THE CHRONICLE OF PHILANTHROPY

DEREK BRAHNEY FOR THE CHRONICLE

CYBERSECURITY

By Ben Gose

JANUARY 11, 2022

It's not immediately obvious why cybersecurity would be a top priority for Land Is Life, a New York nonprofit that works internationally to help organizations led by Indigenous people to protect their way of life. After all, the group often works with people who have had little exposure to modern technology, and many grant applicants apply by phone.

Related Content

How Organizations Can Protect Themselves From Cyberattacks

But cyberattacks are a growing menace to nonprofit organizations around the world, and Land Is Life is no exception. Its security fund distributes small grants totaling around $400,000 a year to assist Indigenous activists and charity leaders who have faced threats. Land Is Life received pro bono assistance from a student-led clinic at the University of California at Berkeley's Center for Long-Term Cybersecurity to make sure the grant applications — and the charity's own data — are secure and don't fall into the hands of those threatening Indigenous people in the first place.

"One of our coordinators in Colombia is also an activist," says Ana Jerolamon, interim co-director of Land Is Life. "She is threatened on a daily basis digitally. We wanted to ensure that information submitted by grant applicants would be secure."

Land Is Life has plenty of company, as more and more charities seek to keep their data safe from cyberattacks. In just the past few months, BoardSource, a research and support organization for nonprofit boards, and Planned Parenthood Los Angeles have gone public about data breaches by cybercriminals.

For years, most charities spent little on cybersecurity, due in part to a lack of funds but also out of a sense that government agencies and businesses would be more likely targets for hackers. That complacency ended after the 2020 ransomware attack on Blackbaud, which affected many charities in the United States and around the world. The good news, tech experts say, is that a growing number of companies and tech-focused charities are offering free or low-cost expert help to address the threat.

"Until recently, data security has been a 'nice to have' for nonprofit organizations," says Michael Enos, senior director of community and platform for TechSoup, a charity that provides technology systems and assistance to other organizations. "Now it's a must have."

For most nonprofits, he says, reputation is everything. If an organization suffers a breach because it was careless with data, donors may flee. "It takes a small period of time for years and years of brand development to go down the tubes if you mishandle this."

Tempting Targets

Nonprofits are an attractive target for cybercriminals because many do little to defend against attacks yet possess valuable data, including donor records. The pandemic, which led to an abrupt change to remote work, left many charities even more exposed.

Microsoft's Digital Security Unit says nonprofit organizations are the most common target for cybercriminals motivated by nationalism.

"Cybercriminals are starting to realize that nonprofits and NGOs are a fantastic market," says Adrien Ogée, chief operating officer of the CyberPeace Institute, an organization in Geneva that works to enhance the stability of cyberspace.

Few charities are prepared to rebuff or respond to intrusions. Roughly 70 percent of the nonprofit organizations that Microsoft works with have not conducted a basic risk assessment to understand where vulnerabilities may exist in their technology infrastructure. And a 2018 survey — the latest available from

NTEN, a nonprofit that helps charitable organizations with technology — found that only 21 percent of nonprofits had plans to respond to a cyberattack.

Sensitive Data

The Blackbaud breach primarily exposed data about donors and the size of their contributions. But it's not hard to envision worse scenarios. Land Is Life's security program helps Indigenous people threatened by governments or others relocate to safer areas or set up security cameras in their homes. Cyberattackers could use stolen data from grant applications to locate and physically attack the Indigenous activists.

BENETECH

Too many nonprofits use homegrown or customized software programs that leave them vulnerable to attack, says Jim Fruchterman, CEO of Tech Matters.

Plenty of nonprofits have sensitive data about vulnerable people, but most aren't doing a good job of securing it, says Jim Fruchterman, founder and CEO of Tech Matters, which helps social-change organizations better use technology. He says he's aware of at least one nonprofit that sent an email with an unencrypted file that included personal information about sexual-assault survivors.

"Nonprofits tap into sensitive issues, and we don't treat that data with the respect it deserves," Fruchterman says. "What happens when a leak of child sexual-abuse survivors gets posted on some list? Are we taking the steps necessary to prevent that?"

Part of the problem, Fruchterman says, is what he describes the "cult of the custom" — the homegrown or customized software systems that many charities use, which are more likely to be vulnerable to cyberattacks. The needs of for-profit businesses tend to be more standardized, and they can afford to pay more, which means tech companies are more likely to create comprehensive software packages to serve them. All too often, nonprofits "have a half-time IT person who throws something together," Fruchterman says.

