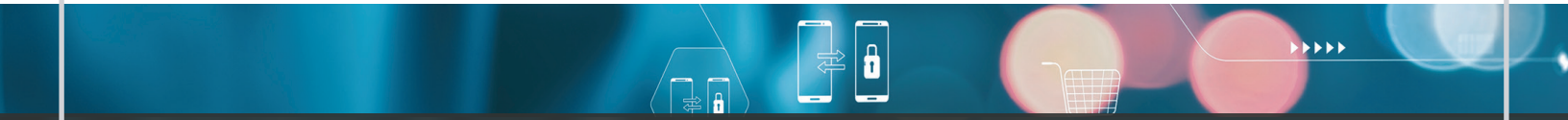
CaseWorthy™



A Comprehensive Guide to Cybersecurity Training in Human Services

WHITE PAPER

Contents

The Importance

The National Organization for Human Services[1] defines human services as "uniquely approaching the objective of meeting human needs through an interdisciplinary knowledge base, focusing on prevention as well as remediation of problems, and maintaining a commitment to improving the overall quality of life of service populations." When we talk about holistically protecting the person, we tend to think about healthcare, mental well-being, accessibility, quality of life, and coordination of services. What these organizations tend to put as an afterthought is the digital identity of those individuals, and the great responsibility we have as human services providers to protect every part of their lives.

Let's face it: by its very definition human services organizations handle a significant amount of sensitive information. This includes everything from Personally Identifiable Information (PII), medical records with Personal Health Information (PHI), financial data, and more. Ensuring the security of this information is essential to maintain trust with the people we serve, as well as to comply with numerous statutory and regulatory requirements like HIPAA.

What these organizations tend to put as an afterthought is the digital identity of those individuals, and the great responsibility we have as human services providers to protect every part of their lives.

[1] https://www.nationalhumanservices.org/what-is-human-services

The Problem

The problem with cybersecurity (generally interchangeable with 'Information Security') training is that much like health care itself, getting trained once is not enough to effectively protect those we are supposed to be safeguarding. Cybersecurity training is a constant and ongoing process, so to be effective we must constantly re-enforce the fundamental information security concepts and practices employees have learned. Additionally, as with health information (if not even more so), the threats we face in an increasingly digital world are always evolving. Users need to be reasonably aware of the new tools, tactics, and techniques the threat actors are using so they can protect themselves, the organization, and the people they serve.

To be fair, there are a few fundamental issues with training your Human Services workforce in information security. First, many Human Services workers typically do not consider themselves technologists; not only can they get intimidated by technology[2], but they can also find it stressful[3]. This is a barrier right off the bat that information security teams must both own and address.

Secondly, let's be honest: many direct care workers simply do not see information security as their job. Many healthcare professionals see 'their' field as the most important thing. While that is very important, we must ensure we all remember that it is not the only thing we should care about. After all, if you were a speech therapist, you would still want to ensure your patient was getting good nutrition, right? Ultimately, we must ensure that we see digital health as part of the whole person care equation.

[2] https://blogs.lse.ac.uk/businessreview/2020/08/24/are-healthcare-workers-stressed-by-information-technology/
[3] https://www.nature.com/articles/s41598-021-96851-1

THE LAST COMPONENT OF COMPLEXITY IS CYBERSECURITY TRAINING BUDGET. THIS IS A MULTI-DIMENSIONAL PROBLEM IN HUMAN SERVICES BECAUSE OF TWO MAJOR FACTORS:

Money

When you start any serious effort into training, you will find right off the bat that there are hundreds of vendors out there just excited to talk to you and your team about why their product is unique, effective, and just what you need. However, all of that comes with a price. Even though cybersecurity budgets have generally continued to increase[4] despite economic challenges, in **healthcare cyber budgets are usually only about 5% of the organization's total IT spend**. While most healthcare information security managers realize that their budget needs to increase, only 40%[5] believe that will happen.

Time

In human services, every minute spent in training is a minute you are not helping a an individual (nor billing for that either). I realize first-hand that this is a constant struggle and taking folks 'off the line' to learn about something like password security can be a hard sell. Many organizations say that they cannot afford to give training time to their staff, but I would argue that with **the average cost of a healthcare data breach at almost $11 million**[6], you cannot afford NOT to.

