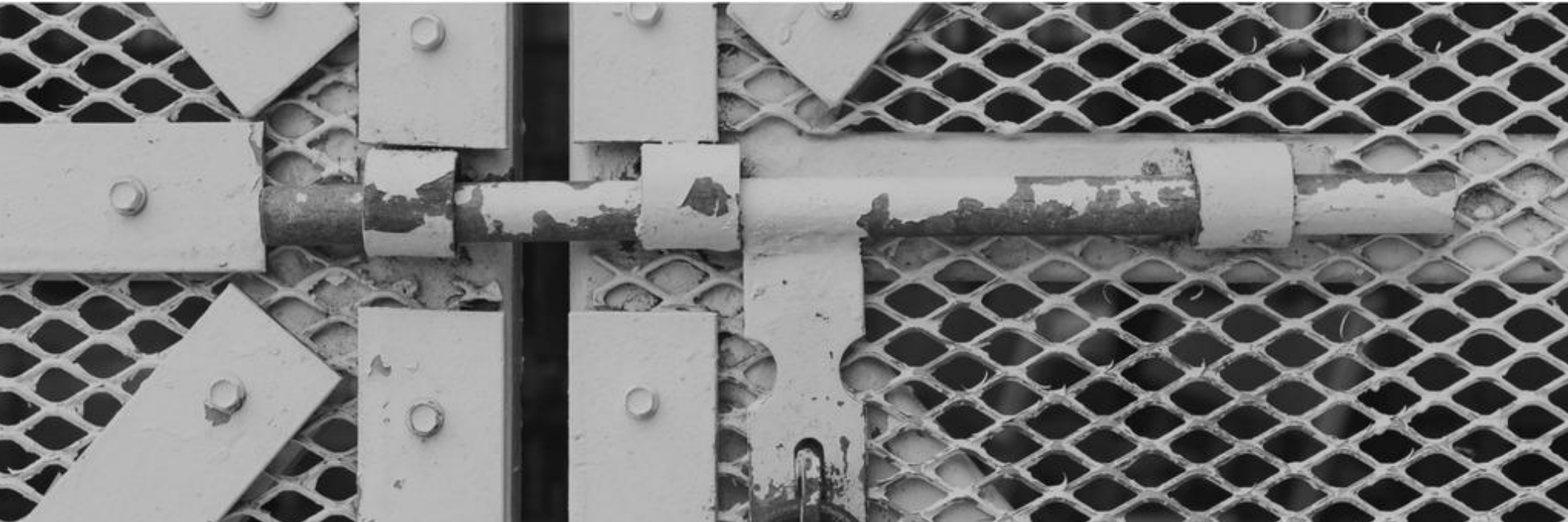


# Cybersecurity Risks for Nonprofits

9 Things You Need to Know

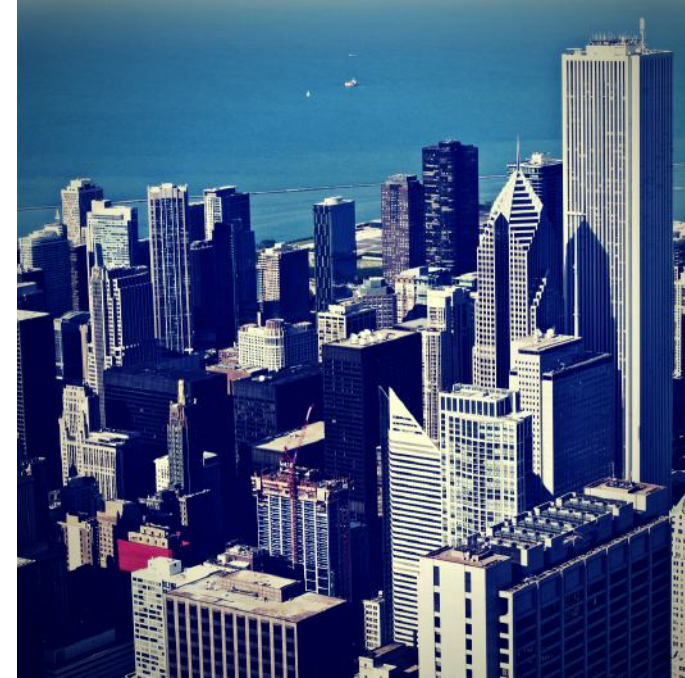


**Nonprofits think they are protected by virtue of their inherent altruism . "I'm doing good work, so who would possibly want to hurt me? I'm doing good for the world."**

