A Whitepaper Prepared by
Sense of Security

Cyber Security – for the Not for Profit (NFP) Sector

Version No: 1.0

Document No: WP-CS-NFP-12-4-1

April 2012

Sense of Security is an Australian based information security and risk management consulting practice delivering industry leading services and research to organisations throughout Australia and abroad. Our strategic approach to security provides you with a capability to assess your risk and deliver qualified guidance on how to protect your information assets. We provide expertise in governance & compliance, risk assessment, strategy & architecture through to, assurance & technical security testing.

Sense of Security - Compliance, Protection and Business Confidence

Sense of Security Pty Limited
National Call | 1300 922 923

Sydney
Level 8, 66 King Street
Sydney, NSW 2000, Australia
ABN: 14 098 237 908

T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455
info@senseofsecurity.com.au
www.senseofsecurity.com.au

Melbourne
Level 10, 401 Docklands Drive
Melbourne, VIC 3008, Australia
ABN: 14 098 237 908

T: +61 (0) 3 8376 9410
F: +61 (0) 2 9290 4455
info@senseofsecurity.com.au
www.senseofsecurity.com.au

Table of Contents

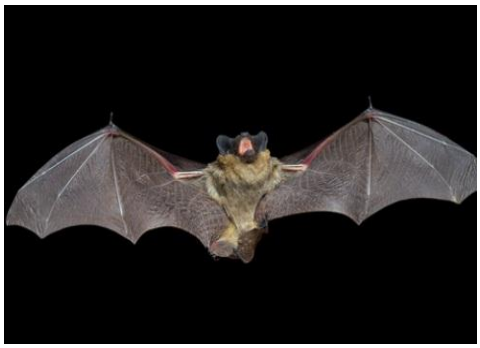
The modern Not for Profit (NFP) organisation is operating in a highly engaged and dynamic environment reaching out to numerous and varied sectors of business and the community. Through interaction with long term subscribers to individual donors, corporate partners, and even international visitors to these shores, the NFP sector has become exposed to an increasing number of cyber security issues as a result of business and operational activities. However, not all NFP's are in a strong position to understand their exposure let alone protect themselves from the associated risks.

This paper aims to address, in a high level yet straightforward manner, essential issues that the NFP sector should be considering and addressing given the extensive and costly technical and operational investments developed and implemented by the NFP. In the highly regulated and compliance driven environment of fundraising, the NFP organisation stands at the coalface of the ever changing and challenging business environment that is now seriously affected by cyber security.

1. What is Cyber Security

Extensive media coverage relating to cyber terrorism, hacking attacks and cyber attacks have become commonplace. All such attacks against organisations and people target confidentiality, integrity or availability of information. In general these attacks reflect the fact that the world is becoming increasingly inter-connected with a high demand for data accessibility and availability across many channels. The internet renders such attacks being precipitated from anywhere in the world.

Cyber attacks are launched, and many are successful, because organisations and people are incredibly vulnerable to attack due to flaws in the components that make up any system - people, process and technology.



While there certainly is an element of well-funded groups, cyber criminals and organised crime, cyber attacks are not limited to elite and powerful groups. Whilst the sophistication of attacks is increasing to defeat new technologies, significant damage can be caused by untrained people with access to the tools and time to use them; like the self- taught hacker truck driver who allegedly destroyed the data of some 4,000 organisations in one fell swoop.[1]

Who are the attackers? Attacks can generally be attributed across groups with certain motives and capabilities.

- Script kiddies - launch attacks for thrills, opportunistic and interested in determining how far they can compromise systems but with no clear attack objective.
- Hacktivisits - have an agenda of causing reputational damage to a group they are targeting by causing online damage and limiting ability to perform business. Protests have moved from placard waving to discrete or distributed attacks against organisations with serious and rapidly escalating effects. Attacks could include defacing web sites, to the full scale denial of service aimed at choking the availability of systems and resources, effectively grinding business to a halt.
- Organised crime – groups intent on launching attacks for financial gain. Such groups could focus on the NFP industry because NFP's hold data with market value, including, personally identifiable information on people, their demographics, disposable income and credit card information. This information can be used for financial gain either directly through fraudulent transactions or by selling stolen details onwards, not to mention money laundering scams or the theft of intellectual property.