We will address both budgetary issues (including the other problems discussed above) as we dive deeper into how you can setup an effective training program.

[4] https://blog.barracuda.com/2023/06/19/cybersecurity-budgets-continue-to-increase-despite-economic-head
[5] https://www.tripwire.com/state-of-security/healthcare-providers-need-to-increase-budgets-for-cybersecurity
[6] https://www.healthcaredive.com/news/average-cost-healthcare-data-breach-11-million/688859/

Developing Your Approach to Training

Minimal information security training consists of having that one session every year that everybody in the company must sit through so you can check the proverbial compliance box. However, that is usually not very effective. This is not just because it's easy to forget what was in the session 11 months ago, but also because you have shown that the training is only so important to the organization. If the company does not think it's important, why should the employees? More advanced companies may have multiple training engagements throughout the year. However, the approach you take to what kind of training you provide is one that deserves careful consideration.

Function

The HIPAA Privacy Rule's Administrative requirements (45 CFR § 164.530(b)(1)[7]) states that training must be "as necessary and appropriate for the members of the workforce to carry out their functions." While there are many different approaches to have function-based training, the time-trusted process is laid out by the National Institute for Standards and Technology (NIST) Special Publication (SP) 800-16,[8] Information Technology Security Training Requirements: A Role- and Performance-based Model. SP 800-16 is a 232-page document with an exhaustive set of principles for Information Security training, but at its core it is based on three core concepts: **Awareness, Training, and Education**. Had we asked a few minutes ago, many of you may have said that Awareness, Training, and Education are synonymous – but they are critical concepts to cover and understand:

[7] https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164

[8] https://doi.org/10.6028/NIST.SP.800-16

Awareness

A learning process that sets that stage for training by changing individual and organizational attitudes to realize the importance of security

Training

Teaching people the basic knowledge and skills that will enable users to perform their job more easily

Education

Teaching and developing the ability to perform the complex, multi-disciplinary activities and skills to effectively implement security in each user's specific role(s) and job function(s)

Essentially, you promote the user's Awareness so you can Train them; that Training provides the fundamental skills of information security so that you can Educate users on the higher-complexity skills they need to effectively do their jobs. Or, more simply put:

01
Change their attitudes towards security

02
Teach users the basic skills of cybersecurity

03
Then teach them their job/role-specific skills

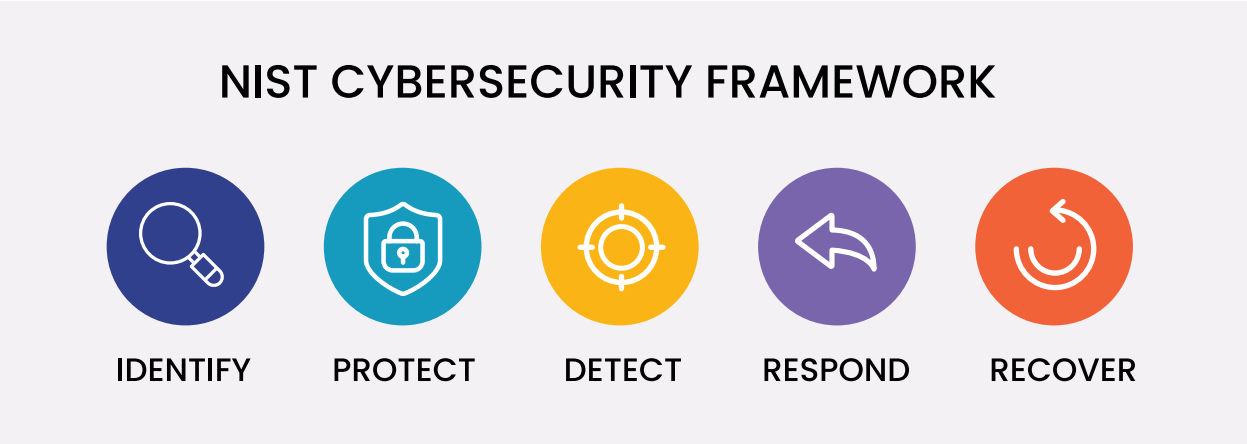
While that may sound like it is all semantics, it does highlight the importance of changing organizational attitudes (Awareness) for the Training to be successful, which is at the root of any effective information security training program (and how to overcome Human Services staff who do not see cybersecurity as their job). SP 800-16 is very focused on role-based training, and it provides a list of subjects that should be covered, a tool to identify organizational training needs, as well as a course development tool. Equally important, SP 800-16 lays out an information security training continuum that provides a crawl-walk-run roadmap for the development and continuing improvement of your cybersecurity education plan based on the Awareness, Training, and Education concepts.

