Mission + Markets Episode 13: Nonprofits and Cybersecurity

***Please note: This is an AI generated transcription - there may be slight grammatical errors, spelling errors and/or misinterpretation of words***.

Hello, and welcome to Mission and Markets, a podcast by CAPTRUST, where we explore trends and best practices for endowments and foundations related to mission engagement, fiduciary governance, and investment management, hosted by CAPTRUST. It's Heather Shanahan, Director of the Endowments and Foundations Practice.

Each episode shares research, resources, and recommendations from industry insiders, so your nonprofit can focus on what's most important, the mission.

**Heather Shanahan:** Hello and welcome to our latest episode of Mission Markets. My name is Heather Shanahan and I am your host. And today I am joined by two cyber security and technology experts. The first is Dave Chatterjee. Dave is a cyber security and technology thought leader and subject matter expert with a PhD and is a tenured associate professor in the management information systems department at the Terry College of Business with the University of Georgia.

Doctor Chatterjee has authored a highly endorsed book, Cybersecurity Readiness, a holistic and high performance approach, a staged publication. He has also written and edited scholarly papers, consulted with companies, served on a cybersecurity swat team of chief information and security officers, given expert interviews, conducted workshops and webinars, and delivered numerous talks at academic and practitioner forums worldwide.

He hosts and produces his own podcast, the Cybersecurity Readiness Podcast Series, publishing over 60 episodes and reaching listeners in 94 countries. We would love to have that type of reach here with Michigan Markets as well. So welcome, Dave. I'm also joined today by One of our own, John Meyer,

John is CAPTRUST's Chief Technology Officer and is responsible for the farm's application development, information security, infrastructure, and emerging technology practices.

Prior to joining CAPTRUST, John led application development teams for both First Citizens Bank and Blue Cross and Blue Shield of North Carolina. He began his career with Accenture and has worked in the industry since 1990 and holds a bachelor's degree from Duke University.

So let's dive on in because this is such an important topic and it's not one that non profit organizations necessarily have access to discuss on a regular basis. So Dave, I'll start with you. What do you see as the current cyber trends and threats that are facing non profit organizations? Are these threats any different from those facing similar sized for profit organizations?

And public organizations, and how do you think these threats vary based on the size of the organization?

Heather, size of the organization doesn't really matter to the hackers. They're pretty savvy and the small and medium sized organizations, the non profits, they are as vulnerable. as the large organizations, as the for profit organizations, because you have to realize that these non profits, these smaller organizations, often serve as vendors, contractors, partners of larger organizations.

So therefore, the cyber attackers Use them as gateways to hack into the systems of larger organizations. Recently I was delivering a talk at a conference in North Carolina in Chapel Hill, which was geared towards educational institutions. And when I was doing my research for that talk, I was surprised, that for educational institutions, the single biggest threat are the ransomware attacks. And as a result of which, classes have been cancelled, institutions have been shut down for days. Most of them, or many of them, have paid the ransom.

The average cost to remediate was 1. 5 million. The time to recover average was over a month. And what's even more troubling, that even after paying the ransom, on an average, only 62 percent of the data was restored. So, the situation is pretty grim, and to add to that, we wrote a paper, It's titled, RESTORED. calculated risk, a cyber security evaluation tool for SMEs. And in that paper, one of our findings that the leadership in these non profits, in these small, medium sized organizations, they're often in a state of, ignorance can be bliss.

So they, they assume that they are in good shape where they are not, and study after study, survey after survey found lack of preparedness, lack of proactiveness. another stat I want to throw out there, 60 to 65 percent of medium sized businesses, they declare bankruptcy after experiencing a major attack. So therefore, in a nutshell, the threats are no different for the smaller organizations compared to the larger organizations. And so the level of preparedness needs to get better.

That's staggering. The threat's not different, but the ability to respond to it. A small or medium organization to come up with a 1. 5 million dollars in response to ransomware is just, it's just not possible. Wow, John, what would you add to this? In regards to how an organization would need to respond.

**Jon Meyer:** I think Dave's Right. on target. In addition to the risk of going out of business operationally, for not for profits, we also have the additional concern of losing donor trust and all the financial support that comes along with it. So, you may be a, Business where, let's say you're a manufacturer, your customers may not notice other than like the operational difficulties if you have a big ransomware attack, but it's very different when you're in a not for profit and then you have to reveal to people that you've lost all of their data.