[1] http://www.zdnet.com.au/distributeit-claims-evil-behind-hack-339319324.htm

- At the top end of the scale are state sponsored attacks. Whilst unlikely to affect the NFP industry, these attacks are focused on gaining political and economic advantage.

The implications of attacks from any of these groups not only cause financial loss and potential regulatory and compliance nightmares, they can also lead to reputational and credibility damage in the market place potentially alienating donors. In short, loss of merchant facilities could be a direct consequence of a data breach whereby the NFP would no longer be able to process any donations through a credit card channel. However, the effect of reputational damage may be longer lasting with diminished confidence in the community to contribute to campaigns.

2. Business Centric, Not System Centric

Many organisations struggle to protect themselves because they are not adequately prepared, having out-dated and ineffective strategies.

The modern organisation is multi-dimensional and the NFP sector is no different. This means that information (data) is frequently available at different layers and locations within the organisation. Organisations need to understand their data and protect their business rather than view their systems in isolation.

Think of a beehive. The bees business is to make honey and protect the queen bee. While there might be honey in particular cells of the honeycomb, they don't protect individual cells. The bees protect the hive, protecting the queen bee and all the honey. In the same way the NFP organisation needs to know where its honey is.

You need to know your data (honey):

- Do you make/initiate/produce data or do you receive it?
- Where it was created and how was it received?

- Where was it sent and who has access to it?
- Where is it, how is it stored and how many systems does it touch?

Looking at one system in isolation is problematic and frequently leads to leaks and loss. For example looking just at a donor database as a single system may neglect the fact that the data within it is accessible via multiple interfaces, possibly published to the internet and/or accessible over some form of mobile application. The NFP should look at donor information more broadly to determine all attributes of data including those listed above; who, when, where and how.

It is not only donor data that requires protection. All information that is important to an NFP must be identified, including intellectual property, business continuity plans, and marketing or campaign strategies that give a competitive edge to the NFP.

Once what needs to be protected is identified, a holistic approach to managing the security of the environment becomes possible.

3. Cloud Computing

Cloud computing is an elastic computing model that provides access to resources on demand. Cloud computing is very attractive, particularly for small to medium organisations, as the model provides an entry point to enterprise grade technology at reasonable prices which an organisation could not afford if it was to deploy independently.

While this has great benefits there are many risks to consider, including;

- Cross border jurisdiction:
    - In many instances data is shared across multiple geographies in a single platform.
    - You should understand the Privacy laws of countries that have access to your data.

- There are many difficulties in keeping up to date with changing laws.

- Multi tenancy, data ownership, data retention and purging:
  - Who are your co-hosted with?
  - Is there isolation between the entities?
  - At what layer is the isolation applied (network, operating system, application)?
  - Who owns the data?
  - When you leave your service provider are there guarantees that all your data can be purged and not retrieved by other parties?

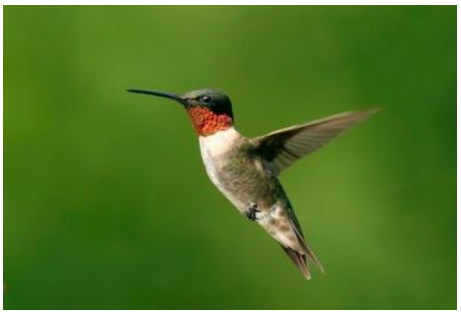
- Split responsibilities, compliance and reporting:
  - Are the responsibilities between service provider and customer well defined?
  - Can contract terms be negotiated?
  - How can the service provision be monitored, assessed and reported on?
  - Do you have a "right to audit" your service provider?
  - Is the service provider independently assessed? Are the reports available for review?

Private cloud will provide more control than public cloud offerings, however this is a less likely option for the NFP to adopt as there is generally no critical mass to warrant it.

The reality is that these sorts of technologies are rapidly taken on and only later do security controls and regulations follow. Many early implementations will be flawed. Poor quality service providers will struggle to meet compliance mandates, and as such, will provide an insecure offering. It is therefore essential that the contract includes provisions to maintain visibility and control over an NFP's outsourced and hosted environments.

4. Mobility

Mobile devices have developed from single purpose voice devices, expanding their capabilities across messaging, social media and personal computing. Today, mobile devices such as smart phones and tablet computers are playing a significant role in changing the way people live, work and communicate, making the world more interconnected, integrated and intelligent.



These devices are rapidly being adopted by organisations and are becoming commonplace alongside traditional devices such as laptops and desktops. Organisations, including NFP's, recognise mobility solutions for their strategic significance and are adopting them to deliver business outcomes.

