INFORMATICA RESEARCH
SECURE PHILANTHROPY

THE 2012 OUTLOOK IN SECURITY & PRIVACY FOR NON-PROFIT AND CHARITABLE ORGANIZATIONS

The world of non-profit organizations has benefitted like no other from technology and in particular from the advent of electronic payment systems coupled with the global reach of the Internet. Since the late '90s, the need for convenience has driven the broad adoption of innovative avenues to facilitated e-philanthropy, from intranet-based workplace fundraising to wireless donation systems with full-featured social networking capabilities.

E-philanthropy has grown by leaps and bounds each year since 9/11 surpassing its previous high water mark almost every quarter (5.7% in the first half of 2011 vs. 3.8% in 2010). The combination of convenience through simplified complexity, the sheer volume of donations (in the hundreds of billions annually) and the inability of the technologically unsophisticated donor audience to keep up with security threats and growing privacy risk, is a potentially combustible mix.

The good news: secure philanthropy has no systemic issues leading to risk exposure and its opportunities to innovate on a global scale while growing donor engagement are outstanding - as long as education and awareness are incorporated at all levels, from development to donor interaction.

Areas of disproportionate risk

Charitable organizations benefit from a powerful human drive to altruistically extend a helping hand and have a positive impact with no direct personal benefit, and as such donors on the whole can be said to hold any other type of commercial enterprise to a higher standard of risk accountability than not-for-profits. This may reduce the drive to adopt and innovate information risk management, at least in the smaller enterprises where resource allocation is focused towards fundraising efforts.

Unfortunately, in some organizations only superficial attention is paid to the security aspects of e-donations and as such is limited to checking for such basics as the lock symbols on-screen, seals of trust and some indication that 'your donation is secured to the same standards as those employed by your banking institution'.

Hackers know how to recognize non-profits that do not allocate adequate resources to protecting personal information. Typical e-giving systems often have built-in risk reduction features such as a limit to donor data retention, anonymity assurance, end-to-end confidentiality and other systems security. Unfortunately, not enough organizations have the interest, inclination and budgets to adequately configure systems, implement policies and educate staff about security and privacy.

© 2012 Informatica Corporation – All Rights Reserved
trust | informatica

Introduction

The efforts of philanthropic organizations are in higher demand in the face of today's global economic unrest. With the evolution of the role of social media in promoting not-for-profit work and social media's fundamental role to connect people and disseminate information about the great impact of charity work, philanthropic organizations find themselves under a great deal of scrutiny and have become targets of cyber attacks.

Donors need evidence that their charitable contributions are wisely leverage and that they can continue to trust their chosen causes. To meet these goals, philanthropic organizations need to pay special attention to protecting their most valuable asset which is directly linked to their work and reputation: donor information and financial reporting.

This hinges on the fact that organizations are increasingly dependent on accumulated and shared information, privacy controls and the planning that goes into the protection of these assets over time.

We explore the evolution of information and financial asset protection in charitable organizations at a time of increased risk to intangibles and associated rise in reputational impact due to broad adoption of social media and other forms of exposure.

What's at stake?

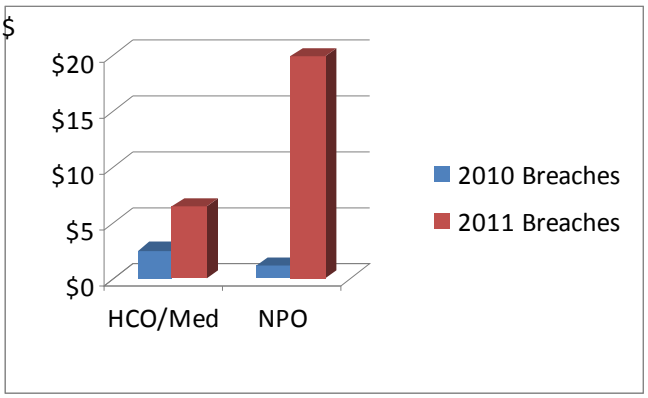
Without much reflection, an uninformed audience can quickly and qualitatively point to a reputational impact of negative events leading to declines in public trust and donation amounts. But this clearly points to a vast gap in the consequences of poor risk management between industries. For instance, in healthcare and finance, we see factors such as large legal 'Swords of Damocles' motivating organizations to adopt and demonstrate proper risk management practices. These can range from class action lawsuits to jail terms for executives. But what's the real impact of fraud, hacking and privacy breaches?

