

Data Protection Within the NPO

Written by Jeffrey Bernstein

Published February 2009 in the Straits Times Newspaper of Singapore as the lead story in the Business Times "BizIT" Section

Data Security Protection is among the most challenging issues facing Internet-connected companies, institutions and governments worldwide. International regulations and standards along with security breach disclosure laws and the continued growing threat from sophisticated exploits, have forced organizations from all sectors to address Information Technology (IT) security assurance as a matter of strategic importance.

At least 43 North American states, the District of Columbia and Puerto Rico have now enacted legislation requiring the notification of security breaches involving personal information. While actual requirements and associated penalties for non-compliance vary from state to state, most laws require immediate disclosure to victims and usually in writing.

A similar regulatory environment exists within the United Kingdom (UK) and the European Union (EU) where numerous laws including the EU Data Protection Directive exist. All of the 27 Member States of the EU, the three additional members of the European Economic Association (Norway, Iceland, and Lichtenstein) and several other European nations that trade heavily with the EU, such as Switzerland, have transposed the EU Directive into some form of national law.

As the most trusted Asian hub for many U.S. and EU companies and as a primary trading partner to both North America and Europe, Singapore is coming under increasing pressure to secure sensitive data, networks and systems. While the financial services, healthcare and power generation verticals are usually the first to come under scrutiny, there is increasingly growing interest regarding the protection of data in the Non-Profit and charity sectors. Non-profit organizations (NPOs) are unique in that while trust is required for successful operation of all organizations, the NPO is always held to a higher standard. The reason, of course, is that by nature the NPO exists and is fueled only by the private individual, government and corporate donors that support it.

Perhaps even more heavy-handed than the various International issues driving adoption of data security strategies within Singapore will be the continued development and implementation of Singapore's "Intelligent Nation 2015 Master Plan for Infocomm (iN2015)". iN 2015 is Singapore's 10-year master plan to help the country realize the potential of infocomm over the coming decade. Led by the Infocomm Development Authority of Singapore (IDA), iN2015 is a multi-agency effort that is the result of private, public and people sector co-creation. In the words of the IDA, "the program promises to give rise to new

CRITICAL DEFENCE

Internet uses that are computationally and data intensive in nature, therefore enabling applications that have been previously difficult to undertake”.

An organization by organization review of Singapore’s National Council of Social Services (NCSS) membership indicates that donations collected by Singapore NPOs are most often made traditionally hand-to-hand or by check sent via mail and without any electronic processing component. Providing an on-demand, web-based donation application can allow NPOs to take advantage of unexpected surges in national and international support and sentiment that may result following a natural or man-made catastrophe (like 9/11, the 2004 Asian Tsunami, Hurricane Katrina or recent terror attacks in Mumbai). In many other internet enabled countries, online donating has become quite popular and has mushroomed NPO donation for this reason alone. Given the technical sophistication of the Singaporean nation and the need for non-profits to be competitive and efficient, large scale adoption of transactional applications to support online fundraising in the Singapore NPO space is very likely.

As the realization of the iN2015 promise trickles down through various Singaporean market segments you can almost certainly be assured that NPO’s will move to deploy web-based applications that will assist with the raising and collection of donations. In fact, a 2008 study by The Non Profit Times already indicates that the number of potential donors using the Internet to find out more about nonprofits has jumped from 25% in 2005 up to 44% in 2008. With increasing attention on the NPO web-presence, the leap to website-application donor funds processing cannot be too far away.

Unfortunately, with the adoption of added technology and implementation of new services, the risk to NPOs for the loss of funds and leakage of sensitive personal data will increase. Malicious cyber attacks that have been traditionally more network-centric are now trending towards transactional web-applications and the valuable data that resides in them. Numerous NPOs (United Way, Red Cross and NAACP to name a few) from earlier adopting nations have already fallen victim to the types of application exploits that have increasingly become regular front page news.

What can be done by the NPO to ensure that technology is utilized without compromise to security? The NPO can adopt a process of Information Assurance.

A viable Information Assurance (IA) program will typically begin with identification and classification of the network and application information assets to be protected within the NPO. This process forms the basis for an organization-wide threat model. Next, a risk assessment is delivered to baseline the security posture of the organization. It is helpful if the assessment considers both the probability and potential impact of any undesired events. The probability component may be subdivided into security threats and vulnerabilities. The impact component is usually measured in terms of cost. The combination of these values should be considered the total risk involved.

Based on the risk assessment findings, the organization develops a well-tailored risk management plan. This plan proposes countermeasures that involve mitigating, eliminating, accepting or transferring the risks to third parties and takes into consideration prevention, detection and response components. A commonly accepted information security framework (like BS7799 or ISO 27k) may also be utilized in designing the risk management plan and baselining the organization’s initial security posture.

CRITICAL DEFENSE

Countermeasures may include the use of technology including anti-virus software, firewalls and intrusion prevention systems. The development and implementation of policies and procedures as well as security awareness training should also be considered. The cost and benefit of each countermeasure should always be considered by the organization which should not seek to eliminate all risks but simply to manage them in the most responsible and cost-effective way.

After the risk management plan is implemented, it is tested and evaluated with regularity and preferably by means of formal third party security assessments. Security managed in this fashion becomes an enabler to the continued viability and success of the NPO.