



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 vast 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), but the combination of convenience through simplified complexity, the sheer volume of donations (in the hundreds of billions annually) and the failure of the technologically unsophisticated donor audience to keep up with security threats and growing privacy risk, is a potentially combustible mix.

Much of our analysis of this *space* is focused on the driving factors behind the unrelenting growth – now accounting for 33% of sector activity - in e-philanthropy as it defies economic downturns and continually strives to maximize donor access to convenient contribution methods unlimited in their scope or preference for cash, corporate stock, usable goods, vehicles, real estate or food items. Indeed, if anyone is willing to give, there's someone willing to receive within a few clicks. And practically everyone gives to one cause or another during the year, but few take more than a passing interest in the underlying risk to the security and privacy aspects of charitable processes whose standardized façades arguably discourage any endeavor that might detract from the fulfillment of the intended act. And we submit that this approach may be flawed.

Secure philanthropy has a vast opportunity to be the next step in the growth of gift-giving by leveraging a number of aspects of risk management normally thought of as residing in the domain of the technology providers. But as we are seeing on a frequent basis, organizations of all sizes and scopes are being targeted for their vast reach, deep coffers and expansive information databases.

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 apparent 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, thus reducing the drive to innovate risk reduction.

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



Unfortunately, there are 9 aspects of risk that are not addressed by the typical e-giving interfaces:

- | | | |
|----------------------------|-----------------------------------|-----------------------------------|
| Human verification | Limited donor data retention | Harmonized risk across methods |
| Anonymity assurance | Transactional processing location | Continuous provider communication |
| End-to-end confidentiality | End-user system security | Continuity & disaster recovery |

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 applied legal penalties for failure to demonstrate proper practices. In many cases, non-profit organizations choose to only superficially adopt such practices with the unfortunate effect of eroding public trust and reducing their ability to carry out their mission.

In many cases, organizations small and large choose to outsource key processes to which they owe competitive advantage while choosing to 'handle' such complex aspects of risk management as security and privacy assurance. Thus, by using *wrong sourcing* as a method to save costs and preserve the confidentiality of activities, the security and privacy practices do not improve and a laissez-faire culture is internally cultivated while the public is placated with standardized messaging designed to streamline the philanthropic process.

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 disproportionate 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 address 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 | A commitment to applied best practices |
| Genuine public education about risk | Clear focus on standards compliance |
| A culture of vigilance & communication | 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. By investing some of the mindshare on awareness and education alone, organizations can derive the kind of loyalty that few commercial enterprises enjoy.

The full 2012 *Secure Philanthropy* white paper is available by request from info@InformaticaResearch.com. Media requests for comment are welcome. Full document to be available from SecurityandPrivacy.ca > *Library*