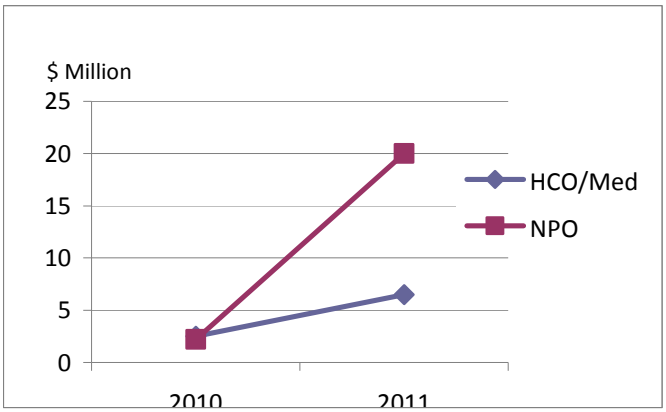
personal information loss	long-term identity breaches
lost contributions	high cost of remediation
ineffective processes	increased operating cost

The vast majority of drivers of information risk management in the *commercial world* can be said to be compliance-based, with industry, sector and geographically applicable legal penalties for failure to demonstrate proper practices. Non-profit organizations don't have to choose to adopt expensive practices to avoid eroding public trust. They need to enhance their ability to carry out their mission.

What exactly are the effects of breaches on unprepared organizations? We took the data from a few sources that show, for example, how many healthcare sector and medical organizations were breached in 2010 vs. 2011 and what the trend was. In the US, there is strong federal and state legislation in effect to protect precisely the kind of patient information that is targeted in medical identity fraud and other hacking exploits. In 2010, 184 healthcare organizations (HCO) reported breaches estimated at $2 - $3 million. A more recent article stated that the cost of breaches for medical / HCO institutions was around $6.5 million in 2011 and the trend is pointing up by 32% in the past year. The same Ponemon Institute report mentioned that 96% of institutions were breached at least twice. We found that for the 9 US non-profit organizations that reported breaches in 2010, at an estimated cost of $214 per record breached, there was a loss of US $1 - $2 million. With the Anonymous attack on Christmas 2011, a loss of $2 million dollars was reported, bringing the 2011 estimated cost of breaches for charitable organizations to almost $20 million:

