SA NREN CSIRT workshop

@Kopanong

26-27 May 2015

Workshop notes compiled by facilitator:

Awie Vlok

avlok@sun.ac.za

CSIR Editors/Contributors:

Roderick Mooi

roderick@sanren.ac.za

Renier van Heerden

renier@sanren.ac.za

(SANReN CA)

Executive summary

With the quantum increases being experienced in digital media developments, universities and science councils are becoming attractive targets for malicious activities that leave these institutions and their intellectual assets increasingly vulnerable. Legislative compliance issues are also contributing to the need for a scaled up capability to pursue compliance and security in the form of a Computer Security Incidence Report Team (CSIRT) to serve the higher education and research community.

A two day workshop attended by nearly 60 managerial and technical representatives from this community discussed and designed a range of options to deal with the emergent collective requirement which formed the basis for the formulation of a minimalist level business model as a starting point with multiple future optional pathways depending on its performance, client satisfaction and the evolving digital security requirements landscape.

The alternative to this proposition would for be for each of +-50 institutions to make their own individual arrangements for establishing threshold capability which would leave the national system of innovation even more vulnerable.

The workshop concluded with a unanimous decision to put forward a business case to institutional decision makers for conditional approval of funding for the activity.

Table of Contents

Abbreviations

AS2018	Autonomous System 2018 (TENET)
ASAUDIT	The Association of South African University Directors of IT
AUP	Acceptable Use Policy
BCM	Business Continuity Management
CCU	Crime Control Unit
CIO	Chief Information Officer
CSIRT	Computer Security Incident Response Team
DHET	Department of Higher Education
DST	Department of Science and Technology
FTE	Full Time Employee
HE	Higher Education
HESA	Higher Education South Africa
ISP	Internet Service Provider
ICT	Information and Communications Technologies
IDS	Intrusion Detection System
IP	Intellectual Property / Internet Protocol
IT	Information Technology
LAN	Local Area network
SMS	Short Message Service
NOC	Network Operations Centre
NREN	National Research and Education Network
OLA	Operating Level Agreement
PURCO	Purchasing Consortium Southern Africa
POPI	Protection of Personal Information
R&D	Research and Development
RSA	REN Services Agreement
SANReN	South African National Research Network
SANReN CA	SANReN Competency Area (research group of CSIR Meraka Institute)
SAPS	South African Police Service
SIG	Special Interest Group
SLA	Service Level Agreement
SLARG	SLA Reference Group
SOC	Security Operations Centre / Service Operations Centre
TENET	Tertiary Education and Research Network of South Africa

1. Introduction

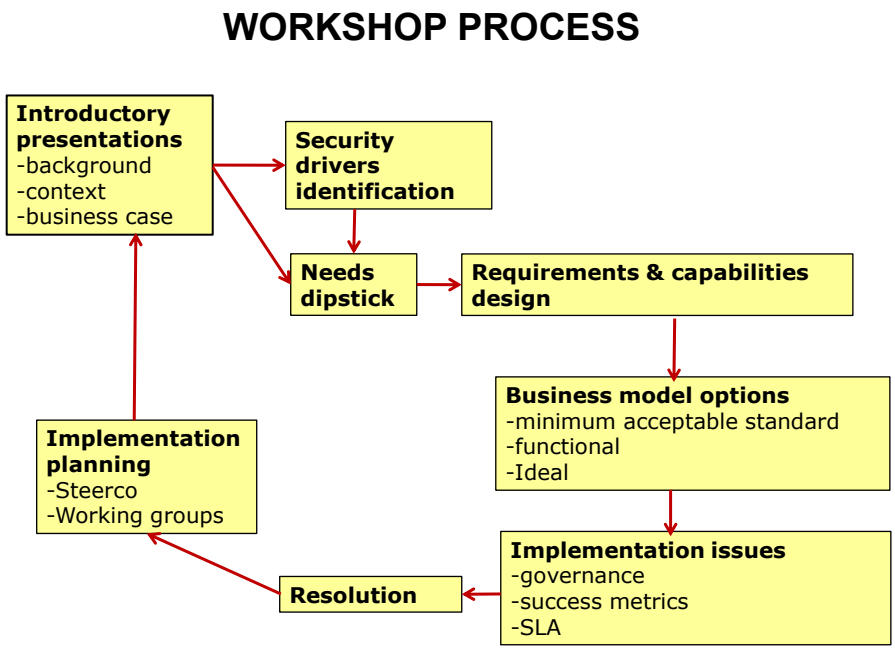
In light of the evolving information security threat to the higher education and research community, the SANReN CA and TENET invited CIOs and IT Directors from universities and science councils in South Africa to participate in a two-day facilitated workshop to explore the establishment of a Computer Security Incident Response Team (CSIRT) for the South African NREN.