As smartphones have moved from the realm of corporate executives to broad consumer appeal, organisations are witnessing a huge crossover of devices into the workplace. Employees are now bringing their own mobile devices to the workplace and are expecting companies to support them. A new acronym has even been created to describe this escalating practice - BYOD (Bring Your Own Device). As the world continues to ride on the mobility wave, it is imperative that a collective balance is established between the need for personal accessibility and the need to control corporate information.

Mobility will present great advantages to the NFP sector but the challenges will have to be dealt with as well. For example, mobile applications on tablets may be used at events to gather donor information, sign people up to campaigns and take payments. Clearly sensitive data will need to be protected in transit and at rest. The organisation will also have to address the mobility challenges at a technical and policy level, specifically where personal devices are used for business activities.

5. Social Networking

In general what is considered personal and private information is rapidly diminishing. Today fewer people have inhibitions about posting sensitive information online, often without understanding the long term implications, not in the least the difficulty of retracting or removing such information.

Because people post all sorts of information, social media sites become a very valuable source for data mining to obtain relevant, possibly sensitive information, about the user or their organisation.

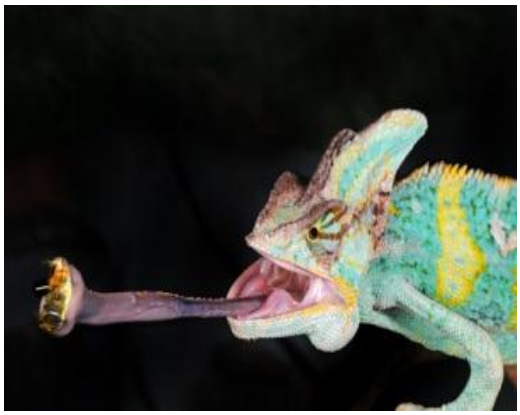
There is every possibility that corporate information

may be published online through personal accounts or possibly leaked inadvertently. Of course staff could also become victims of social engineering, as social network sites are the perfect medium for confidence tricks in order to gain unauthorised access to systems or acquire information. For example, it becomes a trivial exercise to compromise an individual's identity to gain access to a corporate system through the "forgotten password" feature commonly used to reset the user's credential. These features often ask for simple responses to "your pet's name", "your high school", or "your mother's maiden name", the answers to all of these are readily accessible through trolling user profiles in social networks or forums.

NFP organisations need to understand and define its risk appetite in order to determine what information can be published online. Enforcement of this position will need to be dealt with through appropriate technology and policy.

6. Threats

Through the rapid uptake of cloud computing and mobility solutions, the modern organisation has become more connected and interconnected, and therefore increasingly exposed to threats via commonly accessed channels in both breadth and depth. Attacks remain targeted at applications which are easy to compromise due to lack of appropriate security practices implemented at the time the application was developed.



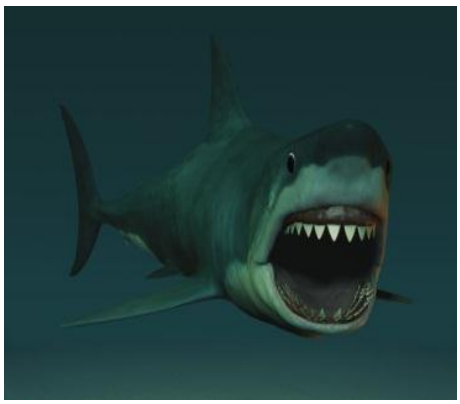
Last year some 7,000 new vulnerabilities were disclosed of which 30-40% will have no vendor supplied fixes to address the flaws.[2] Notwithstanding this, recent studies show that 96% of breaches were avoidable through simple or intermediate controls.[3]

[2] IBM X-Force® 2011 Mid-year Trend and Risk Report, September 2011.

[3] Verizon 2011 Data Breach Investigations Report.

NFP's do not require outrageously expensive information security practices to protect themselves against common threats and achieve satisfactory outcomes. They simply have to apply reasonable due diligence around common, simple and intermediate controls. For example, some 90% of data breaches investigated by the NSW Police's fraud squad could have been avoided if organisations conducted penetration tests.[4]

Consider what an intelligence agency in the Australian Government Department of Defence, The Defence Signals Directorate (DSD), has to say regarding the importance of cyber security measures.