© 2012 Informatica Corporation – All Rights Reserved

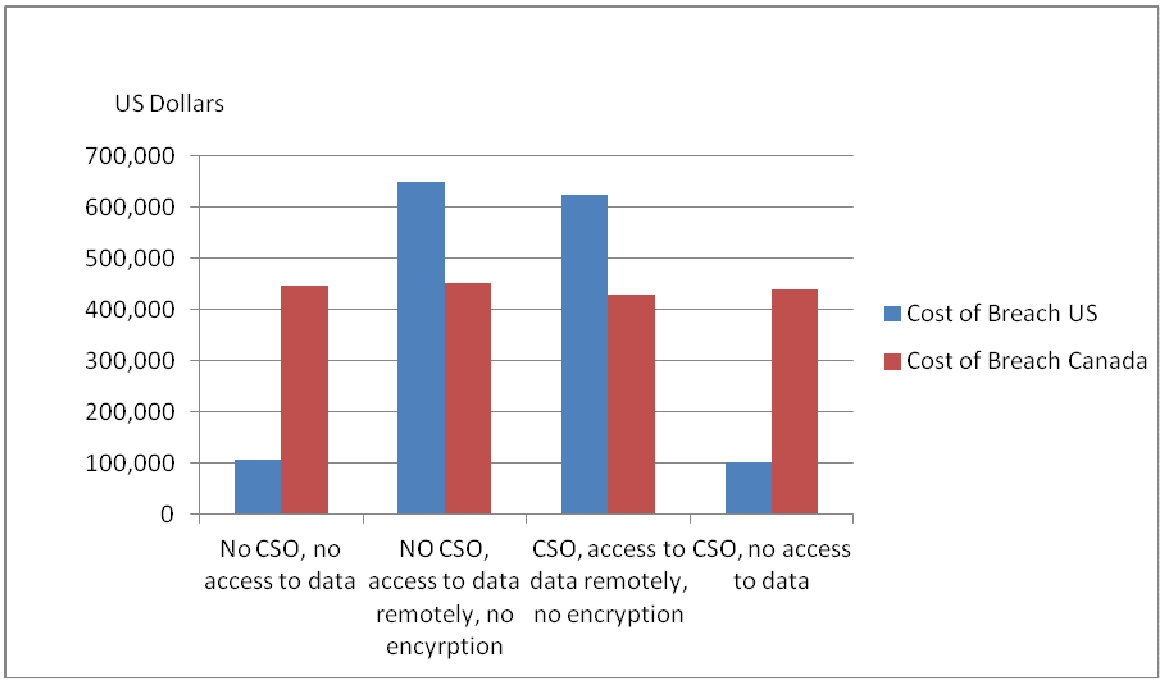




All available sources indicate that breaches in the non-for-profit sector are not directly attributable to criminally malicious attacks but rather due to a lack of security policies, training and documentation, no security officer function and weak practices for encryption on devices which hold or access sensitive donor information.

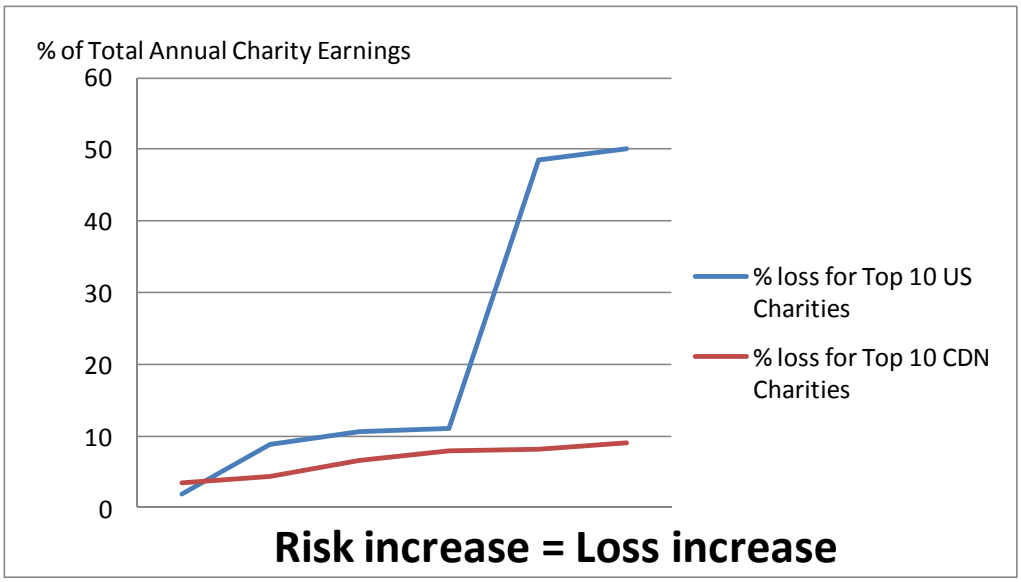
The risk of breach for the top 10 charities in the US and the top 10 charities in Canada, considering there are over 500 employees and over 1,000 records breached (up to 2,000 records) is significant and it could easily exceed the budget allocated for a significant number of staff salaries.

