PREPAREDNESS AND RESPONSE TO CYBER THREATS REQUIRE A CSIRT

Jaco Robertson[1], Marthie Lessing[2], Simon Nare[3]

CSIR, Defence, Peace, Safety and Security

[1]jrobertson@csir.co.za

[2]mlessing@csir.co.za

[3]snare@csir.co.za

PO Box 395

Pretoria, South Africa

0001

Abstract: The military's decision to move from proprietary software to commercially available software leaves the military's Information Technology security vulnerable and potentially unprotected. To be sufficiently prepared to these threats, the military should establish a Computer Security Incident Response Team (CSIRT). This will allow them to protect against and respond to, threats to their information infrastructure.

Keywords: CSIRT, CERT, computer security, military, critical infrastructure, exploits, vulnerability, commercial and proprietary software

1. Introduction

The military is increasingly relying on commercial and civil information and communications infrastructure. Traditionally, the military developed proprietary systems and ran them in isolation, achieving security through obscurity. However, with the military's tendency nowadays to rely rather on commercial and civil systems, they do not have the inherent security of proprietary solutions. Accordingly, the military is exposed to the same threats and risks that plague the public.

The common approach to these threats in civil society is to establish a Computer Security Incident Response Team (CSIRT). A CSIRT's main mission is to respond to threats against an organisation's critical information infrastructure. Threats against such infrastructure take on a myriad of forms and specialised skills are required to manage it. The CSIRT foster and develop these required skills within, whilst expanding an organisation's capability to respond to network security incidents.

This paper proposes that the military should invest in the establishment of a CSIRT. This would allow skilled information security specialists to focus on information and system security threats, whilst personnel of the military can focus on their duties.

2. Motivation for having a military CSIRT

According to Joel Bagnal, executive vice president of the United States government operations at Detica, the increasingly complex Information Technology environment means that many existing cyber-defences are no longer fit for its purpose. *"… All organisations*

need new ways of managing the growing risks and threats to national and international cyber-security… Our cyber-security defences are, in many cases, no longer adequate in today's environment, making us potentially vulnerable to sophisticated attacks" [1].

With the proliferation of commercially available software, especially with the vast penetration of Microsoft's Windows operating system, a class break has become a major threat to any organisation using commercial software. A class break is a vulnerability that holds for a whole class of system. The implication of such a break is that, if one system displays a specific vulnerability, all the systems of that class displays the same vulnerability. Therefore, should a hacker be able to exploit one system's vulnerability, by default he would be able to exploit all the other systems of that class' vulnerability. Schneier explains this: *"… Class breaks mean that you can be vulnerable simply because your systems are the same as everyone else's. And once attackers discover a class break, they'll exploit it again and again until the manufacturer fixes the problem (or until technology advances in favour of the defender again)"* [2].

Schneier elaborates on the severity of an automated class break: *"… Class breaks give attackers leverage because they can exploit one vulnerability to attack every system within a class. Automation gives attackers leverage because they can exploit vulnerabilities millions of times"* [2]. In 2004, the Titan Rain (Chinese hackers targeting United States military secrets) launched a class break against the United States government. The hackers first exploited vulnerabilities at the United States Army Information Systems Engineering Command at Fort Huachuca in Arizona. A few hours later, they exploited the same vulnerability in computers respectively at the Defence Information Systems Agency in Virginia, California and Alabama [3].

As a consequence of relying on the same systems as commercial organisations, the military opened itself to the same risks and threats that civil society deals with. Should a hacker be able to exploit commercially available software used by civilian organisations, the hacker would be able to use the same method to exploit the military's system. This happened in 2003, when a vulnerability identified in Microsoft's Internet Information Server 5.0 and Windows 2000 lead to a hacking attack on the United States military [4]. Where computer systems used to be heterogeneous (each organisation developed its own proprietary system), a hacker exploiting a specific computer system would have little or no effect on other organisations, including the military.