"The threat is real, but there are things every organisation can do to significantly reduce the risk of a cyber-intrusion. In 2009, based on our analysis of these intrusions, the Defence Signals Directorate produced 35 Strategies to Mitigate Targeted Cyber Intrusions – a document that lists a variety of ways to protect an organisation's ICT systems. The CSOC estimates that around 85% of targeted cyber intrusions could be prevented by implementing the top four mitigation strategies as a package.

The top four mitigations are: patching third party applications; patching operating systems; minimising administrative privileges; and application whitelisting,"[5]

7. Defence in Depth

Unfortunately, any organisation that is internet connected and has information that is of value is likely already compromised. Many organisations are relying on out-dated security

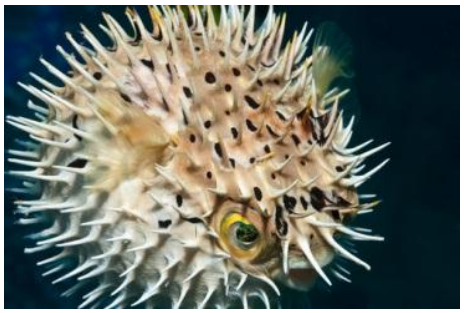
[4] http://www.crn.com.au/News/278512,police-pen-tests-could-thwart-90-percent-of breaches.aspx?eid=4&edate=20111101&utm_source=20111101&utm_medium=newsletter&utm_campaign=daily_newsletter

[5] http://www.dsd.gov.au/publications/Top_4_Mitigation_Strategies_to_Protect_Your_ICT_System.pdf

practices such as a single layer of control at their perimeter (e.g. a firewall), but remain vulnerable on the inside. The outcome is that organisations are frequently compromised.

This is primarily as a result of two factors:

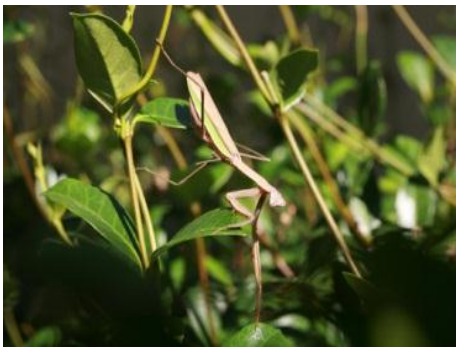
1. The organisation does not know what they are protecting and;
2. The controls are generally perimeter or single layer controls. Once one layer is compromised there is very little or no further protection against an attack on internal systems.



Perimeter security controls are important, but they provide only one layer of security. The modern organisation must have multiple layered controls - this is defence in depth.

Traditional protective controls are technologies such as firewalls and Antivirus. While they serve a purpose, they are not adequate to defend against modern attacks. For example, most current attacks focus on application layer vulnerabilities. Traditional firewalls permit traffic through to web servers because these systems must serve their content, but this also allows the attack to occur through the authorised channel. So additional technologies are required; for example, application layer firewalls (also known as web application firewalls, WAFs) that can detect and prevent attacks that target application weaknesses.

Protective controls should work from the outside to the inside where the data is likely kept. It is however of equal importance to detect and respond to attacks. Security via obscurity in the information age is not acceptable, amounting to no more than a cosmetic measure which is very easily overcome by even a modest attack.



8. Compliance and Regulation

As the world becomes increasingly regulated, expect those regulations to get tougher. It is human nature to react “after the fact”, which is why legal and industry regulations have to adapt to changing market conditions.

In general, the NFP market relies heavily on credit card payments for regular and irregular giving. Organisations in this sector have also developed various channels for campaigns including call centres, online web sites, face to face marketing and traditional printed mail campaigns.

Unfortunately, this sector is not immune to cyber security issues including hacking and loss of sensitive data, such as credit card details, through both online and offline exploitation. In order to bolster consumer confidence and manage the risk of the payment networks, payments effected through payment cards (credit and debit card) are regulated by card schemes and acquiring banks through the Payment Card Industry Data Security Standard (PCI DSS). All organisations that participate in the payment process of the cardholder data must comply with the PCI DSS if they transmit, store or process cardholder data.

As a result of dealing with credit card payments, this sector in general is faced with the requirement to be PCI DSS compliant and the fact that multiple channels exist whereby card payments are effected, the compliance requirements are made more challenging.