2. Scope of workshop

The scope and purpose of the workshop was to discuss the need and model for a CSIRT for the constituency of the South African NREN with the following sub-objectives:

1) Determine the community's need or desire for such a team.
2) Assuming a decision to proceed with a CSIRT (Service, structure, staffing and funding addressed)
3) Establishment of a steering committee and working groups to implement the CSIRT focussing on areas such as policies & procedures, tools and technologies, partners and legal aspects (e.g. POPI Act compliance).

To ensure full delegate participation and to solicit collective wisdom that would culminate in a proposition for broader stakeholder decision making and support, the following process was followed:



3. Dipstick survey

At the start of the proceedings before any of the presentations, delegates were asked to answer a few questions anonymously to indicate their current perceived levels of the computer security threat and the intensity of response required. The results are shown in the following table:

DIP STICK SURVEY: COMPUTER SECURITY INCIDENT REPORTING

n52	A	B	C
At present the computer security threat is...	**Not serious**	**14 Volatile**	**34 Very serious**
My 5 year view on computer security risks is that it will...	**1 Decrease**	**9 Not change**	**49 Increase**
I believe our protection efforts should be ...	**1 Relaxed**	**2 left as is**	**49 Intensified**
Computer security protection activities should be...	**11 Centralised**	**34 Mixed**	**7 Decentralised**
The responsibility for computer security should sit with..	**21 Individuals**	**34 Institution**	**4 Suppliers**
The cost of computer security should be covered by...	**Users (20%), Institution (20%), ISP (20%) Apps suppliers (40%) [NOT IT-5]**		

Delegates were also invited to share any concerns and/or suggestions of relevance to the possible establishment of a CSIRT that they would like to be considered. These were captured as follows:

Delegate concerns:

- We are vulnerable - hacking of crucial information by unknown people may ruin our security credibility
- Universities not taking Information Security serious – "it is IT department's issue" – seen as "grudge spend" (challenges in recruiting for the role) – not sure we can get funding for mandate
- Top down enforcement / imposing control
- Lack of knowledge, resources, computer literacy, security awareness
- Users and institutions cannot cope
- ISPs need to provide higher level service
- Privacy protection
- BCM for individual security
- Loss of IP
- Can we protect against state attacks?
- Lack of awareness (people unaware of risks/assume all is correct)
- Where will this group reside?
- Corporate governance of information security
- Clarity of purpose and agenda from where this will be driven
- Need consensus and direction on way forward
- Security incident management (beyond reporting)
- Possible over reaction or no action extremes
- Activities affecting smaller institutions too (POPI...)
- As education institution to balance freedom with security to encourage and enhance research and learning with secure stable systems (not impede)
- Social networks

Delegate suggestions:

- Provide users more control if security validated
- Compulsory reporting to enable proper stats for risk assessment and awareness raising
- Raise awareness (start at senior management of organisation and down to users)
- Must be in consensus
- Community certified tools
- More workshops & discourse on the subject
- Link funding to enterprise risk register
- Cooperation with other similar entities at all levels to pool resources
- Use commercial products too (to avoid repeating us all activities)
- Information security awareness campaign across all universities
- Should be marketed to the whole organisation
- Determine what should/can/must be secured – avoid too much control
- Have dedicated responsibilities /dedicated personnel for security
- Compliance policies
- If institutions take this seriously it can work – we need to communicate
- Capacity building for skills and skilled staff for sustainable adoption
- Communication and collaboration
- Pro-active defence, not waiting

It is clear that delegates regard the computer security threat as increasing and that intervention is required to protect the information assets of the institutions and people involved.

