early on [10]. This is important because the people served by the CSIRT need to know that they have one and the team needs to know who it is serving [20]. Furthermore, partners and other CSIRTs need to know who the constituency is so that reports and coordination requests can be appropriately directed [20, p. 4]. A constituency can either be internal (within the same organisational structure as the CSIRT) or external; centralised or distributed (across cities, countries or even time zones) [8]. The constituency can be as broad as a whole region or country

or as narrow as a single branch of an organisation to any other logical grouping. Government, banking, and research and education network beneficiaries are examples of constituencies served by sector-specific CSIRTs [11].

To identify the constituency, the CSIRT environment (or industry sector) and geographic region is determined [17, p. 47].

Thereafter, the constituency can be defined by [12, p. 14]

- IP address range,
- domain name,
- autonomous system number(s), and/or
- free text.

IP address range, domain name and free text are most often used by research and education CSIRTs; AS number(s) are typically used by ISP CSIRTs [12, p. 15]. Free text is clear but can make it difficult to determine if a host (identified by IP address) is in fact part of a specific constituency or not.

Active, reliable and trusted contacts should be established as soon as the constituency is defined [12]. Refer to [20, p. 5] for an idea of how to go about this.

C. Authority

> *"Authority describes the control that the CSIRT has over its own actions and the actions of its constituents related to computer security and incident handling activities"* [8, p. 37].

There are four types of authority relationships that a CSIRT can have over its constituency [18, p. 15]:

1) full — the CSIRT can undertake any actions or decisions on a constituent's behalf;
2) shared — the CSIRT can influence the decision-making process;
3) indirect — the CSIRT can exert pressure on a constituent (e.g. an ISP can disconnect services if actions are not taken); or
4) none — the CSIRT can only advise but not enforce actions.

The level of authority should be supported by management and clearly conveyed to the constituency [8, p. 38]. It has been argued that the lower the CSIRT authority, the *more likely* it is that constituents will report incidents and seek assistance [20, p. 9].

D. Funding

Funding has been highlighted in section II as a challenge when establishing a CSIRT. The available budget influences the resources that can be utilised by the CSIRT, especially people. Funding considerations can be divided into sources of income and sources of expenditure. Costs are primarily determined by the hours of operation and staff salaries [10, p. 18].

More specifically, *costs* are incurred for [11, pp. 53–54]:

- start-up equipment and infrastructure,
- staff salaries and benefits, and
- operational and other personnel expenditures (e.g. travel).

These all need to be budgeted for during the initial planning phase of the CSIRT.

Revenue models include the use of existing resources, membership fees, a project subsidy, or charges on a per-use basis [10, p. 19].

Most CSIRTs are funded by a parent organisation (e.g. university, NREN or government) [11]. A combination of revenue models is also possible, for example, core CSIRT services can be funded from existing resources and then premium services can be offered on a pay-per-use basis. More detailed funding strategies for CSIRTs are available from [11, p. 54].

E. Legal considerations

Finally, the CSIRT should be sensitive to local laws and regulations which may include specific requirements for reporting and confidentiality [15, p. 12]. An awareness of laws in other countries, with which the CSIRT cooperates, is also useful [12].

CSIRTs should be aware of laws related to [10], [11]:

- telecommunications and IT services,
- data protection and privacy,
- evidence handling,
- data retention, as well as
- notification requirements (e.g. law enforcement, national CSIRT).

The specific laws relevant to the CSIRT will depend on the CSIRT environment and could include statutory and common or case laws [11, p. 112]. More information on legal issues is available in [18, p. 51-58] and [20, pp. 11–12]. Legal experts should be consulted when considering the legal requirements as this is an area where specialised skills and knowledge are essential.

The following section discusses the detailed decisions required in each of the business areas.

V. Decisions and links for the business requirements

The previous section highlights the following questions which need to be answered prior to establishing a CSIRT.

A. Environment

To determine the environment, as argued in section IV-A, the following questions need to be answered:

1) What *type* of CSIRT
   a) Is it a national, sector or individual CSIRT?
      This affects the scope of operations, constituency, reporting, authority and CSIRT services selection. A national CSIRT has a broader constituency and mandate than an individual company CSIRT. The national CSIRTs focus will be on coordination, trends and incidents of national interest/relevance rather than individual cases. A company CSIRT will be concerned with protecting the company's infrastructure and information and should be more individual-focused.

b) To which *sector* does the CSIRT belong (if applicable)? [Table II].
Different sectors have different priorities. For example, banking sector CSIRTs will be concerned about protecting credit card information and online banking security. Academic sector CSIRTs will be concerned about protecting student records and intellectual property theft. A military CSIRT may be subject to stringent compliance and secrecy conditions.

c) Alternatively, which *type* of individual CSIRT? [Table II]
This alludes to suitable funding models. A commercial CSIRT typically charges for CSIRT services utilising membership fees and/or paid for services while an internal CSIRT is typically funded by the host organisation.