**Becker Polverini, CEO, Co-Founder, PKC Security**





The logo for PKC Security, featuring the letters "PKC" in a large, bold, sans-serif font, with the word "SECURITY" in a smaller, bold, sans-serif font directly below it. The text is white and is set against a dark gray rectangular background, which is itself framed by a thin white border.

GlobalPueblo  
asked PKC Security:

**What do  
nonprofits  
need to know  
about  
cybersecurity?**

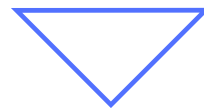
PKC Security is a cybersecurity firm specializing in securing communications and data from global threats. Their clients receive personalized security solutions that leverage technical capabilities in three functional areas of expertise: software, security planning, and infrastructure security.

We interviewed Becker Polverini, CEO and Co-Founder, and Ken Kantzer, Co-Founder, on how nonprofits, both domestic and global, can effectively navigate cybersecurity issues within their organizations.

# Cybersecurity Risks for Nonprofits

## What are 9 things you must know?

1. Have the right **mindset** about security
2. Decide who leads the **IT governance** on this
3. Gain awareness of **top cybersecurity risks** now
4. Why cybersecurity is **not a cost center**
5. The benefits of being **proactive** vs. reactive
6. What you need to know **if you're global**
7. How to best identify **your risk areas**
8. How to prioritize and respond to **threats**
9. Where to start with **best practices**



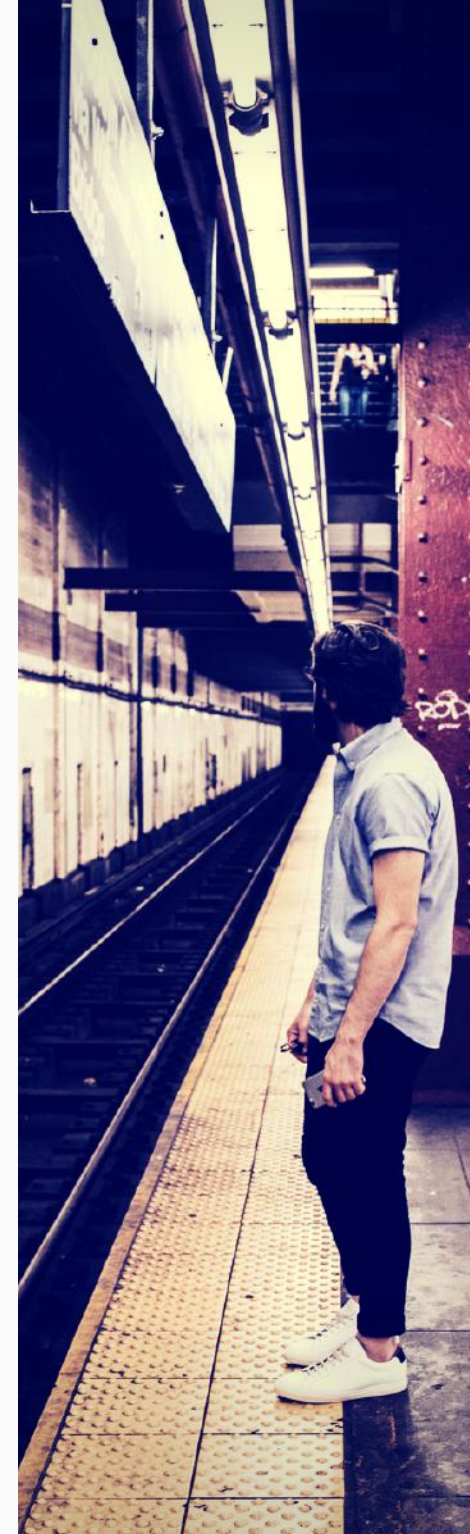
## WHAT MINDSET CAN A NONPROFIT HAVE THAT CAN GET IN THE WAY OF ADEQUATELY PROTECTING THEMSELVES AGAINST CYBERSECURITY RISKS?