[9] https://niccs.cisa.gov/workforce-development/nice-framework
[10] https://doi.org/10.6028/NIST.SP.800-181

SP 800-16 concepts have been evolved with the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework[9] which is documented in NIST SP 800-181[10]. NICE is focused on work roles and the Knowledge, Skills, and Abilities (KSAs) it takes to perform those roles. NICE breaks down training into 7 very role-oriented categories:

- Securely Provision (SP)
- Operate and Maintain (OM)
- Oversee and Govern (OV)
- Protect and Defend (PR)
- Analyze (AN)
- Collect and Operate (CO)
- Investigate (IN)

Another convenient feature of the NICE framework is that it is designed to work with the NIST Cybersecurity Framework[11] should your organization use that for governance of your security program. First introduced by President Obama's Executive Order[12] in 2013, the Cybersecurity Framework was created help private-sector organizations identify, prioritize, address, manage, and/or communicate cybersecurity risks. If your organization does not already have a formal Governance, Risk, and Compliance (GRC) framework, it is a great place to start.



Finally, NIST is currently producing a new document (SP 800-50[13]) which is currently only in draft. "Building a Cybersecurity and Privacy Learning Program" (CPLP) attempts to pull in elements from the other NIST documents to help organizations architect their own cyber and privacy awareness program including "awareness activities and campaigns, awareness training, practical exercises, topic-based training, role-based training, and education programs." While the document is not yet finalized, it may well be worth keeping an eye on for those looking for help to develop a comprehensive approach to your Cybersecurity training program.

[11] https://www.nist.gov/cyberframework
[12] https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/eo-13636
[13] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-50r1.ipd.pdf

Formats

Now that you have thought through what kind of training you need to provide, you must consider how it will be delivered. There are many kinds of security trainings you could offer: instructor-led, Computer Based Training (CBT), competitions (e.g., capture-the-flag or best phishing idea), self-paced, games, table-top exercises, awareness emails, external in-person (e.g., SANS courses) or webinar training, and/or community based (e.g., membership in your local ISSA chapter) just to name a few. Generally speaking, instructor-led training is best when you are teaching new or technically complicated skills,[14] and it is usually more difficult for learners to not pay attention as well. However, instructor-led training may not be realistic for all organizations based on size, geographic diversity, and general scalability.

Whatever your choice, you need to make sure that your training is effective. This is more than just conveying knowledge; it is also about making sure that your users understand the training. The issue here is workforce diversity and there are so many variables: different age groups, genders, races, education levels, experience, interests, and so on. Everybody will tell you that they have the 'best' solution (particularly if you ask a vendor), and that can take the form of everything from CBT to gamification.[15] Ultimately, the cybersecurity leaders must make sure the organization's training is engaging. In my experience, that outcome will vary based on the factors we have already identified, so a variety of training approaches is best. Just remember that you can use various devices to track the effectiveness of your training (e.g., surveys, tests, etc.) and make sure that when you find gaps you address those quickly.

[14] https://www.mindtools.com/ax1r6u5/instructor-led-training

[15] https://www.continu.com/blog/gamification-in-training

Develop a Training Plan

Executive Sponsorship

When discussing your organization's training plan, we would be remiss not to point out that it needs to start with executive buy-in. If you do not get the support of your leadership, you will continually be paddling upstream; fortunately, this is an easy discussion to have in Human Services because as we discussed earlier, HIPAA mandates training.

These are also great opportunities to change the conversation from your information security program being a 'sunk' cost to being a business enabler and advantage. If your Human Services organization does not suffer a data breach but your competitors do, it makes your services much more desirable. It's like the old joke, you do not have to outrun the bear, you just have to outrun the other guy. For example, if you can train the staff on how to avoid a phishing attack, you are also keeping all of your systems and personnel working instead of off-line while you try to recover. Keep in mind that you are probably better off with talking in terms of the potential financial impact (e.g., see Time above for the cost of a breach), but ultimately you need to establish the relationship with your leadership team to make the business case for training… and that is how you solve the 'time' issue we covered earlier.

