CYBERSECURITY ESSENTIALS FOR PHILANTHROPY

Funder Briefing:
Supporting Cybersecurity With Your Grantees

Published on October 15, 2019

Amy Sample Ward, CEO, NTEN
Chantal Forster, Executive Director, Technology Affinity Group
Karen Graham, Director of Education & Outreach, Tech Impact

TECHNOLOGY AFFINITY GROUP

One North State Street, Suite 1500
Chicago, IL 60602

info@tagtech.org

OVERVIEW

A CALL TO PHILANTHROPY

Thriving communities and the outcomes we can help them achieve are what motivate us to do philanthropic and capacity building work. But too often we overlook a risk that could negate all our best efforts if we fail to manage it—a risk that is ever more prevalent: cybersecurity.

The cost of prevention and planning is low relative to the cost of a single catastrophic breach. Yet many nonprofit organizations struggle to make even minimal investments in improving cybersecurity. This problem does not exist for lack of information or services—Tech Impact and NTEN both provide numerous knowledge resources and security services tailored to the needs of nonprofits of all sizes—but rather due to a lack of awareness, prioritization, and funding.

Think about how the nonprofit sector has grown to be more data focused, thanks in part to leadership and capacity building support from foundations that demanded a higher standard. Similarly, foundations could play an important role in boosting the sector to a higher level of cybersecurity.

We are calling on all foundations to take a leadership role in lifting grantees to a higher level of cybersecurity.

NTEN, TAG, and TechImpact are pleased to be collaborating to elevate cybersecurity as a sector-wide concern. The first step to making a change is to build awareness among those with the ability to do and fund capacity building work. That means the conversation must extend beyond IT professionals and include foundation leaders and program staff. Please share this briefing with someone who can make a difference.

AMY SAMPLE WARD
CEO, NTEN

CHANTAL E. FORSTER
Executive Director, Technology Affinity Group

PATRICK CALLIHAN
Executive Director, Tech Impact

FUNDER BRIEFING: SUPPORTING CYBERSECURITY WITH NONPROFIT PARTNERS AND GRANTEES

This briefing answers two questions: *How can foundations better support cybersecurity among nonprofits and grantees? And what is the responsibility of grantmakers for cybersecurity in the sector?*

With input from cybersecurity experts and nonprofit staff, we've written this briefing together with peers at foundations like yours to assess the current landscape and provide pragmatic strategies for supporting grantees. In this briefing, you'll find:

1. The state of cybersecurity among nonprofit organizations
2. Guidance on providing direct funding for security projects
3. Capacity building grant ideas for cybersecurity
4. Where to locate resources specific to grantees' size and structure
5. Thoughts on how to set standards for grantees while avoiding unfunded mandates

Let's get started.

CURRENT STATE OF THE SECTOR

CYBERSECURITY CHALLENGES FOR NONPROFITS

Although awareness of cybersecurity risk and best practices is starting to build among nonprofits, there is a still an alarming gap between the current state and best practice. This is a threat to the sector, to the essential programs and services it provides, and the communities that entrust their personal data to us.

> **"Grantees come to us saying, 'We're in crisis, a ransomware attack is going to cost us thousands of dollars, what should we do?' There are too many sad stories from our community about organizations that had security breaches because they were unaware and unprepared."**
>
> **Amy Studwell, Senior Nonprofit Support Program Officer, Hartford Foundation for Public Giving**

We need to address this—not just within our own foundations, but also among our grantees and nonprofit partners—because the risks are on the rise. For example:

- Risks associated with unsecured Wi-Fi and lost or stolen devices are increasing as work teams become more distributed, and with staff using personal devices to access organizational data and accounts. In a 2018 survey conducted by NTEN[1], with funding from Microsoft, **71 percent of respondents indicated that their staff use unsecured devices for this purpose**.
- Adoption of password policies and multi-factor authentication (MFA) is emerging, but not yet widespread, and **less than half of NTEN survey respondents use MFA**. Only about 40 percent of respondents to the NTEN survey reported that they regularly provide cybersecurity training to staff.

> **"Cyber-crime has a huge negative impact on the community. It disrupts services, diverts resources from programs, and compromises the privacy of our most vulnerable populations."**
>
> **Steve Haviland, CEO, Think of IT**

The existence of policies that address security and privacy concerns is one bright spot. The NTEN survey shows that 71 percent of nonprofits report having backup policies and 55 percent have policies identifying how their organization handles cybersecurity risk, equipment usage, and data privacy.

However, even with strong protections in place, not all attacks can be prevented. Are nonprofits adequately prepared to respond to attacks? In the NTEN survey, only 21 percent said they have **breach-specific** policies and procedures that guide behavior during and after an attack. A cyberattack can have severe consequences not just for operational continuity, but also for an organization's reputation and for the privacy and safety of the people it serves.

In a nutshell, cybersecurity among nonprofits is not what it should be. Why is that?