4. Evolving computer security landscape

Introductory presentations covered a range of topics to provide delegates with information to allow for critical thinking and informed decision making during the CSIRT design phase.

Dr Renier van Heerden: Welcome address

Prof Barry Irwin : Cyber security status quo

- South Africa's Submarine cable network
- Telecoms landscape
- Challenges (more traffic, user expectations, increased threat and increased capacity)
- Research areas
- Rhodes University observations – "we are a juicy target for exploitation"
- Collaborative security (insights to threats, reputation, collaboration, performance and usability)
- The problem – Africa reputation
- Challenges and collaborative fixes (community building, information sharing, reporting, communication and awareness
- Trust and community essential
- Future vision elements

Dr Kamil Reddy: POPI compliance overview

- Importance of compliance and what it involves
- Basic concepts and definitions of POPI and personal information
- POPI's 8 conditions – "it is impossible to have privacy without security"
- Information Officer responsibilities
- Direct marketing/SPAM
- Transborder/crossover flows
- Power of the Regulator
- POPI interventions
- Risks and threats of attacks
- Contingencies and current status
- POPI (S.19) requires organisations to do the following to secure personal information:
  - take "reasonable technical and organisational measures"
  - "identify all reasonably foreseeable internal and external risks"
  - "establish and maintain appropriate safeguards against the risks identified"
  - "regularly verify that the safeguards are effectively implemented"
  - "ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards"
  - have due regard to "generally accepted information security practices and procedures"

Roderick Mooi and Dr Renier van Heerden:

- Background and context
- Why a CSIRT and why now?
- Risks and impact of incidents
- Threats (ISO 27001 and ISO 22301), vulnerabilities and threat agents
- Common attack patterns, enumeration and classification
- SANReN/TENET risk assessment scenarios
- Business case for SA NREN CSIRT
- CSIRT services types and details
- Survey 1 results (2012)
- Potential CSIRT models
- Funding and services options
- Survey 2 results conducted at the workshop during the first day.

5. Security drivers and required response

Technology road mapping principles were applied to identify the key future drivers (blue shaded) that would impact on security capabilities of the research, innovation and higher education fraternity, thereby creating the intervention space (yellow shaded) required to be filled by a CSIRT. ICT trajectories reflect the unprecedented levels of technological advancements affecting the operations of these institutions while "market" refers to the strategic priorities of these institutions. Compliance legislation was referred to that need to be taken into account during the CSIRT design and development phases.

CSIRT Technology Roadmap

ICT trajectories	**Connectivity security; Ubiquitous high speed open access, cloud storage; decentralisation; online library, internet of things; BYOD, access anywhere, hires video services, enhanced research & learning e.g. cloud services, big data, interactive high resolution video**
Market changes	**Innovation from research, more student output by leveraging technology, knowledge management, collaborative research; blended learning, subsidy driven research; big data as method of research; generation and consumption of massive data volumes; rapid development & related security issues caused by going too fast; coping with unanticipated/unpredictable trends**
Customer Require-ments	**Security protection (info, research, mobile data); access (24/7, security, single sign-on, free bandwidth, self provisioning of any service, run any research on the network, diversification & differentiation; total unrestricted anywhere access, complete service, invisible (embedded); integrated and interoperable; more demand on infrastructure (more faster, reliable); cloud scale (handle data like Google/ Microsoft with $1b data centres); "disappearing ICT" (aka under cover or it just works); lower cost but better reliability and quality; agility**
CSIRT Offerings needed	**Day 1 alerts, notifications, announcements, 24/7 call centre, awareness and education,security audits, security training, security awareness (skills and knowledge transfer), technology assessments, cost-effective model to meet important needs.**
CSIRT Capabilities	**On campus services (detection & scanning, assessments, reporting, skills transfer & certification, assist with remediation, follow up/review**
Infra-structure	**SOC, Lab (training, testing, evaluation), scanning platforms, software, repository of information and fixes; partnerships networks**

