



# Secure Philanthropy

The Emerging Challenge of Information Security  
for Non-Profit Organizations

**An Informatica Security White Paper**  
**October 2004**

**Author:**  
Claudiu Popa, President  
Informatica Corporation

## TABLE OF CONTENTS

Introduction	3
Emerging Challenges	4
Threats	6
Solutions	11
Conclusion	14
References	15

Informatica Corporation provides non-profit organizations with information security consulting, services and technology. With expertise spanning 15 years, Informatica is a recognized industry innovator and corporate advisor. Services include executive consulting, security management, complete training programs, risk management, management support and industry-leading security assessments. ([www.InformaticaSecurity.com](http://www.InformaticaSecurity.com))

Copyrights and trademarks of Informatica Corporation include: FlexSecure Verify (audits, analysis and assessments), FlexSecure LockDown (secure systems), FlexSecure DataScrub (secure data destruction), FlexProtect (corporate security support) and FlexProtect SM (security management), WorkLife Learning (corporate training).

## Introduction

The world of non-profit organizations is distinguished by philanthropic pursuits seeking to make lasting social and institutional changes. These changes are always motivated by challenging the status quo and attacking the root causes of poverty, inequity and disadvantage.

These noble pursuits, often marginalized, are seeing growing success. While the increasing number of non-profit organizations is a poor indicator, their rapidly growing budgets are a significant step in the right direction. According to a study entitled “the State of the Nonprofit Industry” by software provider Blackbaud, 75% of non-profits indicate increased demand for their services, increased donations (57%) and increased budgets (59%).

This phenomenal growth brings with it the traditional challenges of any business and supplements them with those specific to non-profit organizations. Increasingly clear is the fact that NPOs need to adopt traditional business practices, embrace business processes and comply with best practices and standards.

While international organizations have adopted internal best practices, standards and policies, national and local charities often operate in isolation, with traditionally reduced budgets and limited access to external expertise. The need for non-profits to collaborate, share knowledge and information is well known and documented. The fact remains that insular thinking and closed management often remain the norm, thus jeopardizing the ‘business’, its assets and critically, its credibility.

The necessarily limited scope of this paper is focused on the increasing challenge of protecting information assets, a core element to the growth and success of every non-profit operation. This topic relies 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 the long term.

The information security and privacy of a non-profit organization is thus at the core of its ability to project effectiveness and inspire trust in its philanthropic pursuits; trust and confidence being the critical selling points in the specialized business of attracting donations and motivating on-going charitable participation from donors and customers.

## Emerging Challenges

With growing budgets, staff and influence an organization needs to take a very serious look at its ability to scale its operations and support its ongoing activities. Technology is a key element that is relied upon to lower operational costs and increase efficiency. The proper management of technology is a challenge for the vast majority of businesses, with no indication of an appropriate budgeting formula and the instinct to reduce visibility into that side of operations. Fortunately, technology providers, in an effort to capture larger pieces of an expanding market continue to make progress in the simplification of their products, making good strides towards compatibility and user-friendliness. As a result, most organizations have adopted technology with adequate degrees of success and some measure of control over IT budgets.

By their nature, non-profit organizations have traditionally limited budgets for anything outside the realm of the 'absolutely necessary'. As a result, obscure concepts such as information security and confidentiality are often dealt with summarily without specific controls and detailed procedures. Without planning, the added organizational stress of an expanding operation, changing business processes, combining office locations and human resource management place unsustainable pressures on the constructs in place to protect organizational assets.

The challenge facing any NPO today is thus to undergo positive change without jeopardizing the very attributes that initiated that change in the first place.

The clarity of thought, strategic detail and planning expertise required to adequately protect the organization is often beyond the capabilities of any business. The ability to see this challenge, to remain open to understanding the risks and the rewards of adequate preparation is the determining factor in an organization's hope of continued success.