[1] https://www.nten.org/article/2018-state-of-nonprofit-cybersecurity/

BARRIERS TO IMPROVING SECURITY

> **"Grantees don't always know what the right solutions are and which budget they should come from. The [funding] system incentivizes spending on programs, and infrastructure spending is bad."**
>
> **Kate Bertash, Director, Digital Defense Fund**

There is growing consensus that cybersecurity is a problem in the nonprofit sector. Lots of tools and practices exist that could make nonprofits safer—so why aren't we seeing more progress? There are a few reasons:

- **Lack of funding.** Many foundations consider technology to be part of overhead and outside of their funding guidelines.
- **Competing priorities.** Faced with a choice between providing direct services and improving cybersecurity, some leaders feel their only option is to leave cybersecurity to chance. Some also struggle with the tension between an open, flexible culture and central, locked-down technology administration.
- **Lack of executive buy-in.** Without a mandate from leadership, cybersecurity initiatives flounder.
- **Weak overall IT infrastructure.** If the IT environment is bare-bones and professional IT advice and management is lacking, security can easily slip through the cracks.
- **Lack of knowledge**. Nonprofit leaders might be experts in their mission focus areas, but they often lack a high level of operational knowledge when it comes to cybersecurity.

These interconnected barriers are tough to overcome, but there are ways foundations can support nonprofits to build a more robust security posture. Doing so will help us all.

THREE WAYS TO BOOST NONPROFIT CYBERSECURITY

Three important ways to give the sector a "cybersecurity boost" are by providing direct funding for cybersecurity projects, offering capacity building grants, and supporting knowledge resources.

DIRECT FUNDING FOR PROJECTS

Providing funds for a basic security assessment or audit is a great place to start. Such assessments identify risk and prioritize improvements, costing roughly $5,000-$10,000 for a small organization. According to Kate Bertash of the Digital Defense Fund, such an investment is small when compared against the risk. "A nonprofit's cost could be $50,000 to $60,000 for a single breach," she said. "Prevention is not that expensive, and it means so much."

Targeted funding can go a long way to make assessment and improvements possible. For example:

- Child Care Aware of America implemented a data center with funding from the Robert Wood Johnson Foundation. Kris Kraviec, the foundation's Director of Software Architecture and Development, provided guidance on the project to help select tools and architecture that met both functional and security requirements.
- The Digital Defense Fund provides funding and expertise to improve cybersecurity among reproductive rights and abortion access organizations.
- Think of IT, in partnership with Rotary Clubs and the nonprofit center at Midwestern State University, is awarding three organizations a combination of security services, managed IT services, and virtual desktop services for one year plus $5,000 cash to help with upgrades.

However, in our inquiries, we found *zero* examples of foundations providing funding exclusively for grantees to make cybersecurity improvements at the grantees' discretion. All funding included advice or directives from the foundation. While sometimes helpful, this can also create an unhealthy power dynamic and risk of the grantee not being fully committed to maintaining improvement. It can limit the grantee in choosing the advisory and support services that best fit their needs.

> **"Straightforward funding for grantees to assess cybersecurity and make improvements—with no strings attached—would go a long way toward making nonprofits better protected and more resilient. It would be a bold move for a foundation to say yes, security is important, and we want grantees to have the power to lead this."**
>
> **Karen Graham, Director of Education and Outreach, Tech Impact**

What about security infrastructure and monitoring, which has an ongoing cost? This requires either general operating funding or ensuring sufficient administrative expenses are built into program grants.

If you want to provide funding for security improvements, there are these options:

- Consider adding a small amount of additional funding to a grant to support a security assessment. Be open to additional funding requests for implementation based on the results and recommendations of that assessment.
- Create a special grant pool for $5,000-$15,000 grants to existing grantees with a simple application and reporting process. This is best suited for foundations that normally provide much larger grants.

> **"Imagine if funders expected technology costs to be included with every single grant application they review. This would support an investment in and the capacity for strategic cybersecurity protections."**
>
> **Amy Sample Ward, CEO, NTEN**

CAPACITY BUILDING

In order to build an organizational culture where cybersecurity is prioritized, nonprofit leaders need to improve their knowledge and skills and get expert advice. Capacity building grants give them access to professional development and consulting services. Below are examples of foundations providing direct support for cybersecurity with their grantees:

- The Hartford Foundation is offering a half-day workshop on security basics for executive directors in late 2019. They will also be sharing stories about organizations that fell victim to ransomware or other attacks, so that others can learn from them.
- The Keith Campbell Foundation for the Environment provides funding for technology projects including consulting services, covers expenses to attend conferences, and provides scholarships to technology courses.
- The Pierce Family Foundation provides cybersecurity training for grantees focused on "personal firewall" anti-phishing awareness, incident response procedures, and setting up multi-factor authentication.

> **"Many nonprofits think they will not get attacked because they're doing good work, which of course makes no difference to a bad person with a set of email addresses. Nonprofits need the same security as large businesses!"**
>
> **David Krumlauf, Chief Technologist, Pierce Family Foundation**

KNOWLEDGE RESOURCES

Support from private and community foundations is essential in order to produce and disseminate high quality, impartial knowledge resources and keep them up to date.