Risk

As you start the thought process for 'how much' training is enough, you must first consider the fundamental building block of information security: risk. How much time you should spend training your staff is directly proportional to the amount of risk their roles represent. For example, if you are in a small rural clinic with 10 patients, you probably have lower risk than a provider in a large metropolitan area. Are your users centralized and accessing the network from Carts On Wheels (COWs) or working remotely from laptops? While size and location are but two factors in the calculus of risk, it does point out that there is not a one-size-fits-all approach. What is important is that you think through and cover (mitigate) all those risk factors in your approach.

How Much

To truly define how much training you should provide, you also must ask what is the intent of your information security program? Do you want to do the minimum training to 'check the box', or are you trying to implement a highly qualified and trained staff from a cybersecurity perspective? As a huge proponent of training myself, I would love to see everyone highly qualified… but what does that really mean? The truth is not everybody needs to earn their Certified Information Systems Security Professional (CISSP) accreditation to be good at information security ***for their job***. This is where the precepts in NIST 800-16 and the NICE

framework come into play; they help you to define what each role needs, then you develop a program to deliver that. Ultimately, many factors play into this decision, but knowing when training is sufficient is a skill unto itself.

Example Plan

Since there is no universal fit for a training plan, we can illustrate an approach by reviewing CaseWorthy's Information Security program that consists of the following:

Initial Training

Every user receives a one-hour instructor-led "Cybersecurity 101" training and must read and accept our Acceptable Use Policy before they are allowed to have any network access.

Introductory Training

After the user is given network access, they are assigned the following CBT modules:

- Security Awareness (15 mins)
- Reporting Phishing Attacks (7 mins)

Ongoing Training

- Monthly user awareness training emails
- Monthly phishing testing
- Email alerts about major industry happenings and/or threats

Role-Specific Training

- Executive Team (CBT, ~10 mins)
- Administrators (CBT, 7 mins)
- Administrators also receive an additional (and more difficult) monthly phishing test
- Cybersecurity members are additionally required to maintain certain annual CPE levels

Annual Training

Annually, all users take a one-hour, instructor-led Compliance and Information Security training.

Cybersecurity Awareness Month (CSAM)

During CSAM (October), the cybersecurity team runs a weekly awareness campaign supported by all or some of the following methods:

- Weekly Awareness Emails
- Month-long Cybersecurity Contest
- Website Blog
- Whitepaper
- Podcast with Cybersecurity Team

Useful Tips

So, you now have an approach and a plan for running your cybersecurity training. How do you make it valuable? How do you make sure it 'sticks' so people remember it? How do you get them to not cringe at the thought? Honestly, there is no golden bullet here, but here are some tips that you can use to help make your training program more effective:

Be Flexible

It is easy to say your team will be providing training on day X and hour Y, and if you do not make it, you will be reported to management. However, this is how we make enemies instead of building relationships throughout your Human Services organization. In addition to offering multiple training opportunities, you could consider alternate delivery methods. For example, we recently had a new batch of users who had to read & sign their Acceptable Use Policy, as well as take a CBT-based Compliance test on training they had recently completed. One user was having technical difficulties but had a priority to get back on the network to support a client need. Rather than wait for their laptop to be fixed, we sent PDF versions of the policy, Compliance slide deck, test, and an attestation form to sign to their personal email account. They digitally signed everything, took the test, and sent that back to our team.

This is a good approach to Cybersecurity in general. Always be ready to find ways to adapt and find other ways to be secure while reducing interruption or complexity to the user. Helping your users overcome those limitations are ways that we help to reduce user's intimidation and fear of technology.

Make it Entertaining

There are a few good approaches to making your training entertaining for your users:

Real-life stories

Everybody loves a good story, and users really enjoy a good story around a real-life event that you have encountered (even if it did not occur with your current company). Stories do not just make the discussions interesting, but they make them relatable by taking the concept from abstract to concrete.

Memes & humor

Just because security is serious does not mean it has to be dry. It is amazing how a good, appropriate, and funny meme at the start of the training can set users at ease. Do not over do these, but one every 5 slides or so seems to work well.

Engaging Visuals

As they say, a picture is truly worth a thousand words. Use good diagrams, high-quality images, and animations where appropriate to demonstrate the concepts you are teaching.