Becker: There are four things we need to dispel generally when we work with nonprofits.

1. The biggest one is that **nonprofits think they are protected by virtue of their inherent altruism.** "I'm doing good work, so who would possibly want to hurt me? I'm doing good for the world."

The issue with that is that cyber criminals just don't care who you are, what you're doing or why you're doing it. The only thing that they look for is opportunity. They want to find the easiest target, the lowest hanging fruit. Then they just use the same technique they use on anyone else in order to try to find wealth that they can steal.

Altruism has nothing to do with it. No matter your mission you're going to end up just being vulnerable.



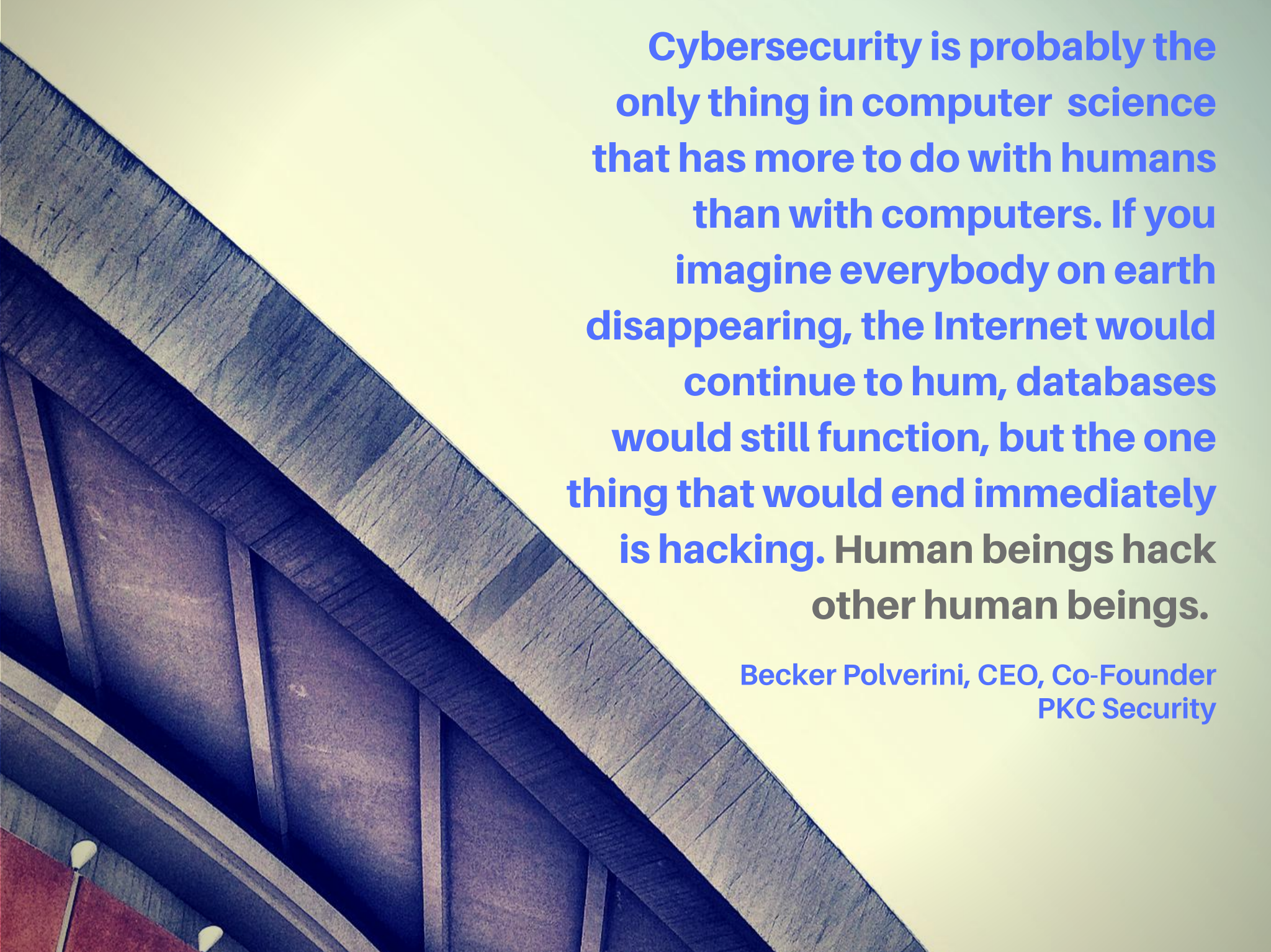
## WHAT MINDSET CAN A NONPROFIT HAVE THAT CAN GET IN THE WAY OF ADEQUATELY PROTECTING THEMSELVES AGAINST CYBERSECURITY RISKS? (CON'T.)