Where computer systems nowadays tend to be more homogenous (many organisations use the same commercially available systems), the risk of a class break becomes more real. Following the military's use of these commercial systems, they are now also at risk. The net affect is that the cumulative time and effort that attackers spend on developing exploits for the mass market can be used in a more malevolent targeted attack, focusing specifically on the military. For instance, WabiSabiLabi (http://www.wslabi.com) is a marketplace that auctions and sells vulnerabilities and their exploits to the highest bidder. This poses a very real risk that an exploit can be sold that was developed for a system, which the military is also using. A person or government with malicious intent might buy this exploit for the sole purpose of attacking the military. However, nothing prevents the military CSIRT from buying the exploit themselves, to proactively develop a fix for the specific vulnerability.

The converse is true as well. Due to the economics of scale, more time and effort is spent on countering these common threats. Should a patch be released to remedy a specific class break vulnerability, both the civilian organisations and the military will benefit from this. Thus, following an attack on commercial software, the military can continue to focus on their

military duties, whilst the military CSIRT can focus on handling the software vulnerability. Although it remains the responsibility of the software vendor to create a patch for the vulnerability, the CSIRT is responsible for identifying potential vulnerabilities and whether vendor released patches are applicable to the military's system. The CSIRT will play an important role in determining the risk of applying a patch versus the risk of the vulnerability.

Applying a patch could bring with it its own risks, it might create a new vulnerability (that could be worse than the vulnerability it fixes) or it might make the system function unpredictably. It might also be that the vulnerability, although it exists, is not a threat in the military's context. The risks will have to be weighed up against each other.

The CSIRT will either use their existing skills set, or develop a new skill set within the military CSIRT to focus on the identification of software vulnerabilities. Since the military uses commercial software and not proprietary software anymore, the military will develop public skills and not obscure skills on obscure proprietary systems.

To compound the problem further, the military not only makes use of commercially available systems, but also rely on civil information infrastructure and systems. Consequently, a failure on the civilian side could render military systems unavailable, or severely impaired. To counter this, closer cooperation with civil society is required. If a civil system fails or is under threat, or poses a threat to a military system, the military should be able to rely on those system custodians to cooperate with or assist the military.

This reliance requires building trust and a human network of relationships that can be called into affect. A CSIRT is the ideal vehicle to accomplish this trust relationship. At its core, a CSIRT needs to network with other CSIRTs. This is very important because threats can be international and incidents can happen across borders. Thus, a CSIRT that networks closely with other teams overcomes the differences in languages, rules, laws, regulations and security cultures. The establishment of a CSIRT generates a security culture within the CSIRT community, where all parties work together with a *"… my security depends on your security"* mindset [5].

The CSIRT community builds on two pillars: collaboration and a web of trust. Collaboration ensures that relevant parties share their experiences and resources, build on best practices and enforce the idea that security is not a competitive environment, but rather a joint effort. The web of trust further enhances the collaboration. A CSIRT needs to trust that another CSIRT is not itself an attacker, and that they do not have any malicious intent. CSIRTs can only achieve this mutual trust relationship by regular interaction and collaboration with other CSIRTs [5].

Since the establishment of CSIRTs is a worldwide trend, with many of them already in existence. The structure and functioning is well known and accordingly security specialists are comfortable to work for a CSIRT. This has the benefit of allowing the military to attract qualified security specialists.

3. Typical threats and risks to information infrastructure

Before either the military or a CSIRT can be prepared for cyber threats or respond to it, it is necessary to take cognisance of most prominent threats and risks to the information infrastructure. The number of incidents has increased at an alarming rate in recent years and this trend is set to continue, especially with the vast number of new Internet users coming online from developing countries such as China, India and Brazil.

3.1 Viruses and worms

A virus is malicious code that replicates itself by infecting other files on the same system. Viruses do not spread themselves from system to system, but requires the operator of the system to spread it. This can happen when an individual forwards an infected email to a number of recipients. The code may be extremely malicious to the extent of destroying the system, or it may be as benign to display only a message [6].

