Damitz
Brooks
Nightingale
Turner
Morrisset

Nonprofit Insights

A Newsletter for Nonprofit Decision Makers

Summer 2018

*Who'd Rob a Charity?*

# Cybercrime: Nonprofits in the Crosshairs

**Online attacks have nearly tri-**pled in three years, according to the FBI, and hackers are increasingly targeting nonprofits alongside private-sector companies. In this threatening environment, every organization must understand its online risks and basic security requirements.

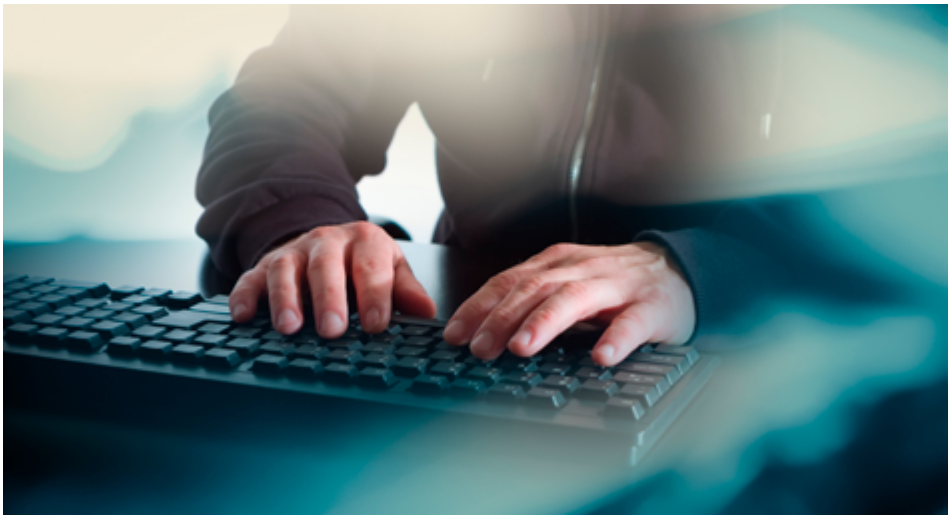
## Who's at Risk?

Your organization is courting cyberattack if it:

- conducts financial transactions online.
- collects anonymous personal information.
- stores any personally identifiable information.

It's a broad list: Most nonprofits do all three routinely, as do most businesses. The value of financial and personal data is self-evident, but anonymous data is valuable too. Its collection is less obvious, and its use is less transparent, but it's the currency of online marketing. All of this information attracts thieves.

Meanwhile, your .org domain designation raises your visibility. Most search engines add a lift in their rankings for nonprofits, so your site may show up high on a searcher's screen. That's all well and good—unless the searcher is a cybercrook looking for marks. If so, the miscreant probably knows that nonprofits lag behind for-profit companies in security.



The civilized mind recoils at robbing a charity or any worthy cause. But cybercriminals are interested in your data, not your mission.

## What's at Risk?

For as long as churches, charities, and nonprofits have received and spent money, fraudsters have tried to capture their revenues and steal their property.

Nowadays even the old standby scams usually rely on some online access—the internet can help kite a check, fake a paid invoice, or print surplus tickets to a big event. A sophisticated cyberattack can reach deeper into your organization and steal larger assets.

Ransomware is a specific kind of attack. It invades your systems, blocks your access to your own data, and demands a ransom to lift the block. Ransomware can paralyze your activity, drain your bank account, or both.

Another set of data can be even more valuable to thieves: financial and personal information about your donors, board members, employees, volunteers, vendors, and visitors to your site. How much information about credit cards, bank accounts, social security, and other business—even passwords—lies somewhere in your computer systems? A sophisticated ring that traffics in this stolen data can use it to defraud the people who trust you.

Any of these cyberattacks, if successful, would likely tarnish your

*Continued on page 3*

*Stop, Look, and Listen*

# How to Invest Wisely in Fundraising Technology

**Fundraising tools can greatly** streamline your nonprofit operations and help you increase revenue. Most tools support a part of the fundraising funnel—organizing donor information, managing events, improving email engagement, and collecting donations. Some larger tools bundle and integrate these and other features.

## Nonprofit Tech Is Accelerating

While technology is an accepted cost of doing business in the private sector, nonprofits are known for keeping outdated systems and software because of tight budgets and core values that promote frugality and thrift. However, it's worth analyzing your needs and the technology solutions on the market. A few well-chosen software tools or upgrades can help your nonprofit thrive.


## Preparing a Discussion About Technology

The following are some key points and trends in fundraising that you can address when discussing technology investments with your stakeholders:

- Expanded visibility for current and potential donors
- Recurring giving options
- Personalized communications
- Improved website function
- More reliance on insights from data
- Ad hoc partnerships with other nonprofits, when mutually beneficial

It also helps to classify areas in which updated technology can positively impact fundraising efforts, such as website traffic analysis, advertising, and email and social media engagement.

## Internal Questions to Ask

Talk to your fundraising leadership and staff about the work their teams do and their challenges. Ask them to focus on functions, not technology—the conversation will naturally bring up the fundraising tools they currently use.

The following are potential topics of discussion:

- Donors' experiences with your web presence and email campaigns
- Ability to work on short notice to build an impactful campaign
- Tool and system integration
- Mobile-friendly web experiences and challenges
- Potential to automate tasks that are currently manual and labor intensive
- Safeguards with donor information
- Trends in online fundraising
- User-unfriendly tools that freeze, crash, are difficult to navigate, etc.
- Regular team discussions around fundraising technology

By analyzing feedback from these discussions, you can identify the most pressing and long-term needs. Schedule sessions with IT, fundraising, and other leaders as needed, and then create a tech-buying committee.