> **"The technology capacity of nonprofits is essential to their ability to achieve their goals, and yet funders do not typically include grantees' technology needs in the scope of work related to those goals. How do we consistently partner with nonprofits during the grantmaking process to ensure they have the technology they need to reach their objectives?"**
>
> **Michael Smith, Manager of Information Systems, Hass Jr Foundation**

Several nonprofit organizations are doing great work in the area of providing knowledge resources. Below are some of the resources our organizations have provided:

- The State of Nonprofit Cybersecurity report by NTEN
- Cybersecurity Basics and Nonprofit Technology Policy guide by TechImpact

More general resources on nonprofit technology and digital transformation include TechSoup's Microsoft Digital Skills Center and Net Hope's Center for the Digital Nonprofit.

Additionally, it is imperative to make sure grantees are aware of discounts on security tools and services. These benefits are available to nonprofits through TechSoup and directly through providers such as KnowBe4.

RAISING THE BAR

PARTNERING TOWARD A NEW STANDARD

How else might foundations move with their grantees toward a higher level of cybersecurity?

Program officers and program directors have opportunities to create fertile ground for cybersecurity improvements. Asking a question about cybersecurity in grant applications, especially when the grant involves tracking personally identifiable information, is one way to shine a spotlight on this issue.

For example, the Rockefeller Foundation uses a 15-point questionnaire as part of due diligence when a grant application includes collection of sensitive data. They make their staff of network engineers and data scientists available to give advice and flag potential problems or risks.

> **"If we ask grantees to collect data, we want to make sure they have security measures in place. If they are breached, that affects our reputation too. We don't want to overstep our bounds, tell them how to do things or whom to talk to. But we make suggestions."**
>
> **Carolyn Wendrowski, Chief Technology Officer, Rockefeller Foundation**

Program officers must be knowledgeable about security standards, know how to flag this as a concern in their grantmaking, and know how to partner with their grantees to protect their data. The knowledge resources in the *Cybersecurity Essentials for Philanthropy* series from TAG, as well as those for nonprofits, will help your program staff to become more knowledgeable about cybersecurity issues. If you need additional expertise, consider inviting a technology professional to be part of your grant review committee.

Of course, there are some pitfalls to creating standards. Foundations should be cautious of creating an unfunded mandate by raising expectations without providing other support to help grantees improve. Also, foundations must be sensitive when inquiring about cybersecurity. Nonprofits may feel they need to hide their shortcomings from funders, fearing that if a security risk is revealed, funding will be denied.

A VISION FOR THE FUTURE

We envision a future where every nonprofit is well-protected from cybersecurity threats and can deliver confidently on their missions. Through honest conversations about overhead and risk as well as various types of direct support, foundations can help nonprofits get there.

Where can you start?

- ✓ Provide direct funding for security assessments and improvements.
- ✓ Include cybersecurity training and access to security consulting services in your capacity building programs.
- ✓ Share knowledge resources about cybersecurity with your grantees.
- ✓ Engage in open conversation with grantees about their security concerns and needs.
- ✓ Educate program staff on data security so that they can spot opportunities for support.

RESOURCES

Below are links to the tools and resources referenced in this document

- Microsoft Digital Skills Center by TechSoup
- Center for the Digital Nonprofit by Net Hope
- The State of Nonprofit Cybersecurity report by NTEN
- Cybersecurity Basics and Nonprofit Technology Policy guide by TechImpact
- Cybersecurity Essentials for Philanthropy series by TAG

ABOUT THE AUTHORS

AMY SAMPLE WARD

CEO
NTEN

CHANTAL FORSTER

Executive Director
Technology Affinity Group

KAREN GRAHAM

Director of Education & Outreach
Tech Impact

ABOUT THIS SERIES

The *CyberSecurity Essentials for Philanthropy* series launched in 2019 is provided by the Technology Affinity Group (TAG) in partnership with member organizations and private sector advisors.

View the full curriculum available for the series at: tagtech.org/cybersecurity

This is an educational publication and is not intended as legal advice. You should contact your attorney for legal advice. The opinions expressed here are the opinions of the individual authors and may not represent the opinions of their employers or of TAG.

TAG CYBERSECURITY WORKING GROUP

This work is led on a volunteer basis by the TAG Cybersecurity Working Group whose members include the following:

Jim Rutt (Chair), Dana Foundation
John Mohr, The MacArthur Foundation
Oleg Bell, Open Society Foundations
Karen Graham, Idealware
Darlene Ott, The Winnipeg Foundation
Dan Callahan, CGNET
Calvin Lewis, Cleveland Foundation
Christopher Jean-Pierre, Wellspring Philanthropic Fund
Steve Jarboe, Accenture
Anthony Putignano, Wizehive
Charles Boname, Vancouver Foundation

FUNDING PROVIDED BY

This series is funded in part through an award from the Robert Wood Johnson Foundation President's Grant Fund at the Princeton Area Community Foundation.