To be clear, the challenges associated with most NPOs management of information assets are as follows:

1. Creating and maintaining a scalable, shared and realistic information protection strategy. Taking into consideration privacy compliance, secure practices, clients, partners and service providers.
2. Adopting a management structure that includes a steering committee, policies and procedures, all dedicated to the protection of information assets.
3. Sharing information security knowledge with other organizations, making privacy policies public and continually improving communications

4. Adopting enterprise-wide awareness of information security risks, policies and resources. Incorporating best practices into employee training, enforcing accountability at the user level.
5. Planning for the long term, not only for scalability and change management, but anticipating and documenting business continuity challenges. According to NetAction, business continuity and planning are non-existent or inadequate in 64% of non-profit organizations. Additionally, over 50% identified backup processes as issues that need to be addressed and over 60% pointed to disaster recovery as an area of improvement.
6. Securing communications and preventing access to unauthorized users. While just under 45% of organizations surveyed identified data encryption as an area of improvement, a surprising 85% either didn't use it at all or had no idea whether it was available. While some organizations recognized the need for encryption, only 4% encrypted all sensitive data, indicating a lack of policies regarding data classification.
7. Enforcing secure practices designed to take into consideration the possibility of malicious activity: incident response, forensic capabilities and the availability of expert support.

Statistics from NetAction 2002 survey of NPOs.

These are the most pressing challenges facing non-profit organizations today. They exist irrespective of size, scale and technology. They are management challenges that can only be met by the combination of multifaceted organizational involvement (i.e. steering committee), professional expertise and knowledge sharing (i.e. with other organizations).

## Threats

The biggest threat is not understanding the risk. Put another way, the lack of security that is evident in business today is an opportunity waiting to be exploited by criminals. This applies to all organizations and to date, criminals have been picking the low hanging fruit, perfecting their strategies and adapting to change.

The philanthropic nature of non-profit organizations, charities, churches and other such institutions is neither a deterrent nor a risk-reducing factor in the decision to carry out an attack. This is one of the biggest misconceptions about the risk facing the industry. The 'why us' and 'we are not a target' are very dangerous misconceptions and they lead to a lower sense of awareness and vastly reduced security. In fact, these organizations are very prone to attack because of their focus on conducting transactions. Fundamentally, the goal of a charitable organization is to make 'giving' as easy and satisfying as possible. This is often done by sharing comprehensive information about the cause and implementing versatile payment systems.

Keeping in mind our earlier assertion that most non-profit organizations operate independently with little knowledge sharing about information protection and best practices, this is where the risk becomes evident. The size of the organization is not a major factor in the risk calculation. In other words, NPOs small and large are at comparable risk for the following reason: small organizations often have reduced budgets and a pressing incentive to increase the number of payment processing methods. Their online presence and presentation are often a testament to limited preparedness and low degrees of risk awareness. On the other hand, large organizations have complex structures and increased transactional volume which also makes attacks on information security an attractive and profitable proposition.

The major threats facing this sector falls into multiple categories:

### **1. Emerging e-philanthropy**

According to the NetAction survey of the non-profit sector published in 2002, all organizations (99%) were connected to the Internet while 92% had their own Web sites (now 99%). Today, there are numerous ways to establish an e-commerce presence at reduced cost to the NPO and there exist dozens of sites, such as 4Giving.com which facilitate the process of researching and giving to preferred causes. It is therefore very likely that today, all organizations are encouraging donations facilitated by the connective power of the Internet.

One of the risks associated with this method is the ease with which an attacker would locate the cause that he wishes to attack. This is yet another reason why a non-profit organization might become a target: they take a stand and as a result,

there are always opponents of the cause who will take steps to squelch those efforts.

Once located, a Web site is a sitting duck, available 24hrs and willing to accept traffic from all visitors. The donation process can be vulnerable in a variety of ways, some of which include lack of visitor authentication, verification of credit card, account credentials, purchasing limits, database back-end access, cross-scripting vulnerabilities, cookie attacks, malformed queries and numerous others.