Worms are similar to viruses. However, this malicious code has the capability to spread themselves via networks, without the assistance of operators. Creators of computer worms exploit bugs and vulnerabilities in operating systems and networking services to enable this.

3.2 Trojans

Software Trojans are typically programs that appear to be legitimate, but contain malicious code. It may imitate the name, or look and feel of a legitimate program normally found on a computer system. Alternatively, a trojan may perform a function that the operator might find of use, for example a downloaded screensaver. However, similar to the original Trojan horse, the malicious code hides within the functional software. The user, deceived by the appearance of the software, willingly downloads the program or install the necessary files, only to unleash a virus, worm or backdoor into the system. This makes them extremely dangerous [7]. The name for this type of malicious code is borrowed from the legendary attack on the city of Troy. The ancient Greeks built a huge wooden statue of a horse, secreted soldiers within and presented it as a gift to the Trojans. After nightfall, the soldiers crept out of the statue, unlocked the city gates and allowed their fellow Greeks to attack the Trojans.

3.3 Botnets and Distributed Denial of Service Attacks

A denial of service attack is an attack that deliberately denies a system access to, or from providing a resource or service. This typically takes the form of flooding a system with fraudulent requests for a service, causing the system to overload. This may render a system unable to service legitimate requests. An alternative technique is to send a large amount of emails to the victim system, resulting in the interruption of the victim's email account or mail servers [8].

A distributed denial of service attack (DDoS attack) takes it one step further by getting multiple agents to attack the same target, making it impossible to stop the attack by eliminating a single attacker. Attackers use botnets with great effect to accomplish this. Botnets are networks of computers infected with bots. A command and control server controls the bots remotely. The biggest known botnet is the 'Storm Botnet', with an estimated 250 000 to 1 million infected machines [9].

The risk to the system does not only lie with being attacked by a botnet, a huge concern to be sure, but the risk is higher of becoming part of a botnet. Bots infect systems by making use of worms or trojans. Once infected with a bot, a computer will become part of the botnet and controlled by an attacker, usually for nefarious purposes. Via the command and control servers, the attacker can command the bots to crack passwords, act as spam relays and launch coordinated attacks, to name a few. Apart from the lost productivity of the computer system, the infected machines become accomplices to the act. Bot infected computers are also known as 'zombie computers' or 'zombie' for short.

3.4 Vulnerabilities and Exploits

Systems may have weaknesses, implementation flaws, holes and unforeseen conditions that hackers can exploit to gain access to the system, disable the system or subvert the system. An exploit can take any form: a virus, worm, bot, trojan or a tool that allows an attacker access to the system. It used to be that these vulnerabilities did not come to light until an exploit has been developed that takes advantage of the vulnerability. These days a great deal of effort is being put into finding vulnerabilities before attackers do.

The moment someone makes the existence of an exploit public, the vulnerability of all affected systems magnifies. The exploit publicises the existence of the specific software's vulnerability, putting all organisations that use that specific software, at risk. The susceptibility of these systems is elevated since software vendors usually only start with a patch for the specific vulnerability, after the exploit becomes public knowledge. This leaves a number of systems vulnerable until relevant personnel apply the patch to the compromised system.

Due to the severity and magnitude of this threat, it is of great importance to invest time and effort in finding vulnerabilities in an organisation's system and fixing it before cyber criminals can develop an exploit. An exploit that is released the same day or before a vulnerability is discovered is now known as a zero-day exploit. It has now become an arms race between system developers and exploit developers. Exploit developers have even started reverse engineering patches to identify the vulnerability. They then develop an exploit, in the hope of using it before administrators can patch the system. Figures from the Computer Emergency Response Team Coordination Centre (CERT/CC) shows that at least 4 129 vulnerabilities were reported in 2002 alone [10].