"If I run a golf course, I have three choices of software to manage a tee time," he says. "If I'm helping the most vulnerable children on the planet, I've got an Excel spreadsheet and paper."

Broad, Automated Attacks

Technology isn't the only problem. The way nonprofits think about the threat of cyberattacks can be just as important. A major hurdle for many organizations is "lack of agency" — the feeling that they simply can't match up against the dark forces trying to hack into their systems, says Ann Cleaveland, executive director of Berkeley's Center for Long-Term Cybersecurity.

"Nihilism is probably too strong a word — but definitely everybody is feeling overmatched," she says.

Other charities, meanwhile, are too complacent. They believe they're far enough off the radar that no attacker would ever target them.

"That's what we hear a lot: 'No one wants my data,'" says Amy Sample Ward, NTEN's chief executive. She says the value of the data often isn't the point for cybercriminals. "They're not interested in keeping it — they just know you're going to pay to get it back, or you'll pay to avoid the reputational damage."

Groups That Can Help

Access Now
This global organization, which advocates for digital privacy, runs a 24/7 helpline for civil-society groups that have experienced cyberattacks.

Citizen Clinic
This student-led effort at the University of California at Berkeley's Center for Long-Term Cybersecurity helps civil-society organizations build greater capacity to defend against digital threats.

CyberPeace Builders
Corporate volunteers in this effort of the CyberPeace Institute help charities around the world strengthen their capacity to defend against attacks.

Microsoft Security Program for Nonprofits

that alerts users when their email or productivity software is hacked. How Organizations Can Protect Themselves From Cyberattacks

She says the image of an evil hacker relentlessly working to break through a system's security is no longer accurate. Instead, cyberattackers are casting a wide net with increasingly sophisticated tools and waiting for someone to screw up.

"It's not the controversial, really prominent organizations that are vulnerable," she says. "It's any organization at this point."

The tools used by cybercriminals — including for phishing attacks designed to get people to reveal sensitive information — are increasingly automated, says Rob Shavell, chief executive of the online-privacy company DeleteMe. "It's easier to cast a broad net than it has been in the past," he says. "They basically automate the software and just wait for people to fall into the traps. Smaller organizations and organizations that never thought they would be targets have become targets."

A report released in May by Verizon that looked at cyberattacks on businesses found that 85 percent of the breaches resulted from somebody making a mistake, such as falling for a phishing email.

Nonprofits need to make sure that all employees receive training in how to detect phishing emails and other unusual requests, says Emily Phan, executive technology officer at Stand for Children, an education advocacy group.

"A big part of vulnerability in today's day and age, regardless of the size of your organization, is the naïveté of your users," Phan says.

Enos of TechSoup says a phishing scheme aimed at charity employees might come from a source posing as the charity's CEO, urgently demanding that large quantities of gift cards be sent to a "donor."

"Unless you look closely, you can be easily fooled," he says.

'Who Is This Email From?'

Many companies that provide education about cybersecurity also offer services to conduct unannounced simulated phishing attacks to test employees. Microsoft has found that businesses and organizations that carry out such simulations were 50 percent less susceptible to phishing.

Catholic Relief Services tests staff members repeatedly to help them "build that muscle" to detect phishing,

COURTESY OF JIM STIPE FOR CATHOLIC RELIEF SERVICES

Catholic Relief Services conducts simulated phishing attacks to help employees learn to recognize them, says Joel Urbanowicz, the group's director of digital workplace services.

"We want them to pay attention to what they're seeing," he says. "Who is this email from? How is it written? Are they putting pressure on me to do something quickly in a way that doesn't feel right?"

Catholic Relief Services got serious about cybersecurity in 2017 after a breach in Central Africa that involved data related to program participants, although no personal information was ultimately lost. "It could have been a significant loss, but we managed it appropriately, and it turned out to not have an impact on program participants," Urbanowicz says.

Nevertheless, the incident helped persuade the charity's leaders to invest in a full-time staff dedicated to cybersecurity. The unit now has a staff of seven serving an organization with roughly 7,500 employees worldwide, at a cost of over $1 million per year (though the organization spends only about half as much per employee as the $535 median at for-profit and nonprofit organizations.)

By creating a unit focused just on cybersecurity, Urbanowicz says, he was able to make someone responsible for avoiding a repeat of the 2017 breach.