The threat to Web based systems is easily understood but often poorly remedied. Certainly the urgency of the situation is rarely brought up and a preference is often placed on superficial efforts such as creating written privacy policies, obscuring lack of security and providing access to documentation that supports the cause. Lack of Web and application security are two of the most serious causes of security breaches because they are poorly understood and inadequately monitored, thus allowing attacks to continue undetected for prolonged periods of time.

## **2. Unauthorized disclosure**

The concern over access and disclosure of data is one of the catalysts of security awareness in the enterprise. Another is the increasing pressure to adhere to industry and regulatory standards for privacy protection. This clear and present threat doesn't necessarily involve technology.

Organizations that lack the enforced use of non-disclosure agreements are at risk of unauthorized disclosure of proprietary information by visitors and service providers. A breakdown in relationships may be all the motivation someone needs to disclose embarrassing information about an NPO, causing irreparable harm to its public image and revenue stream. It is an accepted fact that employees and contractors represent 80% of security incidents. Given the high rate of insider crime it is surprising that organizations take very few steps to protect themselves using contracts, policies and controls.

Unauthorized disclosure is most often associated with the technology that efficiently manages information. Online databases and applications are often compromised by hackers, desktop information is stolen and exploited for profit by spyware and malicious worms. Malware is the hacker's way to penetrate network defenses that are protected by firewalls and other technology. It is a convenient way to take control of computers, turning them into 'zombies' that covertly work as part of a network of 'bots' ("bot-net") to support illegal causes. This type of activity is not only embarrassing, but also a great potential liability to the organization because its technology is being used to carry out a crime. The cost of supporting an investigation and cleaning up systems is often prohibitive, even by the standards of large organizations.

### **3. Unauthorized access**

Accessing data without proper authorization is clearly illegal, but a lack of controls on the part of the victim organization can create a case for the attacker. In recent cases where young hackers were caught stealing resources from government and military systems in the United States, it was alleged that the security measures in place were so weak as to make them entirely imperceptible, thus giving hackers unrestricted access to systems that they 'thought' were part of the greater Internet (and ostensibly placed there for their enjoyment).

The practice of creating hardcopies and inadequate disposal measures is a low-tech example. Most firms print a large portion of their documents, including sensitive information. Once used, and without the benefit of a clear data classification scheme, the document is discarded. Such documents can be found on boardroom tables, on desks, in garbage cans and in Blue Bins everywhere. This implied access authorization can create a very embarrassing situation for any organization and intentional activities seeking to access and collect such data can be difficult to detect.

In particular, wireless systems and remote access capabilities are responsible for increasing the threat of unauthorized access. These technologies are often designed to be convenient and maximize productivity so a balance of effectiveness and security needs to be struck for the solution to be valuable. In many documented cases however, the implementation of such measures turned into a liability as sensitive data was accessed either through the Internet or wirelessly and often without a trace.

Theft of business assets is a serious form of unauthorized access. It often includes a physical breach as well as the actual act of removing private property. Organizations that mistakenly assign information security responsibilities to IT departments are particularly vulnerable because physical access control measures are often weak or non-existent.

Laptops and notebook computers have become very popular over the past few years due to advances in technology and weight reduction. Along with the convenience of using a portable computer is the risk of having it stolen. For thousands of business people each year, this risk becomes a reality when they leave their valuable tool unattended or improperly protected. By failing to properly anchor the system, victims create opportunities for unauthorized access and theft. By failing to adequately encrypt the data they contain, the risk is amplified because now the valuable information is available to criminals.

### **4. Data confidentiality and privacy**

The danger of confidentiality breaches goes beyond cases where hard drives, laptops or servers are stolen. Even simpler situations create more serious damage.

Spam, for example, is a form of unsolicited email that carries with it misleading or entirely unwanted value propositions. The low response rates are offset by the massive recurring distribution and present spammers with a compelling reason to adopt it as a real business opportunity. Undeterred by increasingly stringent legislation but dissatisfied by the low response rates, spammers have established working partnerships with organized crime. Based on the logical assumption that very few people will open emails that are clearly not wanted but even fewer will bother to respond, spammers have more recently started including malicious attacks within their emails.

