SECURITY WITHOUT PANIC:

How Associations Can Reduce Risk

PROTECH

Scamming and cybersecurity threats are on the rise. Credit cards, banks, and other financial institutions are both warning and educating customers to be vigilant. Even AARP and the Social Security Administration are heightening awareness of threats to their members and recipients. Large and medium-sized corporations have repeatedly fallen victim to data breaches where sensitive information has gotten into the hands of those with nefarious intents. And now associations may be in the crosshairs as bad actors look for additional vulnerabilities.

But, with a willingness to talk with experts and to become more informed on the risks, increased protection for associations is possible. Education for team members and instituting best practices can improve defenses and provide additional barriers for cybercriminals to have to overcome.

Brian Scott, President and CIO, ClearTone Consulting, LLC, has experience that tells him a starting point for initial engagements with associations is that they are far from what might be considered a mature level with cybersecurity and emphasized that, "It's really trying to bring them as quickly as possible up to... anywhere even close to an acceptable level before we start talking about a mature level."

"If you're below this [baseline], you should not be sleeping at night. You should be very uncomfortable about where you are in cybersecurity.

– Brian Scott, President and CIO, ClearTone Consulting, LLC

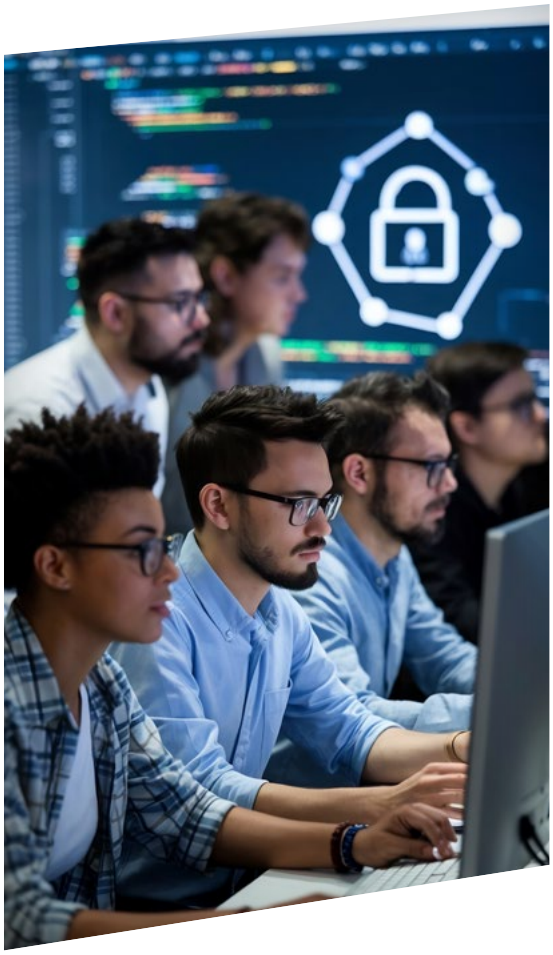
Scott created two benchmarks on a scale of 1 to 5 so associations can better understand where they are with cybersecurity. One is the baseline, and as Scott explains, “If you’re below this, you should not be sleeping at night. You should be very uncomfortable about where you are in cybersecurity. This is the minimum level that you want to get to… ‘Okay, we’ve got the basics… managed.’” The second benchmark is what Scott refers to as an advanced target: Where does an association really want to get to? Where will they feel like they’ve reached a place of maturity with cybersecurity?

One association professional of a mid-sized education association who wished to remain anonymous for this publication indicated that they do mandatory phishing tests and mandatory annual cybersecurity training for staff. They add, “The human side is the main point that we focus on. We feel we have a pretty good lock. Most of our systems are software as a service or platform as a service. We have zero physical servers anymore. There are very few access points for someone who doesn’t already have access. So, we’re focusing on the human side. In terms of the phishing test, we do that monthly. The employees don’t know when they’re going to get it. I have them forward any suspicious email to me, whether it’s the fake phishing one or not.”

Scott refers to phishing in its various forms as “the number one attack vector in today’s world.” The human element in this is huge as people lack understanding or the ability to identify fraudulent attempts. They can easily fall victim opening attachments or clicking on links and going to sites that appear to be legitimate but are really designed for credential harvesting.