From the ensuing conversation it became clear that multiple levels of response may have to be established in future and that the urgent establishment of at least a minimal capacity would be advisable to deal with the evolving threats and from where alternative pathways may be co-crafted by those involved.

Delegates also emphasised the need for members of this "community" to share knowledge on this topic. Erica Ferreira invited delegates to send her an e-mail (erica.ferreira@up.ac.za) if they would like to join a PoPI SIG which was formed under the auspices of ASAUDIT (The Association of South African University Directors of IT). The aim of the PoPI SIG is to draft a Code of Conduct for the HE Sector of South Africa. The Code will be presented to HESA for submission to the Information Regulator. The Code of Conduct will be a statement of the Universities undertaking to comply with the PoPI Act, but will also contain exemptions to be requested from the Regulator. A guidelines document is being prepared to accompany the Code of Conduct. While the Code will be compulsory and binding, the guidelines will contain recommendations on how universities will meet the requirements of the PoPI Act. Membership of the SIG is open to staff from all divisions in all universities. Interested representatives from science councils are also welcome to contact Erica to see how they can participate.

6. The proposed business model option

Small groups populated the Osterwalder Business Model Canvas templates at three levels that would accommodate an essential or minimalist level (A), an intermediate functional adequacy level (B) and a future ideal level model (C).

Delegates unanimously agreed that the Model A should become the core proposition to be tabled at executive decision making levels for approval so that the envisaged CSIRT can be established.

Model A is summarised below while Model B and Model C are summarised in the table below.

Business Model A:

1) Value proposition (*expressing an overall view of the bundle of products and service on offer*)

Enabling institutions to secure their information artefacts by providing timely security intervention for the shared SANReN network (every LAN under AS2018)

Services:

- Awareness & training (optimise coordinate, outsource, in-house?)
- Security alerts vulnerability (credibility)
- Incident handling (light weight, communications, using existing NOCs)
- Knowledge & best practice sharing
- Facilities and Special Interest Group (SIG)

2) Core capabilities (*Outlines the capabilities to run the business model)*

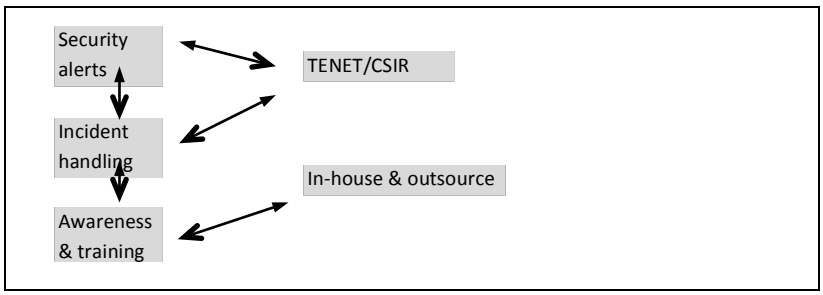
- Alerts and warnings
- Intrusion detection
- Incident handling (off site light weight/ minimum)
- Vulnerabilities advisories
- Awareness and training
- Announcements

3) Partner network (*Outlines network of cooperative agreements with other entities)*

- Interaction with NREN, CSIRTs and SA National CSIRTs (international and national)
- TENET & "CSIR"
- Other NRENS & CSIRTs
- Suppliers (Training, technology vendors)
- SAPS CCU
- PURCO
- Interaction within own community

4) Value configuration (*Describes the arrangements of activities and resources***)**