2. Becker: A second misconception is, “**Well, I’m just a poor nonprofit, I don’t have anything valuable.**” That’s also completely false. There’s intrinsic value in the social networks that a nonprofit has particularly with their donor database and the people that their donors know. Also, donors tend to be people with resources and connections. Those are perfect targets, the kind of people that you want to target. In other words, the people that have enough money to donate to a nonprofit are also the people that have enough money from whom to steal.

3. The other thing that’s really valuable is just **losing face with your donors**: losing the social capital you have with them. If they see that they’re getting an email from you that is obviously spam or an indicator that you’ve been hacked, good luck trying to get them to donate to you again.

The fear of losing their identity or becoming a victim of identity theft by virtue of donating to your organization is going to absolutely inhibit any opportunity you have to get them to donate again.





Cybersecurity is probably the only thing in computer science that has more to do with humans than with computers. If you imagine everybody on earth disappearing, the Internet would continue to hum, databases would still function, but the one thing that would end immediately is hacking. Human beings hack other human beings.

Becker Polverini, CEO, Co-Founder  
PKC Security

## WHAT MINDSET CAN A NONPROFIT HAVE THAT CAN GET IN THE WAY OF ADEQUATELY PROTECTING THEMSELVES AGAINST CYBERSECURITY RISKS? (CON'T.)

4. Becker: The last thing is that **nonprofits think cybersecurity is expensive**. They believe, "I'm not a Fortune 500 company. I'm just a tiny nonprofit." Even if they have a thousand employees, they think, "We use the same IT as other nonprofits because it's just too expensive. We don't want to spend too much on back office."

This one's actually the easiest to dispel. Cybersecurity is much more about habits than it is about technology. Cybersecurity is probably the only thing in computer science that has more to do with humans than with computers. If you imagine everybody on earth disappearing, the internet Internet would continue to hum, databases would still function, but the one thing that would end immediately is hacking. Human beings hack other human beings.





**The question you have to ask yourself is, "Am I being penny wise and pound foolish?" Are you trying to save thirty bucks a month for your back office? Then in the end you've got to explain to your board why you now have a 65% decrease in recurring monthly donations because you got hacked.**

**Becker Polverini, CEO, Co-Founder, PKC Security**



## WHAT MINDSET CAN A NONPROFIT HAVE THAT CAN GET IN THE WAY OF ADEQUATELY PROTECTING THEMSELVES AGAINST CYBERSECURITY RISKS? (CON'T.)

Becker: When people talk about the expense of cybersecurity, they're thinking about it from a tech perspective like, "Oh, I need to use buy this software or, this widget." When in reality what you need to do is **change the manner in how you and your staff engage technology.**

There are a lot of effective, free solutions out there and we'd be happy to recommend some. Good cybersecurity is about a community of people becoming more secure just by valuing privacy and valuing other people having privacy. There are also a lot of solutions that aren't free but are really affordable.

The question you have to ask yourself is, "Am I being penny wise and pound foolish?" Are you trying to save thirty bucks a month for your back office? Then in the end you've got to explain to your board why you now have a sixty-five percent decrease in recurring monthly donations because you got hacked.