## External Questions to Ask

Once you have identified the most promising tools, try them out using free trials. As you test, consider ramp-up time before your team can start using it, base price per user and add-ons that increase cost, end-user support from the vendor, and the overall advancements the tool can provide your fundraising campaigns.

Nonprofits of any size can benefit from fundraising tools that manage or track donors, prospects, volunteers, and contacts. Look for robust segmentation, reporting, and tracking features. Include software-as-a-service offerings; SaaS takes a major load off a small IT group. And look for a strong, user-friendly payment processing service.

*If your nonprofit needs upgrades to its fundraising tools, our nonprofit and technology consultants can help you make valuable investments.*

# How to Defend Against Cyberattacks

*Continued from page 1*

brand and your organization. Insurance may cover some damages, but it can't protect trust, and trust lost is hard to regain. For some nonprofits, such cyberfraud can be fatal.

## Lowering Your Risks

***Calculate your potential loss*** from data theft. Segment your data—donors, employees, etc.—and estimate the damage your nonprofit might sustain if that data were stolen and sold to bad actors. Estimate a range for each constituency, and stress objectivity.

***Identify weak spots***. Aging operating systems or financial software should especially stand out. Consult with a reputable cybersecurity company for a vulnerability scan and penetration test to detect weaknesses. Don't neglect mobile in these reviews.

***Upgrade your systems.*** Nonprofit tech staffs have patched older systems for years, heroically in many cases. But upgrading is a standard business requirement today, and nonprofits can't avoid it. Your decision on systems, software, and hardware upgrades—which, when, and how—can have significant consequences.

***Invest in technology***. What are the most tedious and unnecessary tasks? Could some parts of your nonprofit machine contribute more to the overall mission if you automated or combined some tasks?

Software abounds in the nonprofit industry, so you should weigh reputation and reviews along with cost. Don't skimp on a vigorous antivirus defense or a strong, well-regarded payment processor.

***Upgrade your security consciousness.*** Most cybercrooks hack people, not systems—it's easier. Making it harder takes clear protocols and rules—automatic software updates, strong passwords changed regularly, two-factor authentication, and others. But it mainly takes a culture. Do phishing emails get bites? If you don't know, test. Most of all, train. Formally, informally, lunch and learn—security can be interesting.

***Maintain and back up.*** When hiring a new IT professional, nonprofit is a bonus, but focus on tech skills. Putting your people and investments to work calls for well-oiled IT, from software updates to onboarding and a help desk.

Meanwhile, robust data backup plans and systems are becoming a requirement. To approach 100 percent effectiveness, a backup system must be real-time, 24/7, automatic, offsite, redundant, and secure.

## Insurance

Should you insure your data? It depends on what's at stake, how confident you are in your systems, and how you want to balance the two. As the price of data protection drops with new products and services, more nonprofits are likely to cover their potential liability with insurance.

Maintaining best practices in data security will ease a nonprofit's insurance cost. With or without insurance, use these principles to protect your assets and reputation today.

*Our firm can help you assess the state of your sensitive data and the systems and processes that protect it.*

## *European Privacy Law Affects U.S. Nonprofits*

The General Data Protection Regulation (GDPR), which took effect May 25, is the European Union's new data privacy law. It governs any digital information that can be linked to an individual.

It applies to any organization that collects personal data from any person in the EU, with or without payment. Violators of the GDPR's data security requirements will be fined, regardless of a company's location. Meanwhile, other countries are signaling they may use the GDPR as a model for their own regulations.

So, if your nonprofit sells so much as a coffee mug to a Berliner, you'll need to review the GDPR.

Our goal is to provide the highest quality tax, accounting and consulting services for our clients.

DAMITZ
BROOKS
NIGHTINGALE
TURNER
MORRISSET

*Certified Public Accountants and Consultants*
*A Professional Corporation*

*200 East Carrillo, Suite 303*
*Santa Barbara, CA 93101*
*805-963-1837 Fax 805-564-2150*

# Is Your Nonprofit a "Foreign Agent"?

**Foreign interference in U.S. politics** has been in the news lately, and the controversy affects nonprofits in one important way.

Congressional efforts are under way to step up application of the Foreign Agents Registration Act (FARA)—a law enacted in 1938 amid war and rumors of war to counter pro-German propaganda. Its broader purpose was to inform the American public about foreign attempts to influence public opinion and policy.

FARA requires U.S. persons and organizations that engage in certain activities on behalf of foreign entities to register with, and report regularly to, the Department of Justice. The law specifies five types of activities: political, public relations, political consulting, publicity, and information services.

FARA defines "foreign agent" broadly. That makes the law hard to enforce and has been rarely invoked. If enforcement proceeds now without further guidance, the law's ambiguities will pose a challenge to nonprofits trying to determine their standing.

*Congressional efforts are under way to step up application of the Foreign Agents Registration Act.*

For example: A Dutch group drafts a policy paper addressing environmental damage and asks a U.S. nonprofit to organize a public forum or a session at a conference to discuss it. Because the nonprofit is acting at the behest of a "foreign principal," does that make it a foreign agent? According to the letter of the FARA law, it does.

The law provides some exemptions, including academic, religious, and certain charitable activities. But if your nonprofit fits FARA's definition, you'll have to register with the Department of Justice as a foreign agent. You'll also need to submit semiannual reports about your activities. And noncompliance can bring criminal penalties.

Some organizations may drop international activities and collaboration rather than face the burdens of registration and reporting. Others will need a careful and detailed review of their activities along with FARA's provisions.