3.5 Spam

Spam can be defined as unsolicited email, sent either in mass by commercial sites to recipients who have not requested any contact, or email sent intentionally to annoy or harass the recipient. This can overload a computer system, forcing it to fail or be unresponsive [11]. Although spam as such is not an attack, it does constitute a threat, since machines infected with worms, Trojans or bots can turn that machine into a spam relay. This increased spam activity can then completely cripple the network.

3.6 Attacks against the systems

A targeted attack by an attacker with an agenda is by far the most dangerous attack on a system. The attackers are usually skilled hackers, motivated by agendas varying from terrorism or political inclination, to financial or personal gain. The attacks are in general extremely difficult to pick up, since it happens over a long period of time. The attacker will spend weeks if not months, trolling the system for vulnerabilities, biding their time waiting for the most opportune moment to attack. As these attackers are generally extremely skilled, they leave behind very little trace, if any at all, that they broke into the system.

Opportunistic attackers on the other hand are generally a lot less careful. These attackers typically attack a system for the adrenalin rush or notoriety. They generally leave behind some sort of message proclaiming their superiority, or notifying the system administrators of the vulnerability themselves.

Either attack can be most devastating to an organisation. Not only can it cripple the organisational resources, but it can be detrimental to the staff morale and leave the organisation in disrepute.

4. Background

The military is increasingly relying on information infrastructure and systems for their activities. It used to be that fewer services meant fewer avenues of attack, but systems are increasingly hosting a myriad of services and protocols over a network. This increases the complexity of a system's security, requiring specialised and focused skills. There has also been a shift away from obscure proprietary systems to more readily available commercial systems.

The network-centric approach to warfare is the military's incarnation of the information age's concepts. Network-centric warfare uses computers and communications to link people through information flows that depend on the interoperability of systems [12]. This, however, pushes the security of these systems to the top of the priority list. The military staff is now dependant on the availability of this data. Unavailability and the potential that the enemy could get hold of this are extremely severe risks [13].

4.1 Computer Security Incident Response Team

4.1.1 What is a CSIRT

A CSIRT is an organisation or team that provides services and support to a defined constituency for preventing, handling and responding to computer security incidents. In essence, a CSIRT is a team of experts focused on IT security. They are there to respond immediately to an IT security related incident [14].

4.1.2 Role of CSIRT

The role of a CSIRT can be vast, ranging from providing Information Technology security services to their constituents, including prevention, detection, correction, training and education [15]. Accordingly, it is best to describe its role in respect to reactive services, proactive services and security quality management services.

Reactive services generally apply after an incident has taken place. This includes issuing alerts and warnings to the CSIRT's constituency, handling and responding to the specific security incident and handling any related system vulnerabilities [14]. The most prominent role of a CSIRT is to respond to a security incident and reverse the potential damage caused by it.

What makes a CSIRT's incident response superior to that of normal support staff, is the fact that they focus on Information Technology security. A CSIRT does not handle everyday user queries, and can therefore ensure a timeous and correct response to the incident. In addition, a CSIRT can analyse the incidents, and accordingly identify vulnerabilities or circumstances that lead to the incident. The specialised response team will then be able to patch the system, preventing a repeat of the incident. The distribution of these patches to other systems prevents a series of recurring incidents. CSIRTs might even be able collect forensically sound evidence in case there is the need for a criminal investigation.

Proactive services control a specific situation and prevent an incident from occurring. The most prominent proactive service is to make announcements of new criminal techniques to

educate the constituents beforehand [14]. A CSIRT would be negligent in its duties if it did no prevention. A CSIRT need to ensure that all systems are up to date, and that all known vulnerabilities are fixed, patched or protected. A CSIRT should also make a proactive effort to detect intrusions and new vulnerabilities. This means that CSIRT employees have to constantly investigate and research the Information Technology security discipline. In addition, they need to monitor the system closely to make sure they know as soon as an incident takes place. Proactive services also include training and education.