It, it can be, A double whammy, not only do you take the operational hit, but then all of a sudden your donors don't trust you with the financial information they've given you in the past. They don't trust that you're a good steward. So I think it's a huge challenge. And Dave's exactly right.

No one's immune from this. And the only way you can really respond is to prepare and preparing takes time and investment and smart people. Whether those people are on your staff or the people that you contract doesn't matter. You have to prepare for this and it's just one of those existential threats, I think, that can really make a difference in terms of an organization surviving in a world where hackers, I think, have it pretty easy with smaller organizations in general.

**Heather Shanahan:** Yeah, it sure seems like it. Dave, I'll bounce back to you. The world of cyber security seems replete with these stories of breaches, specifically ransomware, as you just mentioned. Is there any new news here? And what do you think is changing to allow attackers to be more successful? Or is it just that organizations have holes in the bucket,

**Dave Chatterjee:** I don't know if you can call it a new news anymore because artificial intelligence is everywhere. So that technology is enabling the hackers. to get even more sophisticated. When you think about the different types of AI generated attacks, from automated, target profiling to efficient information gathering, personalized attacks, employee targeting, reinforcement learning, there are a variety of things that this technology enables these hackers.

And then there's the, this adversarial AI. which they come in two types, the poisoning attacks and the evasion attacks. However, just like the hackers have this technology to mess with, the good folks, the defenders, the regular organizations, they also have access to the technology There are a variety of ways that organizations Can secure themselves, but it is a continuous process. When we were talking about, in the context of how vulnerable are small to medium sized organizations and nonprofits, and John made some excellent points about how the level of preparedness needs to go up.

The reality is you can't look the other way. You have to see cyber security as a strategic opportunity. If you look at it as a pain, a cost of doing business, let's outsource it, let somebody handle it, which is often the human nature when we don't want to deal with trouble, something we don't know much about.

Unfortunately, you have to take the reverse approach and say, And again, John said this, if the company develops a reputation in being diligent, in making every effort to protect customer data, to protect other stakeholders data, that reputation will help them generate more business in the context of raising funds.

People will be more comfortable sharing their information. So it's actually a win. To be proactive about cyber security and you don't have to be a cyber security expert. I'm a firm believer that if you have a real intent that you are going to make a difference, it matters.

I often like to use this analogy, like sending your kids to school. You don't say that, Oh, I'm sending my kids to a great school. They just turn out fine. I can look the other way and I can do my work. You just can't outsource it. You still have to provide oversight.

And I say the same for cybersecurity. If the leadership recognizes cybersecurity as a core capability, as a strategic competency, they will find ways. of enhancing their level of preparedness, sustaining it without taking their eyes off the main business.

**Heather Shanahan:** Excellent. I'm going to ask you to back up to two terms just to clarify for our audience. POISONING versus INVASION.

**Dave Chatterjee:** So basically, poisoning means you insert malicious data into the training data set. These AI tools, the AI models, they have to be trained. They have to be taught. So they rely on training data. And just like before, even before all this happened, early days of computing, there was a common saying, garbage in, garbage out.

So if you do not train them with good quality data, their predictions, their insights will not be great. So hackers find a way of manipulating the training data sets so they can get results that suit their needs, suit their requirements. And then the evasion attacks, they aim to deceive a machine learning model by crafting input data.

The objective there is to alter the model's prediction through subtle modifications to the input, causing it to fail. to misclassify the data. Once again, the overall goals for the hackers are we will mess with these AI tools So they produced outcomes that, or they produce results that deceive people. If that helps.

**Heather Shanahan:** Yeah, absolutely. Thanks for clearing that up. John, reaction here?

**Jon Meyer:** I think that AI isn't so new, but it's still pretty new for most of us. And I think AI sponsored attacks will be on the rise, particularly, deep fakes where people are making audio sounds that sound like a person. And what I would encourage everybody to do is to really think about how you trust people. like when I talk to my spouse over the phone, I know her voice. I don't really know that it's her. But she and I have shared experience and that shared experience is a way that I can quickly, validate whether I'm communicating with her or perhaps a deep fake. And so I would encourage everybody in business to think about what kind of shared experiences you have in your organization that can be used to validate the person you're speaking with on the other end And where this comes into play is. Hackers asking for money, asking for wires to occur, asking for bills to be paid and all, everybody involved in that process should be able to feel confident that the person they're talking with on the other end is who they say they are.