Videos

A great example of engaging visuals could be short videos from the internet (particularly YouTube). For example, when we talk about social engineering attacks in our initial training, we use a 2 ½ minute long YouTube video[16] from a past BlackHat where a reporter challenges a social engineer to try and get his information from his cell phone company. It does a wonderful job of quickly getting the point across, and over the years has been a great source of engagement and discussion.

Make it a Game

Sometimes even the dullest sounding activities become fun when you make it a game or contest. There are many resources out there for information security-based games and activities, but pretty much anything that your team can think of to engage your users can become a fun game.

For example, earlier we mentioned that we usually do a month-long cybersecurity contest for CSAM. For one year's CSAM one of our team members had the idea that we could offer a competition for any user that could think of an effective phishing campaign that would work against our company. The catch was it had to be based on what they could find based on Open-Source Intelligence (OSINT) sources and not 'insider' knowledge. This made our users think like an adversary, and it is a great way to help them see the weaknesses in our own systems. The two winners received trophies our team designed and 3D printed, so beyond the time commitment, it cost the company less than $20 in materials - and it was very effective. We then entered those phishing ideas as templates in our phishing testing system which went out to all employees (and as an added benefit, we never had another user say our phishing tests were unfair).

[16] https://www.youtube.com/watch?v=lc7scxvKQOo

Use Employee Friendly Language

Everybody expects, and in turn hates, 60 minutes of straight technobabble. Avoid acronyms where possible and use 'plain' English to make the concepts less intimidating.

To test this, you can have a non-technical person review the material to ensure it makes sense. I once worked for a large Internet Service Provider (ISP) and a confusing word or two in an email to customers could mean thousands of calls to the help desk. One of the system administrators had a sister who was very intelligent, dedicatedly non-technical, and happened to be a cheerleader. When we had an email going to all users, we would have her visit and read the email in front of us. If at any point she frowned or had a question, we smoothed that out to make it more easily understandable; we called this the "cheerleader test". The concept is valid - getting a non-technical person to help triage your material beforehand can save a lot of confusion down the road.

Tailor Your Training

It is easy to go and scour the internet for training material you can use. However, using real examples from your own company (e.g., phishing emails) really brings these points home and takes them from theoretical possibilities to 'this really happened'. I keep a folder where throughout the year I can save real instances of these examples to use in the next training update. This also includes examples around real tools the security team has in place, as well as operational processes, locations, and tools the general organization uses. Every time you can tie your training into a real use case, you are making that concept 'stick' by making it relatable.

Keep it Fresh

Speaking of updates, make sure you are updating your training. The phishing email from last month is stale in a year or two, and it might even have information about people who have long since left the company. Also, old articles make your training feel dated even if the information is still applicable. For example, I love using data from the annual Verizon Data Breach Reports (DIBR) for training, but I have to be sure to keep that data updated from year to year. Where appropriate, update that information on at least an annual basis. If you do not, it has the appearance of cherry-picking convenient facts and/or reducing the trainer's credibility.

Reward Positive Behavior

I have seen many security programs where they had tools like a 'wall of shame' where people who failed phishing tests were listed for everybody in the company to see; this is called negative reinforcement. However, numerous studies[17] have shown that positive reinforcement makes new behaviors learned faster and is the most effective approach. More pragmatically, if you reward the first person each month who reports a phishing email with a small gift card, token, or public recognition email, you are developing champions within the business units. However, if you shame people who click on phishing emails, you are only creating more people who despise and distrust your information security program and its team members. Remember, cybersecurity is here to assist and augment our internal business partners – not to be their digital police force.

Top of the Puzzle Box

One of my pet peeves is when training is provided like "do not use removable USB drives" without context or reasoning. If you think about it, doing this effectively treats adults like they are children and may cause them to react accordingly; all people will generally resist anytime they are forced into compliance. As Jeffrey Berk stated in his book *Champions of Change*[18], "people do not mind changing, but they hate being changed."

Do not just tell them a rule, tell them why – show them the top of the puzzle box. Explain why and enable them to make good decisions in use cases you may not have demonstrated. If you tell people that they should not use external USB drives because they could easily transport malware between computers and can automatically run that even without the user's intervention, you have now empowered them and trusted them with knowledge.