## **WHO'S LEADING THE IT GOVERNANCE AROUND THIS?**

Ken: I think the biggest mistake here is to think that your IT staff is already actively working on cybersecurity issues within your nonprofit.

Most of the nonprofits we work with that have successfully addressed cybersecurity have taken ownership of IT governance at the executive level. This can be the CEO at a smaller nonprofit or the Chief Information Officer for larger nonprofits.

For even larger nonprofits that are generally above two hundred full-time staff, they often have roles dedicated to cybersecurity, either a Chief Information Security Officer or some type of head of security role. That's really what it takes to properly address cybersecurity at the policy level and have that actually roll down to your staff across the organization.



## WHAT ARE THE TOP CYBERSECURITY ISSUES YOU SEE NONPROFITS FACING? HAVE YOU SEEN A TREND OVER THE PAST YEAR?

Becker: I don't think today's issues are that much different than a year ago, but these top issues often go unaddressed because they might not be what you expect.

1. One top security issue I always think of for nonprofits is that they have a lot of **personally identifiable information about their staff and volunteers**: social security numbers, healthcare information, bank account numbers. This also includes, contact information for their donors. That's something specific to nonprofits.
2. The second security issue is around **donor billing information**. Hopefully, nonprofits never have access to donor billing information. For example, let's say you have a website that has a mechanism for doing monthly recurring donations. There's no need to ever touch your donor's bank or credit card numbers. In the event you are a nonprofit that is collecting this information, that's a huge issue. You need to be using a PCI compliant service like Stripe or authorize.net to do your donations.

## WHAT ARE THE TOP CYBERSECURITY ISSUES YOU SEE NONPROFITS FACING? (CON'T.)

3. Becker: The biggest issue, the one that people don't talk nearly enough about, is the **general lack of cybersecurity education within nonprofits**. It needs to be baked into onboarding, baked into quarterly meetings, baked into annual meetings.

Increasing security awareness within your organization is something that you should talk about pretty regularly. When we visit a nonprofit, we frequently encounter people at every level in the organization that just don't know what the best practices are around security. Conveniently, education is the most cost-effective way of actually improving cybersecurity at an organizational level.

The lack of cybersecurity education is the biggest issue for organizations everywhere, not just nonprofits.



## WHAT ARE THE TOP CYBERSECURITY ISSUES YOU SEE NONPROFITS FACING? (CON'T.)

4. Ken: **Another thing that is very specific to nonprofits is security relating to volunteers.** A lot of nonprofits have very robust volunteer networks and are able to utilize them very effectively.

The problem is that these volunteers often have access to data that they probably shouldn't. A lot of times this revolves around donor data.

You have a set of volunteers who are at the phone banks calling donors. Without the proper restrictions in place, these volunteers can have access to your entire donor base, often from their own laptops that may not have any security measures in place. It's really important to make sure that this access is managed properly and securely to protect your donors.



## WHAT ARE THE TOP CYBERSECURITY ISSUES YOU SEE NONPROFITS FACING?(CON'T.)

5. Becker: Another risk related to volunteers is **high volunteer turnover**. Besides the fact that it's never really a great idea to have lots of people having access to something sensitive, we found that organizations with high volunteer turnover handle onboarding and offboarding in a really fast and informal way to get it done. Unfortunately, this usually leaves security by the wayside, because security adds friction. This introduces terrible security risks.

A robust onboarding and offboarding process for volunteers has cybersecurity baked into it, and shouldn't be optimized solely around speed. Because, for example, if you have to quickly revoke accounts for several volunteers on an ongoing basis, you're very likely to forget something, which can become a liability later on.

## SO WHAT PLAYS OUT DIFFERENTLY IN THE NONPROFIT SECTOR CYBERSECURITY-WISE THAN IN THE FOR-PROFIT SECTOR?

Becker: The attitudes about spending money on cybersecurity are a little bit different.

**Nonprofits typically view cybersecurity as a cost center.** When you think about it, it's not like cybersecurity necessarily improves your bottom line.