And so if you prearrange that, if your finance department prearranges that when the CEO is going to ask for a wire, that they're going to share some kind of secret word, Or secret passphrase that only those people know. Then you don't have to worry about a deep fake coming along. Because I'll never be able to answer that question.

And I think That by doing that, you will add to that degree of readiness and preparedness.

That's fantastic. I'm glad John, you brought up those points. Unfortunately we are in that world today where everyone has to have a certain. Element of paranoia. Maybe paranoia is a negative word. A positive word would be a higher level of security consciousness. My wife received an email from a major financial institution in the morning and we were about to have our cup of tea and she says, Dave, they're asking me to change my password. I got an email from so and so bank. And before I could respond, she had already clicked on the link and Done the needful. So these hackers are so, tactful.

**Dave Chatterjee:** They're also, they have great resources. They have psychologists working for them. They know when to come at you. So they will target you at times when you are probably just waking up or you're multi processing. So you'll just quickly respond to a request or a query. So I encourage listeners to be very careful.

And it takes a second to just pick up the phone and reconfirm the message that you have received, especially anything to do with finances, financial transactions, opening or closing accounts. Even if the emails or the messages look authentic. Just call and check.

That's just unbelievable.

**Heather Shanahan:** Let's talk about on a professional level. I'm responsible for a mid sized non profit or a small non profit. I don't have a dedicated it. team. This is real and it happens. What do I prioritize with my limited budget to try to reduce these risks?

**Dave Chatterjee:** I want to emphasize here, not having resources is a bad excuse. I've had the pleasure of talking to several legal experts who have said that in a court of law, the judge and the jury are very reasonable in terms of their expectations.

All they want to know is Given the resources you have, given the size of your organization, did you do your very best to secure what needs to be secured? So that's a bad excuse. There has to be an active commitment. by the leadership and they have to put together a team and even if it's a small organization they can still find a way of assigning the role to one or two people and doing things with it and it's a it's it can be managed in a variety of different ways if the intent is there.

Now

We need to decide what's most important to us and how best to secure them. Because once again, making the argument of limited resources, fair enough. We can't protect everything as, as well as you would like, but let's at least secure what's most important to us.

The second thing I would, I want to emphasize our data backups and retention strategy. The ransomware attackers are very sophisticated. They'll go right straight to your backups. And once they access it, they can cause havoc. They know that the only way the organization can come back up and running is from the backups.

So if they can compromise the backups, it's like a checkmate situation. So. That's precisely why a lot of thought needs to be given on how data should be backed up, where all, offline, online, how often should you rehearse your data restoration strategy. You're backing it up, but you are never seeing how well you recover exactly.

And final point I want to make here. Treat every employee in the organization. Treat all your business partners as a member of your cyber team. This is not about having four or five people who are trained in cyber security, have certifications. And they work under a CISO, which happens in large organizations.

This is a more practical approach, where we need to raise the level of security awareness amongst everybody, so everybody does their part. As you've probably heard this many times, cybersecurity readiness is everybody's business. So we cannot just outsource it to a set of folks and expect miracles to happen.

We all have to play our part.

**Jon Meyer:** I would say that it goes a long way to do an hour of training a quarter about cyber security. Rather than doing nothing, I think if you don't do anything, then everybody's going to say you're being negligent in today's day and age.

It's reasonable for you to expect to do some training on how people shouldn't be clicking on links and emails that they don't know where they've come from. Cybersecurity training is not expensive. A lot of it's available from the government, from CISA. You don't have to buy anything. You just have to devote some time and energy.

And then, I would say, Every organization should have a cyber security assessment once a year. If you don't have your own staff, then you have to hire that. But you're going to get valuable suggestions. They're going to make you focus on the low hanging fruit

it's about dotting the I's, crossing the T's, showing that you've put some form of due diligence into making sure that you're not just wide open to attack.

You just have to make those efforts. And if you do, I think it goes a long way towards keeping you safe.