For the top 10 US charities based on 2011 earnings (ranging between $6 million and $1.2 million for each of these) and the top 10 Canadian charities based on similar annual earnings, we were able to calculate the impact of breaches:



© 2012 Informatica Corporation – All Rights Reserved
trust | informatica

When we take in consideration that the economic downturn indicates a drop in staff in different profitable sectors and that the top 10 charities pay anywhere between 9% to 21% of their charitable funds to salaried employees, it is evident that a breach and economic hardship could devastate even the top 10-25 global charities. We note however that many of the larger non-profits do embrace best practices and have a high level of awareness around security and privacy.



In many cases, organizations small and large choose to outsource key processes to which they have competitive advantage while choosing to insource such complex aspects of risk management as security and privacy assurance. Thus, by using *wrongsourcing* as a method to save costs and preserve the confidentiality of risk-related activities, security and privacy practices do not improve. The risk of developing a laissez-faire culture is a real one, as organizations increasingly determine their inability to manage multifaceted risk at the control level.

Opportunities for positive change

The industry has many opportunities to leverage its advantages and change the status quo. By matching a vast capability to reach a welcoming audience of donors, a clear message of awareness and deep financial resources, the power of distributed risk mitigation can be used to address the gap between the success of this sector and its ability to withstand a large variety of security-based and privacy-oriented attacks. By adopting proper governance, risk management maturity can improve all operational aspects of e-philanthropy, resulting in stronger, more consistent growth in donations and increased public respect. For this to happen, six aspects of proper information risk need to be addressed:

- Overall risk maturity must increase
- Genuine public education about risk
- A culture of vigilance & communication
- A commitment to applied best practices
- Clear focus on standards compliance
- Effective approach to collaboration

2012 has the potential of being a landmark year for non-profit organizations that adopt a progressive stance towards risk management. A commitment to introduce best practices can be achieved by implementing policies to govern access control, need-to-know and the principle of least privilege. Hardened systems and environments should be periodically reviewed and encryption properly implemented. Check simple controls such as antivirus and firewalls and make sure they are monitored. Relatively inexpensive technology can supplement these measures, increase the risk maturity of these organizations and offset resource constraints.

© 2012 Informatica Corporation – All Rights Reserved

Most large not-for-profit organizations are aware of best practices and many implement them adequately. We encourage them to share their practices in a collaborative way to raise the bar on acceptable protection for the sector. Valuable investments in education, policy implementation and protection of donor information using inexpensive technology and processes will result in continued growth in this sector while public trust will be fueled by trust in proper risk governance (for a change).

References

1. Security and Privacy Issues in e-Philanthropy. Feig, Ephraim. Kintera.
2. Philanthropy is Becoming a Click-and-Give Enterprise. O'Keefe, Mark.
3. Knol , Technology and Non-Profit Organization. Holmes, Sean
4. Nonprofit IT Staffing: Staffing Levels, Recruiting, Retention, and Outsourcing. http:// nten.org/research/nonprofit-it-staffing-staffing-levels-recruiting-retention-and-outsourcing.
5. Nonprofit IT Staffing: Budgets, Salaries, Training and Planning. http://nten.org/research/nonprofit-it-staffing-budgets-salaries-training-and-planning.
6. Non Profit Technology/Backup Survival Guide http://www.nptechnews.com/management-features/backup-your-survial-guide.html
7. Philanthropy Journal http://philanthropyjournal.org/resources/fundraisinggiving/value-hosted-data
8. Ponemon Institute http://www.ponemon.org/blog/post/cost-of-a-data-breach-climbs-higher ; Ponemon Institue 2011 Study on Privacy and Security in Healthcare and Data Breach Calculator
9. James Austin. "The E-Philanthropy Revolution is Here to Stay." Chronicle of Philanthropy.

© 2012 Informatica Corporation – All Rights Reserved