For-profits generally perceive it in a way that is essentially intellectually equivalent to a financial audit. They say, "Well, we have a fiduciary responsibility to our shareholders. This is necessary as part of our risk profile to go do this."

What we see in nonprofits more often is that they don't perceive it as having a responsibility to their board and to their donors. They see it essentially as, "This makes my back office look more heavy. This makes it look like donations are not getting to the field." They're much less likely to want to pay for cybersecurity.

## SO WHAT PLAYS OUT DIFFERENTLY IN THE NONPROFIT SECTOR CYBERSECURITY-WISE THAN IN THE FOR-PROFIT SECTOR? (CON'T.)

Becker: The attitudes about spending money on cybersecurity are a little bit different. **Nonprofits typically view cybersecurity as a cost center.** When you think about it, it's not like cybersecurity necessarily improves your bottom line.

For-profits generally perceive it in a way that is essentially intellectually equivalent to a financial audit. They say, "Well, we have a fiduciary responsibility to our shareholders. This is necessary as part of our risk profile to go do this thing."

What we see in nonprofits more often is that they don't perceive it as having a responsibility to their board and to their donors. They see it essentially as, "This makes my back office look more heavy. This makes it look like donations are not getting to the field." They're much less likely to want to pay for cybersecurity but they need to look at this the way the for-profit sector is beginning to look at it. **Cybersecurity in the nonprofit sector should be seen as a fiduciary responsibility to your donors.**



## DOES THERE HAVE TO BE SOME KIND OF SECURITY BREACH IN THE NONPROFIT WORLD TO REALLY GET PEOPLE TO FOCUS ON CYBERSECURITY?

Ken: Yes, I would say that's true not just for the nonprofit sector, but also the for-profit sector. **Prevailing attitudes toward security are very much reactive rather than proactive.** You always see an uptick in improving cybersecurity practices after an incident.

That's often a great time for executives to have the momentum that they need in order to make these changes and get them approved by the board. It doesn't have to be a major, destructive cybersecurity incident. It could even be something as simple as, "One of our staff lost a laptop. The laptop was unencrypted and had our donor database in Excel sheets on it. We'd like to work on improving our organization security around data leakage and data loss."

That's a great way to get the conversation started and make it very tangible to the people who may otherwise be skeptical.

## WHAT ARE SOME OF THE UNIQUE NEEDS OF LARGE NONPROFITS OR THOSE THAT WORK OVERSEAS?

Ken: I think there are two **very specific nonprofit demographics** here that we can break out here. **Large nonprofits**, let's say more than fifty million or seventy-five in revenue, are at the point where they should start thinking about things like cyber insurance.

That would probably need to be led by someone who understands risk, ideally their CFO.

Then the second category is **nonprofits that work overseas** pretty heavily. Maybe they have a headquarters in the states or Europe, and then a substantial staff either in offices overseas or individually working overseas. For those organizations, it makes more sense to have IT governance come from a strategic perspective rather than a technical one. Overseas staff often are using their own technology already by necessity due to unique technical challenges.

Rather than trying to roll out a technical solution to your team that may not even work in countries with poor internet access, it's much more important to offer cybersecurity training for these staff members. Integrate it with training on physical security and general awareness of the political environments that they're working in and include training on surveillance and censorship.



## WHAT IS THE BEST WAY FOR A NONPROFIT TO IDENTIFY RISK AREAS? IS AN AUDIT THE BEST APPROACH?

Becker: Yes, we would recommend **getting a professional risk assessment**. These are not expensive. It's absolutely the best thing that you can do to identify risk areas. By and large, people who haven't studied cybersecurity are not good at identifying what are the actual risks. If you try to self-educate and you're not a practitioner, you're probably going to pick the wrong security risk to try to fix. This is what the risk assessment will prevent. You'll have professionals actually go into your organization, understand your work flow in detail, and then actually address specific identified risks for your organization.

**Very practically, the reason why the risk assessment is good for nonprofits is that they are great for the board meeting.** You take this risk assessment to your board. It will outline security hot spots and list the weaknesses that are intrinsic to your work and organization. This allows you to defend the increase in the IT budget at the board meeting.