Lastly, s*ecurity quality management services* include awareness building and security consulting [14]. A CSIRT is also required to build a relationship with other CSIRTs. Seeing that most systems these days are closely coupled, a CSIRT cannot stand on its own. It has to rely on other CSIRTs to reach where it cannot. It should maintain contact with CSIRTs in other countries in order to be aware of new threats and respond quickly to an emerging threat.

4.1.3 Who are its constituents?

A CSIRT's constituent is the user base that a CSIRT has to protect against an incident. A CSIRT needs to define its constituents based on services it has to offer and the clients it will be offering the services too. It is necessary to define a CSIRT's constituent clearly to ensure that the response team focuses on those systems that are critical to the constituents. In other words, a CSIRT cannot respond to anybody's security incidents. Furthermore, they cannot respond to systems that are outside of their control, or that of their constituents i.e. they cannot respond to other people's systems.

However, a CSIRT has to build relationships with other CSIRTs, and accordingly can assist their fellow CSIRTs in a crisis. In a military context, a CSIRTs constituent would be the critical information infrastructure that the military requires to be secure, and up and running during time of war and peace.

4.1.4 History

Although the first research on secure military computer systems was already published in 1973 [16], it was only in the late 1980s that security response teams was taken seriously. In 1988, an *ad hoc* response team was established, in response to the release of the first internet worm, consisting of experts from MIT, Berkeley and Purdue. This team developed fixes for the software bugs and procedures for the eradication of the worm. Once the threat of the worm subsided, the Defence Advanced Research Projects Agency (DARPA) decided to institutionalise the concept of an internet emergency response team. Carnegie Mellon University's Software Engineering Institute accordingly established the CERT/CC near the end of 1988 [17].

In 1990, the Forum of Incident Response and Security Teams (FIRST) was established as a network of individual computer security incident response teams that work together on a voluntary basis to deal with computer security problems and their associated prevention. This forum aims to promote better communication and coordination amongst response teams [18]. FIRST currently have a membership of 193 teams across 42 countries.

Another coordination centre is the European Network Information Security Agency (ENISA). This agency serves as a centre of excellence in network and information security, and stimulates the cooperation between the public and private sectors. ENISA coordinates European CSIRTs and helps to establish new CSIRTs [19].

Amongst others, these CSIRT coordination centres enable any country, organisation or military to establish their own CSIRT, focusing specifically on their own needs.

4.1.4 Establishing a CSIRT

Once an organisation have decided to establish a CSIRT, the organisation need to either set up an internal task team to do so, or cooperate with a fellow CSIRT or a company assisting organisations in establishing their own CSIRT. The AusCERT suggests a number of steps to follow that can lead to the successful establishment of a CSIRT:

- Establish mandate, mission, define constituents
- Define services and scope
- Determine resources required
- Define funding model
- Study existing models
- Build a library of reference material
- Attend conferences and training, existing staff
- Hire experts or train new staff
- Run in trial mode
- Liaise with other CSIRTS, build relationships
- Get feedback [20].

There are numerous online resources to assist with the establishment of a CSIRT. For instance, there is an ENISA step-by-step guide available at http://www.enisa.europa.eu/cert_guide/index_guide.htm and the Handbook for CSIRTs at www.cert.org/archive/pdf/csirt-handbook.pdf. The CSIRT community itself are very keen to help establish new CSIRTs, assisting with programs, training and mentoring of new response teams.

5. Benefits of having a military CSIRT

The military needs to focus on keeping the country's citizens safe from terrorists and hostile countries or entities. By establishing a military CSIRT, the military benefits in three distinct ways, and a number of indirect ways.

Firstly, as explained earlier in this paper, a CSIRT handles all Information Technology security incidents on behalf of the military. This leaves the military to focus on their priority: protecting the country and its citizens.

Secondly, by establishing a CSIRT specifically for the military, the military can inspire the necessary confidence to protect the country adequately. A military that cannot keep its own infrastructure safe from threats and attacks, cannot be counted on to protect the country's infrastructure successfully.