**Heather Shanahan:** Great points. I love the idea of, it's going to take a village. It still might come down, but at least your fortress is a little bit stronger with everybody engaged. And I think anything that organizations can do on an institutional level carries over in people's personal lives. Just, hey, be smart,

If you're aware at work, be aware at home too. So let's talk about third party risk management. From a supply chain standpoint, what can small organizations do? And then cyber insurance, cyber risk insurance. How does that work? Is it effective? Should everybody have it?

**Dave Chatterjee:** I think it's great to start with cyber insurance. Let's say I'm a small to medium sized organization. I don't know much about how to secure myself from different types of cyber threats. See if you can buy some cyber insurance because the insurance providers will do their due diligence, will make sure that you have a certain level of.

defense in place, a certain level of preparedness before they will even consider giving you insurance. Not only that, they have the resources that they will provide to help you assess your potential vulnerabilities in your systems, in your networks, help plug those loopholes. So in a way they are guiding you in securing the organization.

So to that extent, The risk level is less, so that also helps them because the cyber risk insurance market is not that big. And so if everybody starts claiming insurance,

We will not be able to get cyber risk insurance anymore. So therefore it is in their best interests. They want to make sure that their clients not only have a certain level of preparedness, but they have to sustain it, maintain it, to be eligible to receive coverage.

So I think that's a great way of protecting yourselves, especially if that's not something you're good at.

And when you talk about third party service providers, it goes back to being very deliberate. Don't be in a rush to sign a long term contract. Wet them thoroughly, learn about how they have been performing with other organizations. Once you've signed, have very robust SMAs, closely monitor performance.

So there are a lot of things that organizations can do because almost no organization today operates by themselves. So we know of numerous attacks. that came through the systems of these business partners.

we are all in this together. One more point I want to make, and this is something I say every time I get an opportunity, and that is you can try and get all the help you want. You can have monitoring tools in place, but when you receive threat intelligence, please do something about it. It has happened time and again when organizations were caught napping when they had the intelligence. They just didn't do anything about it. And maintain a log, maintain a document, and I know it's easier said than done, but do the best you can, where you list the types of intelligence you received, what did you do about it, and why.

So then later on in a court of law, you can show the judge and the jury that yes, We had these kinds of insights. We decided not to act for this reason. We decided to act for this reason. That shows real intent. That shows that you are not being negligent. So we don't have to get overwhelmed by all these cyber security best practices.

Just use plain common sense Keep asking the right questions. And before you know it, you have a pretty good security strategy in place.

**Jon Meyer:** I guess we can all say that, it's not a matter of if, it's a matter of when at this point that that we have issues. John, anything that you would add I think Dave's spot on with the cyber risk insurance. It may be too expensive for a lot of organizations to obtain. And they are becoming pickier and pickier during their underwriting process. So you may find that you don't qualify, but you're going to get a free assessment, it's a good exercise.

And having a little insurance may not cover the risk that you have. if you look at what the financial exposure is for losing a data record containing personal information, it's about 200 a record. By the time you're all said and done with paying for remediation, paying legal fees, it can be quite expensive.

So if you're sitting on 10, 000 donors, for example, you multiply that by 200, that gives you an idea of your, your insurance coverage that you might need to make yourself whole. And that's why Dave said earlier, so many businesses that have a big breach go out of business. Costs can be phenomenal.

I think the same thing applies to your service providers. You should do as best a job as you can doing due diligence on those service providers. Most of them have what they call a trust center. They'll share with you the formal documentation that they have around how they keep things secure, who has audited them.

You also really want to ask who's responsible if they have a breach and who's going to pay for that, right? Because frequently, if you look at normal contracts, you don't get the liability coverage that you would like, or it's limited to, two or three times what you've actually paid them.

That doesn't do anything for you if they've lost all of your customer information, all of your donor information, and you now need to deal with all of those donors. So that stuff's complicated. It's not always easy to negotiate deals with a lot of suppliers, especially if you're very small, but it's worth asking.

So at least you can know. And I feel like a moderate supplier due diligence program can go a long way towards at least understanding where you sit in that risk. That risk perspective.

**Heather Shanahan:** Let's keep going on that theme there, John. So if an organization is looking to hire an outsource IT consultant, what should they be asking? What are the important things for them to consider?