Responsibility

Finally, make everybody own their responsibility in the information security program. Far too often people see information security only as a concern for the folks under the CISO's org chart, but no security program can be successful if that is the case. Stress the teamwork aspect of cybersecurity, that we all have a role to play. I love to tell our company that cybersecurity is a team sport, and it has the added value of being true. This is a message that you have to tell every employee at the beginning, and constantly throughout the year – then you have to treat and empower them to show you meant it. We must make information security a team effort.

[17] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3050464/

[18] Berk, J.A. (2004). Champions of Change

Resources

Earlier we discussed the difficulty sometimes with finding enough budget to get good training in your organization. However, it is possible to get quality training without breaking the bank! The following are some resources that are available for free that you can use to help develop your own effective information security training program:

You!
The reality is that you have forgotten more about your organization than we will likely ever know. Using the information in this whitepaper, your knowledge, and a few hours of your time, you can put together a slide deck that reaches the folks in your team. Be willing to own this and make it fun.

Cybersecurity & Infrastructure Security Agency (CISA)
CISA has a number of free training resources available for civilian entities

- https://www.cisa.gov/resources-tools/training
- https://www.cisa.gov/cybersecurity-training-exercises

Fortune
This lists free online cybersecurity courses from top universities
https://fortune.com/education/articles/here-are-5-free-online-cybersecurity-courses-hosted-by-top-universities/

Health Care Industry Cybersecurity Task Force Resource Catalog
While the list is dated, there are still great resources here
https://www.phe.gov/Preparedness/planning/CyberTF/Documents/hccs-tf-resource-catalog.pdf

Infosec Institute
List of 13 free training resources
https://resources.infosecinstitute.com/topics/professional-development/13-cyber-security-training-courses-you-can-take-now-for-free/

National Institute of Standards and Technology (NIST)
NIST also has a list of free training resources
https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content

U.S. Department of Health and Human Services security awareness and training courses
HHS's list of free training resources
https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/security-awareness-training/index.html

YouTube
There are hundreds of free training videos available on YouTube… caveat emptor (buyer beware)
https://www.youtube.com/

NIST Special Publication 800-16
https://doi.org/10.6028/NIST.SP.800-16

NIST Special Publication 800-50 (Draft)
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-50r1.ipd.pdf

National Initiative for Cybersecurity Education (NICE) Framework

- **NICE Framework**
  https://niccs.cisa.gov/workforce-development/nice-framework
- **NIST SP 800-61**
  https://doi.org/10.6028/NIST.SP.800-181
- **Using the NICE framework PDF**
  https://niccs.cisa.gov/sites/default/files/documents/pdf/using%20the%20nice%20framework_pdf.pdf?trackDocs=using%20the%20nice%20framework_pdf.pdf
- **NICE framework one pager**
  https://www.nist.gov/document/niceframework062017.pdf

Conclusion

There are any number of obstacles to the development of an effective cybersecurity training program in the average Human Services organization. However, the information security program that has a well-defined approach to how they will offer that training, and an effective approach to providing that training, can be successful. What we, as information security professionals, must keep in mind is that as the saying goes, 'Rome was not built in a day.' We are aiming to develop a successful cybersecurity training program, and that is a marathon – not a sprint. We cannot let small setbacks here and there deter us; instead, we must keep our eyes on the horizon and take the incremental success as you continue to work through and constantly improve your training curriculum and associated processes.

About CaseWorthy

CaseWorthy is a family of products helping organizations to combine their program data and business operations into a single scalable solution. CaseWorthy strives to maintain the highest level of information security to protect its systems, data, and clients. To demonstrate its commitment, it maintains HITRUST and SOC 2 certifications to certify the program through independent third party evaluation. Our commitment extends beyond compliance; it's a proactive approach that drives us to continuously invest in cutting-edge technologies, adopt best practices, and foster a culture of security awareness among our team. By collaborating with industry experts, sharing insights, and staying vigilant against emerging threats, we contribute to the collective resilience of the business community and demonstrate our dedication to a safer digital world for all.

About the Author

Shayne Champion is the Chief Information Security Officer (CISO) at CaseWorthy. With almost 30 years in Information Technology (IT) and Cyber Security industries, Shayne has experience spanning a wide range of technical domains. He has built, worked in, lead, and/or managed a wide variety of IT organizations prior to joining CaseWorthy in 2020.