Some typical examples of CSIRT types include:

- An NREN CSIRT is an academic sector (research and education) CSIRT.
- A bank CSIRT is an internal individual CSIRT (stand alone or under a banking sector CSIRT).
- A university CSIRT is an internal individual CSIRT (usually under an academic sector CSIRT).
- A law enforcement CSIRT could be an internal, government sector or other CSIRT depending on the specific environment.

The South African Cybersecurity Hub described by [21] is an example of a national CSIRT.

2) What *geographic area* will be covered by the CSIRT?
A global or regional CSIRT has very different implications on the constituency and services, for example, than an internal CSIRT for a single site. These include timezones (hours of operation), languages, viable services and other issues. In addition, a CSIRT can span single or multiple cities, provinces or even countries. The geographic area has a significant influence on the team model selection.
3) Which *organisational model(s)* will the CSIRT use? Will it be

- independent — with its own management and employees,
- embedded — hosted in an existing organisation,
- independently distributed among campuses, or
- voluntary — made up of team members from the community?

Answering these questions provides a mission for the CSIRT and subsequently *reveals* the constituency. The environment additionally *scopes* the legal considerations by revealing applicable laws and regulations (see section V-E).

These associations are summarised in fig. 2. Clearly, determining the environment is the first step for establishing a CSIRT.

Fig. 2. Links from the Environment

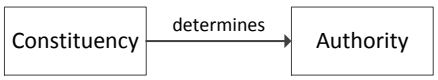

Fig. 3. Link from the Constituency to Authority

B. Constituency

Once the CSIRT sector and geographic region (i.e. *environment*) is identified, the constituency can be defined by one or more of the following (see section IV-B):

- IP address range,
- domain name,
- autonomous system number(s), and/or
- free text.

Together with the environment, the constituency *influences* the services that will be provided by the CSIRT. Their needs, skills, expertise, etc. all have an effect. The constituency also provides insight into the type of systems and network(s) the CSIRT needs to support as well as possible funding models. For example:

- If the constituency are the employees of a single organisation then central funding is likely.
- If applicable, would the constituency be willing and able to pay for CSIRT services?
- Should this be a government-funded CSIRT?
- Does a business case need to be made to secure management support and/or to apply for funding?

As explained next, the constituency is highly correlated to the authority that the CSIRT may have.

C. Authority

The nature of the constituency *determines* the type of authority which the CSIRT may have and exercise. Figure 3 shows this link. Once the type of authority — full, shared, indirect or none (section IV-C) — has been determined, it needs to be communicated back to the constituency. As argued previously, CSIRT management staff must support the authority relationship.

Authority affects the services which can be provided by the CSIRT. For example, it is not possible to provision some CSIRT services, e.g. incident tracing and intrusion detection, without some level of authority [20, p. 9].

D. Funding

As part of establishing a CSIRT, the *source(s) of funds* need to be identified [10, p. 19]. Section IV-D provided four main options: existing resources, paid membership, project subsidy and/or paid for services. Clearly, income relies on the environment as well as the nature of the constituency (e.g. whether they would be willing to pay for CSIRT services). These links are shown in fig. 4.

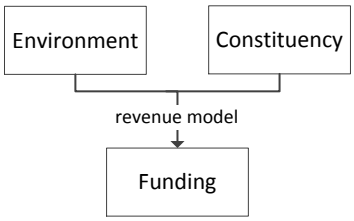

Fig. 4. Links to Funding/Budget

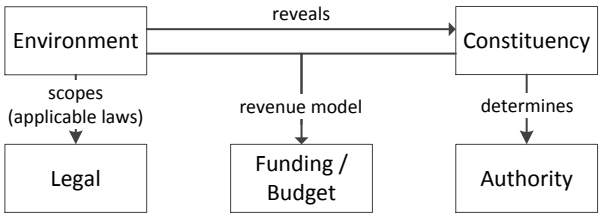

Fig. 5. Relationships between the business requirements

In section IV-D it was argued that the main contributors to CSIRT expenses are the *hours of operation* and *staff salaries*. Conversely, the available budget determines *how many people* can be employed (and at which *skill* level). Thus, the team model and staffing decision go hand-in-hand with funding, determining the primary costs. The other area influenced by funding is the *equipment* required by the CSIRT. Although these two areas fall outside of the business requirements, their consideration is a logical progression following the business decisions.