These attacks range from identity theft, to phishing to malware and generate thousands if not hundreds of thousands of dollars for their perpetrators. The threats are many and they range from stolen financial data, passwords to bank accounts and online trading accounts to installing software that records keystrokes (keyloggers), software that remotely controls the user's computer, video camera or any other connected device. More recently, hackers have reportedly accessed network-connected photocopiers to download and view sensitive documents copied internally.

## **5. Business continuity and data integrity**

One of the reasons why information security is a more complex concept to understand than traditional business subjects is that security breaches can take various forms. When we think of a situation involving the theft of property, it is easy to understand the process and the repercussions. With information security, we face a situation where we can have unauthorized access to our data, theft of our data, corruption or unauthorized editing, destruction of the data or some combination thereof. In fact, information security suffers from the belief that when a hacker accesses data, it is *only* disclosed and viewed without proper authorization. It isn't really lost since we can always retrieve a backup copy.

This awareness gap is particularly hurtful to non-profit organizations, where data is extremely sensitive and valuable. If exposed, victim or beneficiary information can create a dangerous situation. The liability to the NPO can also be substantial. In our own research, we see a gap of approximately 42% between perception of having adequate BCP and actual results. This type of discrepancy will render most of the business continuity planning ineffective when the time comes to apply it. Additionally, most organizations are not aware of the necessity to detail continuity planning procedures and circumstances. For example, very few managers have created lists of critical resources, in combination with specific vulnerabilities and sources of emergency support. Reality check: do *your* routers & switches 'fail open' or not? It can mean the difference between complete a compromise of confidential data, and simply dropping an Internet connection.

In cases where data is changed or corrupted, the unauthorized access is often difficult (if not impossible) to detect because nothing is really missing. In attacks involving data integrity, information is often corrupted and in organizations that

depend on a lot of data, it is nearly impossible to determine what has been compromised and what hasn't. In such cases, almost all businesses take the cautious route and restore a recent backup, losing productivity and all work done in the interim.

Of course, for such an option to exist, the organization must first have backups and secondly be able to restore them reliably. While the majority of organizations have some kind of backup scheme, most fail to test them regularly by performing regular 'restore' procedures, cycling tapes or even calculating if the backup interval is something they can live with.

Outsourcing is often a very effective way to address security issues and even protect against disasters. Off-site storage of data and document backups is a convenient way to protect sensitive information by keeping it off the premises. In case of a fire or other catastrophic event, this data can be retrieved and restored at an alternate location. Unfortunately very few organizations adequately audit the companies they entrust their data to, from the couriers to the site policies in place to protect it. The threat of complete disclosure and loss is hard to imagine, but an organization whose data backup records are stolen can be entirely cloned, down to the last email, in a matter of hours.

Again, protection in the form of strong hardware encryption is considered an adequate measure to protect against theft or unauthorized disclosure of the vast amounts of information typically included in backup data.

The last of the most significant threats to a non-profit organization's security is the typical lack of preparation for an actual breach. Incident response measures that are not documented and rehearsed are ineffective. For many companies, the belief that they can't be a target or are adequately prepared reduces their readiness for a breach. Some companies actually realize the risk involved but consider the likelihood of detecting a breach or being able to do anything about it so remote that no retaliatory measures are ever planned. In such cases, the damage done by hackers and criminals can not only be serious, but permanent since they are given a good chance to get away with it. Incident response procedures and forensic controls need to be in place to reduce the damage and reduce the risk of letting the crime go unpunished.

Information security threats affecting businesses and non-profit organizations are the same. They have the same motivating factors, use the same technologies and tactics, and cause equally serious damage. The differences are that in the business world, companies that understand the risk have tied it to its impact on business and sales, thus creating a compelling reason to implement adequate protective measures.