**Jon Meyer:** Yeah, so most organizations first hire an I. T. consultant to run their I. T. operations and they do that in advance of hiring an information security consultant who can really gauge the effectiveness of security. So for an I. T. consultant, what's really important is, are they going to service you well?

And one of the best ways you can understand that is to both look at their service level agreement and to speak to customers they're currently serving. so it doesn't do you any good to have an IT consultant on board that's going to take five days to get back to your people if they're down.

That's not useful. You need reasonably fast responsiveness. Understanding that, if it's 24 hours a day and it's around the world, that's very different than if it's, 8 to 5 or 9 to 5 Monday through Friday. You're going to pay more to get kind of 24 hour coverage. But you need an IT consultant who is going to be responsive and who is committed to security.

And the way they're going to demonstrate they're being committed to security is they're going to tell you, hey, this software is out of date. We need to get it updated. This server is out of date. We need to get it updated.

I think that the natural next step there.

Is to hire an independent information security consultant who can look over your shoulder and be your guide to make sure they're supporting security. That's added expense, of course, but at the same time, you don't really want the Fox. Guarding the chicken coop, right? So the person who's doing the work for you Will tend to be less critical about their failures to do the work properly Than an independent person.

Both of those people play a critical role.

**Heather Shanahan:** Yeah, that makes sense. All right, Dave, I've ignored all of your advice or in spite of all of your advice, I have an issue. I have a crisis. What are the first steps I need to take?

**Dave Chatterjee:** I'd love to answer that question, but I want to back up a little bit and share something that I didn't share. And it goes back to, how do you secure the organization if you have limited resources, so on and so forth. One of the things I would recommend organizations do at the very beginning is You know, identify the different threat scenarios and literally make a note of if this were to happen, what are the consequences?

If this was what to happen, what are the consequences? Why do you do that? Because that's the way you get the attention of The senior leadership.

another thing I want to mention here is the importance of doing some tabletop exercises, making sure that these service providers that we, the organization hires to provide them with the security service. Will they be available when the incident happens?

It so happened in one organization at 4. 30 in the morning, they experienced denial of service attack, and they tried to reach the outsourced organization where their data centers were located. They couldn't. The chief technology officer personally went there. The security guard wouldn't let him in. So they ran into all kinds of hurdles.

**Dave Chatterjee:** I encourage organizations to do some security drills. They may not be perfect, but something is better than nothing. And again, It adds to your scorecard of trying to be as diligent as possible. Now I'll say a few things and then turn it over to John about, if there's a crisis.

And this comes from folks who do it for a living. And they have a couple of advice for organizations. First, they say it really helps to have those log files. So you can make our jobs a lot easier if you call us for help. If you have maintained the log files. Second, the best thing that the leadership team can do is to give the incident responders and the IT department some breathing room and not ask for status updates every 30 minutes.

It's totally understandable that it's crisis, everybody is panicking, they want information. But you've got to give them some time to do their work. Third, when something bad happens, don't start restarting or shutting down servers. Because that removes evidence.

And the fourth point, Which is, I think, extremely important. Don't be in a rush to communicate to the world what happened, because I know how organizations are. They want to tell the world we are under control. most of the time, the bad things show up last.

So it will be at the end of the forensics when they will say, oh, we found this evidence of data exfiltration. So therefore, while I'm not saying that You just go silent because now you can't. SEC has a requirement where you have to be responsive. But at the same time, don't be in a rush to share based on some initial insights.

Let the investigation happen and go back with the facts. Informed insights,

**Heather Shanahan:** yeah, that makes sense. Think about large organizations that have had breaches. You're not in the public immediately hearing about it. It's usually, pretty far down the road before you're notified. Even though it would be very difficult not to panic. I understand that. John, would you share here?

**Jon Meyer:** I think Dave's advice is spot on. PR is critical. There are crisis communication firms that exist to help you manage communications that are critical for your organization. And there is an art of balancing transparency, i. e. letting people know something has happened, With sharing too much information versus sharing too little information.

And so the crisis communications people are excellent at that. We're not exactly sure what it is to it's become a cyber attack to it's become a cyber attack and lots of data has been taken out of the organization and so we have effectively had a breach that snowball can be communicated in a way that makes you seem more on top of it. And that's not my expertise, But we do have people who are experts in that and they tell me, write out those scenarios like you were going to broadcast them on the evening news and say them in a way.