- Embedded/ distributed
- Clarify roles and responsibilities to detect, collect, analyse, consolidate, deliver and disseminate
- Services & agreements with partners
- Recognise & formalise affiliations with others CSIRTs
- Contracts – outside suppliers
- TENET/CSIR recognition/affiliations with CSIRTs



5) Customer relationship (*Explains the relationships of the firm with its customers*)
   - Collaborative, advisory, supportive, consultative based on mutual trust
   - TENET as legal body – RSA & AUP
   - Community (Web, forums, annual meetings, e-mail and SMS alerts)
   - Incident handling (call centre system)

6) Distribution channel (*Describes the channels for communicating with customers)*
   - Public (NREN public list)
   - Restricted list with red, orange, green indicators
   - Incident handling as per existing security contacts
   - Anonymous reporting ?

7) Target customer (*Describes the customers to whom value is offered)*
   - SA NREN community
   - ICT departments
   - Internal clients (TENET)

8) Cost structure (*Summarises the monetary requirements of running the business model*)
   - Staffing:
     - Awareness – in house CSIRT resource (senior manager)= 0.5 FTE
     - Security alerts – at least 1.5 senior engineer = 1.5 FTE
     - Services – Senior = 0.5 to 1 FTE; and Junior = 1-2 FTE
   - Overhead/operations:
     - Training (no central procurement; central quotes & bargaining)
     - Equipment
     - Access to CSIR/DST R&D and infrastructure
     - Invisible overhead 7% (covered by savings on TENET input costs OR DHET?)
     - Memberships
     - Office (coffee/tea, stationary, etc)
   - Capex?
   - Work station/office space
     - Consider pros and cons of location (SANReN (CSIR), TENET, Institution)

9) Revenue streams (*Identifies the revenue streams through which money is earned*)
   - Several options discussed
     - Government funding (sectional CSIRT)
     - Subscription models

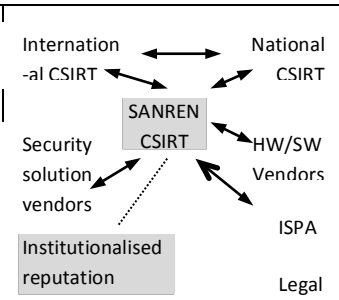
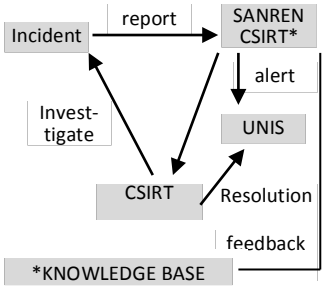
- Professional service offerings (like commercial)
- Non-cash resources (human capital and real estate)
- Donations

- Preferred model is a mix of
  - Services based
  - TENET savings rather than additional funding
- Avoid subsidy/cross-subsidised models

7. Alternative business models

While Business model A was accepted as basis for recommending immediate deployment of the CSIRT, models B and C were described as attractive longer term dispensations based on current understanding of the situation and trajectories but not affordable at present.

	Option A	Option B	Option C
	Minimalist-essential	Intermediate - Functional	Advanced global good practice – Ideal
	<R2m per annum	<R6m per annum	<R16m per annum
1) Value proposition	Enabling secure information artefacts. -Alerts and warnings -Incident handling (off site light weight) -Vulnerabilities advisories -Awareness and training Intrusion detection	Provide security management to higher education and research community through rapid, cost effective services based on understanding NREN requirements: -Alerts & advisory -Intrusion detection -Incident reporting, handling & response coordination -Vulnerability handling -Announcements -Technology watch -Awareness -Information dissemination -Education and training -Artefact handling -Audits (bi-annual) -IDS -Security reports (on demand) -Knowledge base creation & population -Call centre (24/7) -Legal compliance	Global player with full range of services, expert staff and independent international speakers: -24/7/365 efficient response and on-site support/remote support -SLA -Business continuity (redundancy) -virus signatures -flexibility ito customised bundles -risk management -skills transfer & competencies Development -Certification & accreditation. -business audits & risk assessments -SOA -Policies
2) Core capabilities	- Alerts and warnings - Intrusion detection - Incident handling (off site light weight/ minimum) - Vulnerabilities advisories - Awareness and training - Announcements	-Scanning -Anomaly detection -Pattern recognition -Trending , base lining -Reporting and resolution -Skills transfer	Full compliment of staff Full services range by best practice experts Top level hardware, tools & research/testing laboratories, reliable systems infrastructure