## WHAT IS THE BEST WAY FOR A NONPROFIT TO IDENTIFY RISK AREAS? (CON'T.)

Becker: We've seen this happen. The head of operations or the CTO says, "I just know that something is wrong security-wise. I don't know where it is, but I know that something is off." They pay for the risk assessment. It confirms what they thought. They get validated. They take that validation, the details of why it's true and what needs to be done, to the CEO, who goes **"Great. I can now take this to the board, and get the increases I need in the budget in IT to go get this done."**

We've seen that work very successfully for large nonprofits who, in essentially a quarter, turn around their cybersecurity from completely exposed to prepared. People feel like it's easy to get self-educated on cybersecurity. I think this is particularly true with younger CEOs. Executives who are a little bit more established in business understand that they're not experts on everything. I think we've seen it cause a lot of damage when they try to go outside their element.

## **IF A NONPROFIT DOES A RISK ASSESSMENT AND THEY HAVE LIMITED RESOURCES TO RESPOND TO THE IDENTIFIED THREATS, WHAT IS THE BEST WAY TO PRIORITIZE AND RESPOND TO THOSE THREATS ?**

Ken: I think this can be broken down into two separate questions. One is how to respond and the other is how to prioritize. As far as responding, I think people often underestimate how much effort is required to implement the solutions that are the most effective.

Just to give you a very concrete example, most of the time credential management is pretty high on the list of security issues that need to be addressed. The solution to credential management is often times getting your staff to use password managers instead of storing their passwords on their laptops unencrypted, putting in place policies for how staff can share credentials between people, getting staff off of shared accounts onto their own separate accounts for things like PayPal. These tasks require a lot of hands-on work with staff to educate them on how to use these tools and how to change their practices.



**I think the biggest piece of education that we can share with nonprofits is that people mistakenly have a very binary view of cybersecurity.**

**They see it as I am either secure or I am nonsecure...In reality, you go from being nonsecure to being prepared, because you'll never be able to mitigate all of your risk.**

**Ken Kantzer, Co-Founder, PKC Security**

## IF A NONPROFIT DOES A RISK ASSESSMENT AND THEY HAVE LIMITED RESOURCES TO RESPOND TO THE IDENTIFIED THREATS, WHAT IS THE BEST WAY TO PRIORITIZE AND RESPOND TO THOSE THREATS?(CON'T.)

Ken: So for responding, I recommend appointing a responsible party in that organization. It doesn't have to be at the executive level, but some person who will put in the time required to implement the solutions

Then there's the question of prioritization. **Usually when you get a risk assessment, it will have a lot of mitigations. A good risk assessment will already have those prioritized for you based on the amount of risk exposure from each mitigation.** A simple approach here is, especially if budgetary resources are limited, to work on the top five. Take the top five threats, that'll probably cover eighty percent or eighty-five percent of your total risk. If you can nail those and get them solved, then you've made a huge step forward in terms of lowering your risk overall.

Becker: I think the biggest piece of education that we can share with nonprofits is that people mistakenly have a very binary view of cybersecurity. They see it as I am either secure or I am nonsecure. If I do all of the things in my mitigation, then I go from being nonsecure to being secure. When the truth of the matter is that as with anything in risk, it's actually a spectrum.



## IF A NONPROFIT DOES A RISK ASSESSMENT AND THEY HAVE LIMITED RESOURCES TO RESPOND TO THE IDENTIFIED THREATS, WHAT IS THE BEST WAY TO PRIORITIZE AND RESPOND TO THOSE THREATS?(CON'T.)

Becker: Everything has an expected value. In reality, you go from being nonsecure to being prepared, because you'll never be able to mitigate all of your risk. **All you need to do is get your risk below an acceptable threshold.** Every organization, board, and executive needs to understand where that threshold needs to be with respect to their workflow, with respect to the geopolitical nature of their work, with respect to the compositional makeup of their organization.

They need to figure that out and need to be intentional about calculating what that threshold should be. In order to prioritize and respond, the best thing you can do is listen to the cybersecurity professional that gave you the audit.