That is cognizant of how the situation is going to unfold. I think all of the technical steps around not turning off servers, so much of this has changed because of the cloud. You may not even have servers anymore. You may not be in control of them. But what you do have is partners who are committed to making sure that the cloud appears safe.

And they will help you and you will have to let them know, but they will help you

So I would just say that really think about these scenarios, know who you would contact for in a critical situation.

Make sure your leadership team has the concept of being pulled together for critical events. you should have a critical incident response plan and team ready to go. And and then rely on the experts to help you.

**Heather Shanahan:** It's a lot to digest. As we're sitting here talking, I'm thinking about, former life when I was responsible for a nonprofit organization. We were fortunate that we had a community member who had expertise, was with a crisis management firm that had volunteered his support. But I'm thinking, most of the time, Executive leadership teams aren't thinking about when you look at your board matrix and where you have holes and where it might be valuable to grab somebody with expertise from the community, man, that's it right there.

Even if it's somebody that isn't going to come in and do the work for you

as a board member who could at least provide guidance. That would be hugely valuable, so there will probably be a run on IT executives after this conversation to try to serve on board roles, but, people don't know what they don't know, so,

**Dave Chatterjee:** but you know, you have a point there, Heather, it's very important to be able to ask the right questions and there is an increasing push. In fact, there is, I think, an SEC requirement now that they're in, especially in public companies, that they want somebody on the board who provides that cybersecurity perspective, who has the relevant credentials, the relevant expertise.

So it's very important. That folks at the top are aware they don't have to be experts, but they should be asking the right questions. So, so I think you're spot on there about when you, I think you jokingly said that they'll need IT people on the, in the leadership team. That expertise is important.

So, so some thought needs to be given to how to structure the organization. It's not enough to hire a CISO and you just check the box and say done.

You have to think about it substantively. If you're going to hire somebody, empower the person. Empower the team so they can be successful. Don't hire somebody so you have a scapegoat. I might sound a little too strong here. But I'm just being practical.

**Heather Shanahan:** I know I've learned a great deal.

I know our listeners will too. So I appreciate your expertise. I hope that we. Scared everybody into taking a look at this if they're not already just it's so critical. So any parting words here as we wrap up?

**Dave Chatterjee:** Like I said, I would not use the word scare. I'd say treat cyber security as a strategic opportunity, an opportunity to get ahead and an opportunity to perform better than your competitors. So embrace it. And don't get too overwhelmed or concerned by all this advice and all the best practices.

Just follow your common sense, take it one step at a time, and you'll know what to ask next, what to ask next.

You will do everything possible to get the right kind of help. You're not prepared for those things in life. You just go with your instincts. You go with your sense of commitment. And so that's why I feel that It boils down to having that commitment, having that true intent that can really help organizations do better.

**Jon Meyer:** Beautifully and well said, Dave.

**Dave Chatterjee:**

**Heather Shanahan:** Thank you for joining us today for Mission and Markets, and please subscribe wherever you listen to podcasts. The discussions and opinions expressed in this podcast are those of the speaker and are subject to change without notice. This podcast is intended to be informational only. Nothing in this podcast constitutes a solicitation, investment advice, or recommendation to invest in any securities.

CAPTRUST Financial Advisors is an investment advisor registered under the Investment Advisors Act of 1940. CAPTRUST does not render legal advice. Thank you for listening to Mission Markets.

**Disclosure: CapFinancial Partners, LLC (doing business as “CAPTRUST” or “CAPTRUST Financial Advisors”) is an Investment Adviser registered under the Investment Advisers Act of 1940. However, CAPTRUST video presentations are designed to be educational and do not include individual investment advice. Opinions expressed in this video are subject to change without notice. Statistics and data have come from sources believed to be reliable but are not guaranteed to be accurate or complete. This is not a solicitation to invest in any legal, medical, tax or accounting advice. If you require such advice, you should contact the appropriate legal, accounting, or tax advisor. All publication rights reserved. None of the material in this publication may be reproduced in any form without the express written permission of CAPTRUST: 919.870.6822 © 2024 CAPTRUST Financial Advisors**