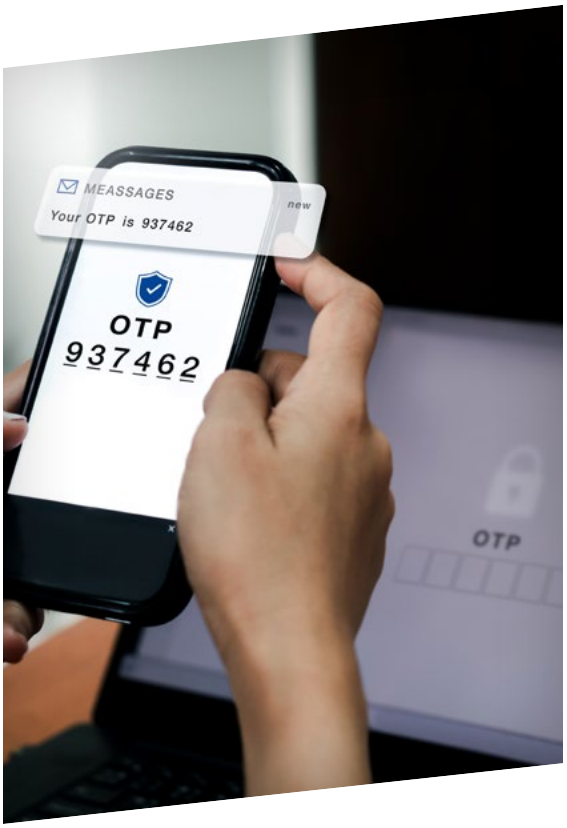
Scott has serious concerns with the extent to which associations are training staff and conducting phishing simulations. In a nutshell, generally he doesn't think it's often enough; and he doesn't believe organizations are able to determine how effective their approach is. Scott runs through a hypothetical conversation with an association executive who has told him that they do a phishing simulation once a quarter, and he asks: "What happens if someone fails? Is that working for your organization? Is that an effective methodology and can you measure whether your staff are really understanding what to do?" Scott adds that if their response is one of confusion or indicates a lack of knowledge or that they can't, then they haven't set up their training correctly and that the process needs to have leadership buy in. He explains further in the voice of an association leader, "This is so important. As a leader, I want to talk about it… We're going to follow these stats. We're going to see what our average fail rates are. We're going to have a company goal, and I want everyone to know that this is an important thing because it's our job to protect our members' data."

The anonymous association executive indicated that they had made a custom GPT that is a training video library. Employees can ask questions, and the custom GPT will respond with an answer and will direct them to a relevant video on the topic. If there is not a video on a topic that's being inquired about, the custom GPT will prompt the administrator to create one. They themselves stay current on trends related to cybersecurity by attending EDUCAUSE conferences, through webinars, and by surveying the landscape for vendor products and services beyond what their MSP (Managed Service Provider) addresses.



"As a leader, I want to talk about it … and I want everyone to know that this is an important thing because it's our job to protect our members' data."

– Brian Scott, President and CIO, ClearTone Consulting, LLC



When asked about what they would advise an organization regarding the first three or four steps they should take with cybersecurity, they advised, "Enable and enforce MFA (multi-factor authentication)... Limit the number of people who have that admin access and then enforce MFA on every other user account. I would get a strict non-browser password manager, meaning not the one that comes with the browser, but a service like LastPass or 1Password or... one of those services for every employee and make sure that all passwords are unique across every service. Then I'd make sure I knew what my backup and restore policies were going to be."

This executive also reports: "In the past couple months, I've been worried about our email reputation. This is not so much about us being a victim, but if someone were to compromise one of our systems and spread something out to other people or pretend that they're us. I've locked down our DMARC fully now (in February)... we are full reject on anything that doesn't fully pass DMARC."

According to Wikipedia, "Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email authentication protocol. It is designed to give email domain owners the ability to protect their domain from unauthorized use, commonly known as email spoofing. The purpose and primary outcome of implementing DMARC is to protect a domain from being used in business email compromise attacks, phishing email and email scams."

"Security succeeds when it is easy to do the right thing and safe to report mistakes."

– Ryan O'Donnell, Co-Founder & CTO, Vortacity

"Security succeeds when it is easy to do the right thing and safe to report mistakes," reports Ryan O'Donnell, Co-Founder & CTO, Vortacity. "Training helps, but the durable improvement comes from workflows: clear 'how to report' steps, fast support when someone flags an issue, and reinforcement from leadership that reporting is rewarded, not punished. You also want backstops that do not rely on

perfect human behavior, like identity monitoring and canaries that generate immediate alerts if an attacker starts probing for sensitive data."

O'Donnell offers final words of advice: "In the AI era, many attacks will look like normal logins, even when they are not. Associations should assume some phishing will succeed and focus on reducing the time from compromise to detection. That means investing in continuous identity monitoring and pairing it with simple active defense, like canary tokens placed in high-value association workflows. Done well, those tripwires can turn a quiet compromise into a minutes-fast alert and response, before funds move or member data leaves the environment."

In under 40 minutes, you can get additional insights from O'Donnell based on his recent appearance on the Reboot IT podcast with host Dave Coriale, CAE of DelCor. The episode "Cybersecurity Maturity: What Associations Need to Know" covers "the evolving threat landscape, the importance of proactive security measures, and how organizations can build a culture of cybersecurity without fear or shame."

As the reader can see, it's not a time to panic, but a course of action needs to be taken. Virtually all associations can improve on this front through technology, training, and putting solid processes in place. The key is being educated on options and making incremental but significant progress, getting to acceptable levels quickly, and staying abreast of both emerging threats and technological advancements to counter them.

"Associations should assume some phishing will succeed and focus on reducing the time from compromise to detection."

– Ryan O'Donnell, Co-Founder & CTO, Vortacity