In what was referred to as *"… the biggest military computer hack of all time",* Gary McKinnon is accused of causing more than $700 000-worth of damage by hacking into 97 American military computers at the Pentagon, NASA, the United States army and the navy. In addition, the United States charged McKinnon with stealing 950 passwords and deleting files at Earle naval weapons station in New Jersey [21]. Although he is not associated with the attacks, it is believed that McKinnon sufficiently crippled the United States defence systems in the wake of the 9/11 attacks, leaving the military system vulnerable [3].

Lastly, a military can only be successful if the warfare is uninterrupted. This implies that the military can rely on certain critical information infrastructures during wartime, with no interruptions. Should this infrastructure become unstable or even unavailable, it might jeopardise the war effort, potentially causing serious losses or even loosing the war.

Indirectly, a CSIRT can help the military to have a centralised coordination for Information Technology security issues within itself. This centralisation allows for specialised handling of and response to Information Technology incidents, assisting users to recover quickly from security incidents [22]

The North Atlantic Treaty Organisation (NATO) is an alliance of 26 countries from North America and Europe that are committed to safeguard the freedom and security of its member countries by political and military means. NATO recently started with the establishment of its CSIRT, called the NATO Computer Incident Response Capability (NCIRC). In addition to the normal CSIRT duties, the NCIRC focuses on three specific subject areas: technical expertise and standard operation procedures for analysis of specific computer incidents and intrusion detection system events, forensics and law enforcement, and cyber defence exercises [23]. NATO recently launched the Virtual Silk Highway project, which aims to equip all participating countries with CSIRT technology. Although NATO does not formally require all member countries to establish their own CSIRTs, their example shows the importance of the matter. Their initiative improves cooperation between member countries by creating a CSIRT national contact point, and serves as an example of how a CSIRT can contribute to the success of the military.

To summarise, a military CSIRT can handle all Information Technology security incidents on behalf of the military. Therefore, CSIRT can contribute to the military's efficiency by ensuring that the military has sufficient uninterrupted resources and critical infrastructure, allowing the military to focus on their duties, and not on matters totally unrelated to the war, such as viruses that can potentially cripple the infrastructure.

6. Conclusion

Military organisations around the world seem to believe that their Information Technology and critical infrastructure is secure, but a closer audit of their network architecture, software and hardware, present a gloomy picture on how internally prepared for cyber attacks they are. As long as the military is using e-mail, the internet and commercially available systems, they run the same risk as the rest of the civilian technology infrastructure. An impact on the military infrastructure will affect their internal operation, which will in turn influence their ability to render ICT services to their internal stakeholders. It therefore follows that once there is a disruption to the internal operation of the military, the consequence could affect their fulfilment of their mandate.

The SANDF Philosophy on Information Warfare makes it clear that the military can no longer operate effectively without information infrastructure: "… *Africa, and hence South Africa (and the South African National Defence Force) cannot escape the impact of the Information Age. It is therefore both a national and military strategic objective to leverage the advantage posed by modern communication, computer and information systems, and to mitigate the vulnerabilities introduced by the presence and use of these systems*" [24]. Accordingly, they will have to act on the challenges it brings.

In conclusion, as long as the military is using e-mail, the internet, civilian information infrastructure and commercially available systems, they run the same risk as the rest of us. They are part of the interdependent network, a part of the global village. It is recommended, nay imperative that they establish a CSIRT as part of their risk mitigating strategy.

References

[1] Williams, I. (2008). *Current cyber-security defences 'ineffective'*. http://www.vnunet.com/vnunet/news/2219331/cyber-security-ineffect. Accessed 24 June 2008.

[2] Schneier, B. (2006). *Beyond Fear*. Boston: Springer Science+Business Media (pp. 94-99).

[3] Espiner, T. (2005). *Chinese hackers breach US military defences.* http://software.silicon.com/security/0,39024655,39154524,00.htm. Accessed 24 June 2008.