3) Partner network	-All institutions -TENET & "CSIR" -Other NRENS & CSIRTs Suppliers (Training, technology vendors) -SAPS CCU -PURCO -Interaction within own community		Best practice suppliers & institutions, other CSIRTs, vendors, national CSIRT, auditors private & government partnerships, local & international partnerships
4) Value configuration	-Embedded/ distributed -Clarify roles and responsibilities to detect, collect, analyse, consolidate, deliver and disseminate -Services & agreements with partners -Recognise & formalise affiliations with others CSIRTs -Contracts – outside suppliers -TENET/CSIR recognition/affiliations with CSIRTs		Experts, laboratories and intelligent knowledge base configurations, independent contributors, embedded, dedicated team, SLAs and OLAs.
5) Customer relationship	-Extended REN agreement -Governance -SLAs	-Trust based -POPI -Advisory relationship for legal, technical, security	Trusted, reliable, mandated. Aligned institutional policies, managed SLA & contracts; customer engagement; communication & control mechanisms. Service management and reporting
6) Distribution channel	Physical & electronic via ICT departments (like TENET info flow)	- E-mail - Social media - Web portal - Discussion groups (web conference of meetings)	Awareness campaigns, print, e-mail, web portal, telephone, remote access, communication strategies, proactive, response, mobile Apps, reporting/reviews.
7) Target customer	- ICT departments - Internal clients (TENET)		All staff and students, stakeholders, research institutions, NREN users.
8) Cost structure	-Direct(staff) -Indirect (infrastructure)		Infrastructure, staff, marketing, training, hardware, software, membership/ vendor support, maintenance, training, certification, licensing, travel
9) Revenue streams	-See options discussed -Preferred model mix -Avoid subsidy model		Expertise led income via customised services, deliver extra services, consulting, training, seminars to broader market. Core funded by DST/ DHET.

Workshop delegates discussed the possibility of reducing Option A to even more of a minimalist option such as a R1m per annum two person operation and domain experts indicated that this would introduce a sub-critical capacity level that would not be able to deliver the required service to the estimated 50 member community.

8. Way forward

Following a discussion introduced by Duncan Grieves the workshop decided unanimously to adopt a "Fast tracking" approach rather than the more conventional and originally anticipated approach of establishing a steering committee and working groups. This consensus approach suggests the development of a business case to be presented at a follow-up TENET SLARG (SLA reference group) meeting later this year. The case will ask for conditional commitment based on a majority of institutions opting in.

In terms of specific actions the implications are:

Action 1: Use the workshop results to consolidate a clear concise compelling business case (two pages executive summary plus reference material) to be tabled at the appropriate decisions making forum for approval (Roderick Mooi & Dr Renier van Heerden in close collaboration with reference group institutional helpers and SANReN CA/TENET Heads).

Action 2: Present the business case to IT Directors for conditional approval of the CSIRT service. Conditional implies choices based on number of incidents, number of institutions and service quality. (Duncan Grieves and Leon Staphorst).

9. Concluding remarks

Delegates were asked to share their opinions of the two day workshop from which the following conclusions could be drawn:

- Good attendance suggest the importance of the topic
- This was a well timed and necessary platform for this community
- Highly informative

Senior leadership at the workshops concluded by thanking everyone for their participation and emphasising:

- The high quality of inputs by the presenters
- Strong engagements of delegates
- Strong convergence of views on the urgency and starting point.

AV; 2Jun2015