In the case of non-profit organizations, a similar shift in thinking must be adopted. By understanding the sensitivity and value of information, the losses due to downtime and fraud, it is easy to make a case for a strong, up-to-date security strategy and all the protective measures that accompany it.

## Solutions

To alleviate risks facing today's non-profit organizations, we must implement and embrace proactive security measures. A first step is to understand that information security is a moving target, continually requiring minor adjustments in strategy and procedures to remain protected. The second step is to understand that security is a governance issue, not an IT problem. By delegating information security responsibilities to the IT department, businesses and NPOs alike place themselves at higher risks of breach. This is not because IT staff is not capable to manage technology or implement security controls but is due to the simple fact that security is a management responsibility. Management is authorized to create policies, responsible for investing in training for enterprise-wide awareness and solely able to determine the value of information assets to the organization. Once a non-profit organization understands these simple facts, it is ready to implement lasting change and adopt secure practices with coordinated efforts from all departments and employees.

**Security measures** are best practices designed to be applied to non-profit organizations regardless of size and scope. These can be scaled to fit the budget and risk exposure of any NPO:

1. an overall security strategy describing the organization's dedication to preserving the security of proprietary assets, member and customer data and transactional information. The security strategy is a document that inspires as well as it reinforces the responsibilities and promise of upholding secure practices in the organization's philanthropic pursuits.
2. policies outlining acceptable use, restrictions and accountabilities for the use of resources and access to valuable assets. These detailed, documented regulations need to be understandable by all employees although not necessarily globally accessible. In particular, a data classification scheme specific to the organization needs to be created and adopted as the foundation of these policies. This often complex scheme includes the definition of different types of information assets, their owners and accepted methods of access.
3. an enterprise-wide awareness program, including recurring seminars that address specific issues, common problems and general discussions about risk and accountability. This program needs to take place on a recurring basis and be conveniently designed to engage, educate and motivate employees to embrace policies.
4. procedures describing best practices and acceptable use for employees, contractors and third parties. These documents must be made available to staff as a reference supplementing policy training and awareness efforts.

5. guidelines outlining common sense practices and summarizing everything from industry regulations to the use of specific software; these have a place within the information security library of every non-profit organization because they reduce the time it takes to train new employees and they are often reprints of existing product documentation, simply edited and incorporated within the overall documentation library.
6. Compliance with regulatory standards and privacy laws is of critical importance to all non-profit organizations. Because of a dependence on a positive public image necessary to build the trust of donors, NPOs need to constantly present a credible 'value proposition' preferably complemented by seals of compliance. Understanding, knowledge of and adherence to industry standards such as ISO 17799, WebTrust and PIPEDA are not only valuable because of the added credibility they promise but also because of the discipline they enforce. This also presents organizations with a good reason to make the effort and investment necessary for continued compliance.
7. Information security audits are the first step in the process of mapping threats, determining risk to specific business assets, detecting vulnerabilities, exploiting security holes and creating plans for mitigating risk and preserving long term security. To be effective, audits need to be independently conducted (with the NPO's IT's participation), repeated regularly, adapted to changing conditions and resulting high risk fixes need to be quickly applied.

### **Controls and Monitoring**

Technology is an enabler. It allows organizations to operate efficiently with relatively few resources, to store large amounts of sensitive data and to automate transactional processing. But technology can also be used to enforce security. In the hands of trained IT professionals coupled with good internal policies, it can mean the difference between an attempted attack and a security breach.

1. Security monitoring is one of the best uses of technology applied to the protection of business assets. By using technology to monitor technology, organizations have a chance to monitor and optimize defenses, detect and prevent breaches, and even compile incriminating information about cyber-criminals. Common technology includes intrusion detection systems (IDS), server and application logging, transaction logs, activity logs, network scanning, memory resident malware (malicious software) scanners, etc.
2. Network management involves the distribution of network-connected storage to comply with data classification, the distribution and application of operating system patches, the collection and analysis of log data, user management, password policies, authentication strategies, remote access, etc. Organizations with limited budgets need to weigh the benefits of granular network management practices with its benefits. The decision of investing in

network management technology carries with it the added cost of experienced professionals to run it. For larger NPOs, this investment is an absolute necessity. For smaller ones, their limited size offers the opportunity for tighter, less expensive controls that can be managed without an increase in IT staff.