[4] Lemos, R. (2003). *Microsoft flaw leads to military hack.* http://news.cnet.com/Microsoft-flaw-leads-to-military-hack/2100-100. Accessed 24 June 2008.

[5] Ito, Y. (2008). *Setting CSIRTs in Africa Region*. www.afnog.org/afnog2008/conference/talks/AfNOG-Setting_Up_CSIRTs_in_Africa_Region.pdf. Accessed 15 June 2008.

[6] WordNet. (2008). *Computer Virus.* http://wordnet.princeton.edu/perl/webwn?s=computer%20virus. Accessed 25 June 2008.

[7] Kruse, WJ. & Heiser, JG. (2002). *Computer Forensics – Incident Response Essentials.* Boston: Addison-Wesley.

[8] Seth, K. (2007). *Cyber crimes and the arm of Law - An Indian perspective.* Cyber Security and Threats CyST' 2007. http://www.sethassociates.com/pdfs/Presentation-cyst%202007-final.ppt#257,1,Cyber Security and Threats- CyST'2007. Accessed 28 January 2008.

[9] Krebs, B. (2007). *Just how bad is the Storm Worm?* http://blog.washingtonpost.com/securityfix/2007/10/the_storm_worm_maelstrom_or_te.html. Accessed 25 June 2008.

[10] Furnell, SM. (2003). Vulnerability exploitation: the problem of protecting our weakest links*, Computer Fraud & Security.* Elsevier. Volume 2003, Issue 11. Pp 12- 15.

[11] Author Unknown. (2003). *Terminology: Spam.* http://index.realcartu.com/frames/s.html. Accessed 25 June 2008.

[12] Wilson. C. (2004). *Network Centric Warfare: Background and Oversight Issues for Congress*. Congressional Research Service, The Library of Congress

[13] Tiboni, F. (2004). *Army rebuilds networks after hack attack*. http://www.fcw.com/print/10_31/news/83986-1.htm. Accessed 26 June 2008.

[14] Killcrece, G. (2003). *Security Professionals Workshop: Creating a CSIRT.* http://net.educause.edu/ir/library/pdf/SEC0302.pdf. Accessed 25 June 2008.

[15] Author unknown. (2003). *Background on CSIRTs and CSIRT Co-operation*. Resource document, The European Computer Security Incident Response Team Network. https://www.ecsirt.net/cec/background/index.html. Accessed 28 February 2008.

[16] Payne, B. (2006). *History of Computer Security Research*. http://www.bryanpayne.org/research/history.php. Accessed 26 June 2008.

[17] Howard, JD. (1997). *An Analysis of Security Incidents On The Internet 1989 – 1995*. http://www.cert.org/research/JHThesis/Chapter3.html. (Accessed 23 June 2008).

[18] Author Unknown. (Nd). *FIRST History*. http://www.first.org/about/history. Accessed 25 June 2008.

[19] ENISA. (2006). *Activities.* http://www.enisa.europa.eu/pages/01_03.htm. Accessed 26 June 2008.

[20] Smith, D. (1995). *Forming an Incident Response Team*. http://www.auscert.org.au/render.html?it=2252. Accessed 25 June 2008.

[21] Harris, G. (2008). *US accuses Gary McKinnon of hacking crime.* Times Online. technology.timesonline.co.uk/tol/news/tech_and_web/article4186428.ece. Accessed 25 June 2008.

[22] ENISA. (2008). *The benefits of having a CSIRT*. http://www.enisa.europa.eu/cert_guide/pages/05_01_03.htm. Accessed 25 June 2008.

[23] ENISA. (2007). *NCIRC NATO Cyber Defence Workshops.* http://www.enisa.europa.eu/cert_inventory/pages/05_03.htm. Accessed 26 June 2008.

[24] Forrest, A. (2004). *SANDF Philosophy For Information Warfare*. Council for Scientific and Industrial Research. Internal document: Information Warfare Philosophy.