E. Legal considerations

As noted in section IV-E, relevant laws are dependent on the CSIRT environment. A global CSIRT requires a different understanding of laws and regulations as compared to a CSIRT operating in a single country (though at least an awareness of the most important laws affecting external partners is required). This relationship to the environment is shown in fig. 2.

When establishing a CSIRT, legal advice should be sought on the relevant laws detailed in section IV-E. In South Africa for example, the following legislation should be considered:

- the Electronic Communications and Transactions (ECT) Act 25 of 2002,
- the Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) 70 of 2002,
- the Protection of Personal Information (POPI) Act 4 of 2013, and
- the Cybersecurity Policy of South Africa (currently in draft form).

These acts and policy can be accessed through the download links provided in table III[7].

VI. Combining the business requirements and summary of decisions

The business requirements need to be addressed at an organisational level prior to establishing a CSIRT. As revealed in the previous sections, the initial decisions that must be made are

1) determining the *environment*,
2) figuring out who the *constituency* of the CSIRT will be,
3) understanding the subsequent *authority* relationship,
4) selecting a suitable *funding* model, and
5) identifying and applying any relevant *laws and regulations*.

[7]Note that this list is not intended to be exhaustive, some amendments have been made which should be investigated for relevance and the identification and implications of legislation should always be done in consultation with legal experts.

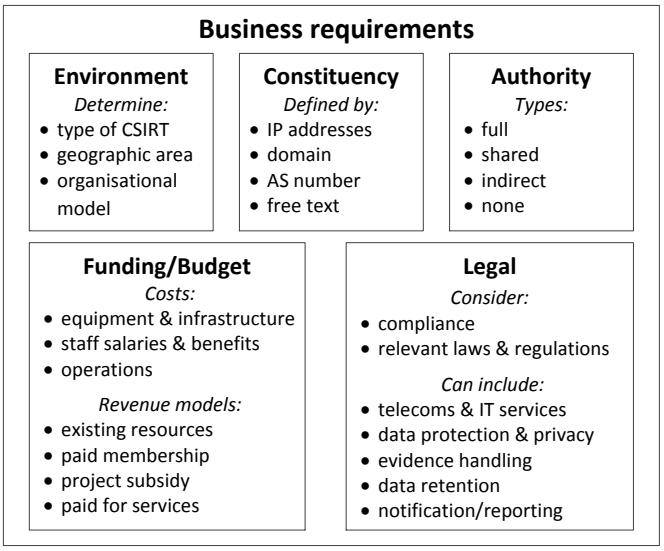

Fig. 6. Summary of the business requirements

These decisions and their inter-relationships are shown in fig. 5. Authority and legal considerations can be directly determined from the definitions of the environment and constituency as explained earlier. Funding represents the material "resource" for equipping the CSIRT.

The primary decisions that need to be made in each of these areas are summarised in fig. 6. For the environment, these decisions include determining the type of CSIRT, the geographical area covered and the organisational model. The constituency is then determined from one or more of IP address range, domain, autonomous system and/or a free text description. Following that comes the authority of the CSIRT. Will it have full, shared, indirect or no authority over the constituency? Costs can be estimated based on required equipment and infrastructure, staff salaries and benefits, as well as operational expenses. This leads to a budget which can be used to motivate for funding. The revenue model can be determined from the environment and constituency as one or more of the following: existing resources, paid membership, project subsidy and/or paid for services. Finally, relevant laws and regulations must be identified and studied for impact.

TABLE III
SAMPLE OF APPLICABLE LEGISLATION FOR A SOUTH AFRICAN CSIRT

Act/Policy	Link (verified 10 April 2015)
ECT Act	http://www.gov.za/documents/electronic-communications-and-transactions-act
RICA	http://www.gov.za/documents/regulation-interception-communications-and-provision-communication-related-information--13
POPI Act	http://www.gov.za/documents/protection-personal-information-act
Cybersecurity Policy	http://www.gov.za/documents/electronic-communications-act-south-african-national-cybersecurity-policy-draft

Compliance to these laws and regulations must be included in CSIRT activities going forward. Only once these decisions are made should one proceed with the establishment process.

VII. CONCLUSION

Experience has shown that establishing a CSIRT is all but a straightforward process [13], [20]. The aim of this paper therefore, is to address the possible deficiencies and challenges by identifying and correlating the business requirements that need to be considered upfront when establishing a CSIRT. To do this, we conducted a review of related literature to identify, firstly, the primary sources, and secondly, the core CSIRT business requirements. The resultant concept matrix (table I) clearly shows that none of the selected primary literature sources addresses all of the areas with respect to the business requirements. In addition, the different sources each emphasise diverse areas of consideration (with varying levels of detail). Potential implementers of a CSIRT are therefore exposed to the real danger that some of the pre-establishment issues might not be considered or only partially addressed.