Any audit worth its salt will prioritize and will include a list of mitigations. They should articulate what your response should be in those mitigations. If you ever get a risk assessment that misses those two components, then it's not worth its salt.



## WHAT CYBERSECURITY BEST PRACTICES WOULD YOU RECOMMEND FOR A NONPROFIT TO CONSIDER THIS YEAR?

Ken: We've talked a lot about **doing a risk assessment**, so certainly that. In addition to that, one of the big trends, especially in the last couple years that nonprofits should be aware of, is **a type of hacking attack termed "whaling."**

You may have seen some of these incidents in the news. Basically what happens is someone emails the CEO, gets access to the CEO's email, and then uses that email to trick whoever is in charge of finance to send a bank or wire transfer to an account that is overseas. This is something that nonprofits need to be aware of as they often do transactions overseas. That's already a natural part of what they do. They are also sitting on financial resources. **Whaling is a huge trend. The FBI reported last year that over eight hundred million dollars was successfully extracted in the last six months from these types of attacks.**

## WHAT CYBERSECURITY BEST PRACTICES WOULD YOU RECOMMEND FOR A NONPROFIT TO CONSIDER THIS YEAR? (CON'T.)

Ken: **A best practice is for executives in particular to receive some sort of training in terms of how they handle their security, both for their corporate accounts, but also their personal accounts and personal email.** I think it's often a misconception that those two things are fully separate, and that whatever happens in the personal realm won't really affect the nonprofit itself. We've seen a lot of nonprofits actually go out and look for this type of executive training. It does exist out there.

Becker: Another cybersecurity best practice would be, particularly for this year, is to **make cybersecurity hygiene a strategic goal for the entire organization.** From the very top, have the CEO say, "One of the strategic goals for this year is improving our cybersecurity hygiene." **That doesn't cost a dime. It sends a huge statement to both volunteers and staff that cybersecurity matters.** It will open up a really important conversation around security education and around the habits in the organization that are dangerous. Even though people are not necessarily great at calculating risk, I do think that anyone who uses a computer in these organizations has at least a rough idea that they're doing something dangerous. I think if they hear the CEO saying, "This is a strategic goal. We will care about our hygiene," it will produce the right amount of fear in the staff to not do the wrong thing and more importantly, instills a sense of responsibility.

## WHAT CYBERSECURITY BEST PRACTICES WOULD YOU RECOMMEND FOR A NONPROFIT TO CONSIDER THIS YEAR? (CON'T.)

Ken: Another best practice is something that every nonprofit, and really any person in general should do,; **please start using two factor authentication!** Essentially what that means (and a lot of people will recognize this from what they do with their banks currently) is in addition to your username and password, you'll be prompted for a code that will be sent to your phone or some mobile device. You'll enter that in as an additional second factor of authentication. What this does is it ties the security of your account not just to someone who is able to guess your password, but to the possession of a physical device.

What this means is a hacker, even if they guess your password, would still have to physically go to your office or home and steal your phone in order to log into your account. **It's probably the biggest bang for your buck that you can possibly do in terms of securing your accounts both for your personal life, and for your corporate and nonprofit life.** That's what we recommend. The best first step is to start using two factor authentication for Google apps, for your email. Almost all the major email providers now have a way of turning on two factor authentications in your settings.

**Have more nonprofit cybersecurity questions?**  
**[info@pkcsecurity.com](mailto:info@pkcsecurity.com) OR [www.pkcsecurity.com](http://www.pkcsecurity.com)**



# Be part of a great development experience. Globally.

Access the benefits of an engagement experience built on global business savvy, deep cultural understanding and strong technology know-how. Global Pueblo was founded in 2008 and is headquartered in **Wheaton, Illinois** with a Global Development Center in **Chandigarh, India**. We've worked with nonprofits to startups to the Fortune 500 to provide **cost-effective consulting, software and web development and global engineering teams**. With 30+ countries where our management team has provided technology services, our clients benefit from deep experience when it comes to building **high-performing global teams**.

FIND OUT MORE

BEFORE YOUR NEXT PROJECT