The biggest challenge has been filling open cybersecurity positions. For-profit companies and the federal government scoop up much of the local talent. (Catholic Relief Services is based in Baltimore, not far from Washington, D.C.) Urbanowicz says he frequently has to hire people without any experience and hope they grow into the position. He's also trying to hire people at the nonprofit's international offices, but he says it is still challenging to find candidates with experience.

The shortage of candidates doesn't affect just charities; some of the biggest players in technology are beginning to take action. In October, Microsoft launched a national campaign with community colleges to recruit 250,000 people into the cybersecurity work force by 2025.

New Sources of Help

Finding workers is just one challenge for charities. Paying them is another. Urbanowicz says Catholic Relief Services has used unrestricted donations to expand its cybersecurity force.

Cybersecurity is expensive. The typical for-profit corporation spends $8,000 per employee per year on technology; charities typically spend $3,000, according to research conducted by the Berkeley center. Of that amount, a nonprofit might spend only 5 to 10 percent on cybersecurity — or about $225 per employee per year. Most experts say that's not nearly enough.

Foundations and donors have historically been part of the problem. Foundations have opened their wallets to protect their own operations — 61 percent of foundations pay for cybersecurity insurance, according to a 2020 study by the Technology Association of Grantmakers, and roughly the same share hire outside security firms to conduct simulated phishing attacks.

But they have been less eager to help cover the costs of cybersecurity for grantees — for the same reason that grants for general operating support remain relatively rare: Many foundations and individual donors prefer to pay for programs.

"Nonprofits tap into sensitive issues, and we don't treat that data with the respect it deserves."

"Donors want nonprofits to spend only a certain amount of money on overhead, but they don't realize that they're putting their own contributions under threat because nonprofits won't have the ability to protect their data or the funds that they get from donors," says Ogée, COO at the CyberPeace Institute.

Some grant makers, including the William and Flora Hewlett Foundation (a financial supporter of the *Chronicle)*, Craig Newmark Philanthropies, and the Gula Tech Foundation, have made cybersecurity a

particularly technology billionaires — to increase the sliver of philanthropic spending that goes toward cybersecurity.

But many nonprofit tech experts believe donors need to support cybersecurity more explicitly as part of their everyday grant making. "A lot of this stuff shouldn't even be considered overhead," Fruchterman says. "It should go into the direct cost of the grant."

Corporate donors have also contributed to the problem. Historically, many tech companies have donated equipment or software to charities but haven't done enough to help them figure out how to use it.

"When working with nonprofits, particularly underresourced nonprofits, the latest whiz-bang tech solution isn't going to help them," Cleaveland says. "They don't have anybody who can administer it after the company walks away."

Today, more companies are figuring out that what charities really need is donated technology expertise. In October, Microsoft launched a new security program for nonprofits with a goal of working with 10,000 organizations this year and 50,000 within three years. The program includes free access to a program that alerts organizations when their accounts have been compromised, as well as free security assessments and training for IT administrators and others.

An increasing number of nonprofits are also offering help. Access Now, a global organization that advocates for digital privacy, runs a 24/7 helpline for civil-society organizations that have experienced cyberattacks. The hotline, with offices in Tunis, Manila, and San José, Costa Rica, now receives about 250 calls a month, up from just 10 when the hotline started in 2013.

Over the summer, the CyberPeace Institute created a network of volunteers, called CyberPeace Builders, that will provide up to 120 hours of pro bono cybersecurity assistance to nonprofits. The network hopes to help 1,000 nonprofits and develop a network of 3,000 volunteers by 2025.

Berkeley's Center for Long-Term Cybersecurity also has big expansion plans for its Citizen Clinic — the one that assisted Land Is Life. The center, along with the Massachusetts Institute of Technology, the University of Alabama, Indiana University, and others, has launched the National Consortium of Cybersecurity Clinics. The consortium hopes to add more college and university partners and spread to states and regions throughout the country, helping small nonprofits and others that can least afford cybersecurity technical assistance.

"We are very hopeful that funders will be interested in this," Cleaveland says. "It's a way of addressing this market failure — a way of getting around this issue of helping nonprofits that are starved for overhead."

A version of this article appeared in the January 11, 2022, issue.

We welcome your thoughts and questions about this article. Please email the editors or submit a letter for publication.

TECHNOLOGY

Ben Gose

Ben Gose has written for the *Chronicle* since 2002 and has done profiles of several major philanthropists.