An oversight, e.g. not selecting a revenue model, might jeopardise the complete implementation of the CSIRT. Rework, resulting in delayed implementation and cost overruns might be another outcome. For example, selecting services without considering the constituency and related authority of the CSIRT may result in impractical offerings.

This paper presents a comprehensive list of the identified business requirements together with associated decisions in five areas: the environment, constituency, authority, funding and legal considerations. Key questions are posed and motivated to assist with making the required decisions. The relationships between these areas are explored as an indication of the order with which the decisions should be addressed — thus feeding into the subsequent areas for consideration. This allows for better planning and a more methodological approach to establishing a CSIRT.

Once the business requirements have been "satisfied" and the viability to continue establishing the CSIRT determined, the next step would likely be determining the CSIRT services and staffing the initial team. These are topics for future research.

REFERENCES

[1] D. Goodin. (2015, Apr.) Just-released WordPress 0day makes it easy to hijack millions of websites [updated]. [Online]. Available: http://arstechnica.com/security/2015/04/27/just-released-wordpress-0day-makes-it-easy-to-hijack-millions-of-websites/

[2] B. Donohoe. (2015, Apr.) VMware fixes Java information disclosure vulnerability. [Online]. Available: https://threatpost.com/vmware-fixes-information-disclosure-vulnerability/112007

[3] H. Dalziel. (2014, Mar.) Information security conferences of 2015. [Online]. Available: https://www.concise-courses.com/security/conferences-of-2015/

[4] Black Hat. (2015) Welcome to Black Hat USA 2015. [Online]. Available: https://www.blackhat.com/us-15/

[5] S. Ranger. (2014) Inside the secret digital arms race: Facing the threat of global cyberwar. [Online]. Available: http://www.techrepublic.com/article/inside-the-secret-digital-arms-race

[6] Editorial Board. (2015, Apr.) Preparing for warfare in cyberspace. [Online]. Available: http://www.nytimes.com/2015/04/28/opinion/preparing-for-warfare-in-cyberspace.html

[7] SANS, "Information technology - Security techniques - Information security management systems - Overview and vocabulary," Standards South Africa, Standard 27002, 2009.

[8] G. Killcrece, K.-P. Kossakowski, R. Ruefle, and M. Zajicek, "Organizational models for computer security incident response teams (CSIRTs)," Carnegie Mellon Software Engineering Institute, Tech. Rep., December 2003.

[9] C. Alberts, A. Dorofee, G. Killcrece, R. Ruefle, and M. Zajicek, "Defining incident management processes for CSIRTs : A work in progress," Carnegie Mellon University, Tech. Rep., October 2004.

[10] ENISA, "A step-by-step approach on how to set up a CSIRT," ENISA, Tech. Rep., 2006.

[11] G. Killcrece, K.-P. Kossakowski, R. Ruefle, and M. Zajicek, "State of the practice of computer security incident response teams (CSIRTs)," Carnegie Mellon Software Engineering Institute, Tech. Rep., October 2003.

[12] ENISA, "Good practice guide for incident management," ENISA, Tech. Rep., 2010.

[13] M. Grobler and H. Bryk, "Common challenges faced during the establishment of a CSIRT," in *2010 Information Security for South Africa conference*, 2010.

[14] L. Hunnebeck, *ITIL® Service Design*. London: The Stationary Office (TSO), 2011.

[15] N. Brownlee and E. Guttman, "Expectations for computer security incident response," RFC 2350 (Best Current Practice), Jun. 1998. [Online]. Available: http://www.ietf.org/rfc/rfc2350.txt

[16] SANS, "Information technology - Security techniques - Code of practice for information security management," Standards South Africa, Standard 27002, 2008.

[17] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide," NIST, Special Publication 800-61. Revision 2, Aug. 2012.

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

[19] J. Webster and R. T. Watson, "Analyzing the past to prepare for the future: Writing a literature review," *MIS Q.*, vol. 26, no. 2, pp. xiii–xxiii, Jun. 2002.

[20] D. Smith, "Forming an Incident Response Team," in *FIRST Annual Conference proceedings*. AUSCERT, 1994, pp. 1–37.

[21] M. Grobler, J. van Vuuren, and L. Leenen, "Implementation of a cyber security policy in South Africa: Reflection on progress and the way forward," in *ICT Critical Infrastructures and Society*, ser. IFIP Advances in Information and Communication Technology, M. Hercheui, D. Whitehouse, J. McIver, William, and J. Phahlamohlaka, Eds. Springer Berlin Heidelberg, 2012, vol. 386, pp. 215–225.