It is also important to note the changes that are being experienced in privacy reforms.

In recent years the Australian Law Reform Commission has produced and recommended significant and important reforms to the sector, the reigns of which have been taken up by government.

In its 2008 Report, For Your Information: Australian Privacy Law and Practice,[6] the Australian Law Reform Commission (ALRC) considered the range of privacy protections available in Australia and made a number of recommendations. As part of that report, the ALRC recommended that federal legislation should provide for a statutory cause of action (a right to sue created by law) for serious invasions of the privacy of natural persons.[7]

The New South Wales[8] and Victorian[9] Law Reform Commissions have also recommended similar causes of action.

Even more recently, the Commonwealth continues to focus in on privacy matters with strong calls for feedback regarding the ALRC recommendations.[10] Expect that laws will continue to be reviewed and reformed, with such legislation likely to pass through Parliament in due course. Perhaps politicians are awaiting a major data breach as impetus.

Changes in corporate and employee behaviour are expected to see adaptations to regulations. For example, the rapid uptake of cloud computing has already required the government to provide regulatory guidance.[11]

PCI DSS requirements and procedures are adapting to highly virtualised payment environments. New guidance papers are being released on virtualisation, cloud computing, hosting service providers and connections to payment gateways, providing essential direction for regulatory compliance.

[6] Australian Law Reform Commission, *Report 108 — For Your Information: Australian Privacy Law and Practice* (2008), ch 74 and recs 74–1 to 74–7 (ALRC Report), available at <www.alrc.gov.au/publications/ report-108>.

[7] New South Wales Law Reform Commission, *Report 120: Invasion of Privacy* (2009) (NSWLRC Report) available at <www.lawlink.nsw.gov.au/lawlink/lrc/ll_lrc.nsf/vwFiles/R120.pdf/$file/R120.pdf>.

[8] Ibid.

[9] Victorian Law Reform Commission, *Surveillance in Public Places: Final Report 18* (2010), ch 7 (VLRC Report) available at <www.lawreform.vic.gov.au/wps/wcm/connect/justlib/Law+Reform/Home/Completed+Projects/Surveillance+in+Public+Places/>.

[10] In response to changes in the market, the government released a paper "A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy" which was open for response until 4 November 2011.

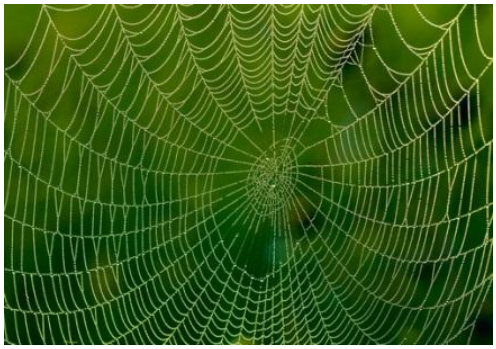
[11] Australian Government Cloud Computing Strategic Direction Paper, Dept of Finance, April 2011 Version 1.

An increasingly mobile work force and expectations for BYOD will require organisations to improve their security governance models. Organisations must be made resilient to threats and more readily adaptable to changes in regulation and compliance.

The implications for the NFP sector are that reasonable measures will have to be applied to protect the sensitive data and privacy of clients, subscribers and donors.

9. Awareness - Conclusions

NFP's should adopt a risk based approach, identifying the information assets within the organisation.



Think back to the bees. Know what your data (honey) is. Know what you are protecting. Know where it is, what it is and who has access to it.

Appropriate controls can then be looked at, and a governance model implemented which will include the requirement to test the adequacy of protective, detective and responsive controls.

Begin by adopting simple measures which will raise the bar of security across the NFP organisation. For example, restrict administrative rights, patch systems and apply strong passwords.

Seek assistance from third parties to implement effective strategies and always bear in mind that there are existing information security management standards that are designed to provide coverage across the NFP organisation.

Attacks are increasing in volume and sophistication. As a result, the implications have become more severe. Compliance requirements should not define strategy. Rather, strategy should enable the NFP to become compliant and robust enough to enable responses to any cyber attack or regulatory requirement in the dynamic, versatile and engaging world that is the NFP's domain.

"Cyberspace is a 24 hour a day world, one in which old assumptions about geographic boundaries and time zones are obsolete. This is one of the great benefits of modern technology — cyberspace is always open for business. But this also brings great challenges to those who guard our electronic borders."

Senator John Faulkner