Distinct, specific strategies to limit access, enforce strong passwords, enable security features (EFS, file and folder auditing, etc), securing remote access (including wireless and mobile systems), can be optimally effective in controlling costs while reducing risk to a manageable level.

## **Tools**

Distinct technology and tools used for the management of information security represent individual pieces in the overall asset protection strategy. They are managed by the IT department and are implemented specifically to support documented policies and procedures.

### **Key elements of security technology include:**

1. firewalls are an intrusion prevention system used to control network access
2. anti-virus software that seeks to detect mal-ware and disinfect systems
3. network scanners that can also automate part of the network audit process
4. intrusion detection systems with varying degrees of sophistication
5. encryption to protect the confidentiality of files and communications
6. authentication to validate the identity of authorized system users
7. data destruction software to ensure the inability of sensitive information to be recovered

Numerous technologies and solutions to emerging security problems continue to reach the market on a daily basis. Some are superbly effective at simplifying security management while others increase the complexity and the overall risk to the organization.

When selecting a solution designed to protect information security, non-profit organizations must look at the calculated risk (based on an analysis or audit), determine their ability to support the solution with human resources and training, and finally create a sustainable budget that takes into consideration ongoing licensing, upgrading and associated costs.

Regardless of the risk, the technology solution must always be the last to be selected, as part of the overall information security strategy and in conjunction with the data classification framework that has been adopted. Choosing security technology before finalizing security policies and communicating the information protection goals of the organization is a strategy that is bound to fail and carry with it a high cost both in dollars and in credibility.

## Conclusion

To conclude, this document is based on research conducted by our firm. All feedback and insight provided by Informatica's non-profit clients, including identities, shall remain confidential. The topic of information security as it applies to all organizations in this sector is vast in its implications and specifically meaningful in every context. Institutions that seek to implement proper protective measures must look at the business world for best practices and adapt available solutions to their needs, perception of risk and expected growth.

It must be emphasized that information security is a governance issue, requiring a high degree of commitment to understanding risks and threats, involving layered planning and an overall strategy. These elements together with adequate training and professional support will yield the adequate degree of risk protection, budgeting and preparedness that are critical in the long term execution of the strategy.

With all these elements in place, a non-profit organization can confidently compete in an increasingly crowded market, effectively communicate its goals and credibly demonstrate the degree of commitment that is of critical importance in gaining the trust of its audience.

## For More Information

Call: (416) 431-9012

Email: [NPO@InformaticaSecurity.com](mailto:NPO@InformaticaSecurity.com)

Visit us on the Web: [www.InformaticaSecurity.com](http://www.InformaticaSecurity.com)

Informatica Corporation  
67 Yonge Street

Toronto, M5E 1J8  
Ontario, Canada

## References

1. 2004 State Of The Nonprofit Industry Survey. BlackBaud, Inc.
2. Distinguished Philanthropy. Skloot, Edward. The Surdna Foundation.
3. Information Security for Churches and Small Non-Profit Organizations. SANS.
4. Maintaining Your Data: Internet Security. Electronic Transactions Assn.
5. Security and Privacy Issues in e-Philanthropy. Feig, Ephraim. Kintera.
6. Philanthropy is Becoming a Click-and-Give Enterprise. O’Keefe, Mark.
7. Computer Security Practices In Non-Profit Organizations. NetAction.
8. Doing Well By Doing Good: Innovative Foundation Investments in Place-Based Smart Growth Development. The Founders’ Network.
9. High Engagement Philanthropy. Filling the Performance Gap. Letts, Christine and Ryan, William.
10. Inside American Philanthropy. Nielsen, Waldemar. Norman, University of Oklahoma Press.