501Secure.org

Cybersecurity Assistance for Nonprofits

501Secure Cyber Chapbook Series

Building a Cybersecurity Awareness Program for Your Nonprofit

Third Edition

January 2026

As the 501Secure program enters its third year, our expert volunteers continue to serve the nonprofit community with practical cybersecurity information, awareness programming, expert guidance, and free services.

We hope you find this cyber chapbook on developing an awareness program helpful.

501Secure.org
Cybersecurity Assistance for Nonprofits

Questions about this guide or the 501Secure program contact the 501Secure Team at info@501Secure.org.

For immediate cybersecurity assistance, email help@501Secure.org.

“**When we rely so heavily on technology, it’s easy to take the threats we face because of it for granted.** Combined with the rapid pace at which technology and associated attacks change, we must do our best to keep ourselves, our families, and our colleagues aware and vigilant.

Humans all learn differently, but one thing is certain: we all learn by repetition. **It’s important for awareness of cybersecurity risks and best practices to be frequent and varied.** The key to a good security awareness program is connecting new ideas with old ones. People learn most quickly when they can relate new information to things they already know. To maximize retention, messages should be straightforward, build upon prior knowledge, and rely on real-world examples and comparisons to tangible, non-technical concepts. **Additionally, there should be a mixture of delivery styles covering at least reading, listening, watching, and doing.**

Cybersecurity education that sticks can be the difference between a user who clicks a link and a user who stops to think. And that difference can save an organization millions."

—Randy Rose, Senior Director of Security Operations & Intel at CIS

Read the full article, “Why Employee Cybersecurity Awareness Training Is Important.”
from Center for Internet Security: https://www.cisecurity.org/insights/blog/why-employee-cybersecurity-awareness-training-is-important

It is true that building a cybersecurity awareness program is a big job. Even so, you can make progress despite limited resources, if that is a barrier.

First, launch an awareness program with the understanding that it must be on-going to be effective. It will have distinct phases over many years. It can be achieved with small steps and simple efforts. It will require modest initial planning. It will require commitment, resources, shared responsibility, and patience. Eventually, you'll want to develop metrics for measuring progress. If you are charged with leading the effort, you will experience tremendous growth personally and professionally as a result.

Ask for help outside your organization when you need it. If you do not have a technology background and/or are new to cybersecurity, trust that as you grow your own awareness, your understanding of cybersecurity terms and principles will develop and in turn support the growth of your program.

There's never been a more critical time to begin building cybersecurity awareness in a nonprofit organization. Here are some basic first steps to jump start your awareness program.

1. Obtain explicit and visible support from your Executive Director.

The work of a cybersecurity awareness program focuses mainly on changing minds and habits to reduce staff behaviors that could lead to a serious security incident. Integrating secure ways of working into daily routines takes time and initially works against people's natural inclination to continue doing things the same old way. Senior leadership must champion your cybersecurity awareness program through both word and deed. This must include allocating time and available resources for program development and participating in a formal launch of the program. A program launch can be as simple as an all-staff meeting or an email that contains the following:

- why there is a need for the program
- ask specifically for staff cooperation
- explain what staff can expect in the next six to 12 months
- name the person(s) who will be leading the effort
- emphasize that cybersecurity awareness is a permanent addition to organizational life

Other executive actions should include the approval of standards for accountability, such as requiring staff to complete assigned training within a certain period and requesting that the program lead provide regular reporting on training outcomes and program progress.

As the program develops, the executive director and program lead can begin to explicitly link cybersecurity awareness to mission and business goals and begin asking staff to demonstrate the efforts they are taking to implement data security procedures.

Executive directors are busy people. However, prioritizing leadership's completion of assigned trainings in a timely manner and modeling the security behaviors that are being asked of staff encourages compliance and improves general awareness.

Executive leadership is a prime target for cyber criminals. Extra precautions should be taken to safeguard the devices, accounts, and data they handle. Creating role-based training for leadership should be on your "to do" list. But it's also important that an executive director complete the same training as their staff, so that they acquire the shared language that they can use to talk about security. If executive leadership is not completing assigned trainings, make an appointment with them for a live presentation. Provide a checklist to the administrative assistant to help executives complete security tasks.

2. Create a project charter with a timeline and milestones.

Select a realistic but energetic timeframe to cybersecurity awareness maturity. Consider an initial two-year goal for building a program foundation and an extended goal of achieving an advanced level of cybersecurity awareness, meaning deeply integrated security habits and attitudes, by year five. This timeframe still requires a brisk pace of organizational advancement but avoids the pitfalls that may come with aggressive action. Progress will vary by organization size. For smaller organizations, change may be easier. Set a timeframe and adjust it as you go along.

Initial milestones can be the first- and second-year deliverables. The following case study example represented by the list below was drawn from a small 48-person nonprofit with a budget of $5M. The organization first established an IT Security program charter. Some items on the list represent on-going efforts, others were discrete projects with a clear ending, and some were not easy to quantify:

- Completed gap analysis using the NIST CF framework
- Presented to executive director a prioritized list of mitigation interventions to reduce cybersecurity and data security risk
- Assembled small ad-hoc and permanent teams to complete action-learning project tasks and provide ongoing training, oversight, and incident response.
- Completed data inventory and classification for all data we handle and store
- Clear written policies that guide implementation of data handling, IT Infrastructure, and cybersecurity best practices that support our contractual and regulatory responsibilities.
- Strengthened relationship between IT staff and the rest of the organization through the use of a common cybersecurity language and through the shared responsibility for ensuring the consistent availability, integrity, and confidentiality (CIA) of the organizational and client data we all steward.
- Review of current permissions, document access, data handling, and storage methods and recommendations for change to improve our security posture using the "least privilege" model
- Add and maintain regular IT Security Program related activities to administrative calendar
- Informed by the above actions, provided an on-going program of basic and incremental cybersecurity training to all organization employees, contractors, and volunteers.

3. **Establish a dedicated role (e.g., cybersecurity awareness educator, chief information officer, data privacy lead, etc.) to develop, implement, measure, and manage your program.**

If you are new to cybersecurity and awareness training, your own learning is essential. Initially, this work also requires a lot of meetings, thinking, planning, and curating of content. It can be done part-time and once the program is sufficiently developed supported possibly at quarter-time with the help of volunteers.

As a cybersecurity awareness program leader, you'll be encouraging your organization to work together on cybersecurity awareness training and projects. To achieve this, you may need to reach outside the organization for assistance from volunteers, consultants, and vendors. You may attend trainings or conferences. Having a clearly defined awareness role with an appropriate title can be helpful with these interactions.

4. **Take a whole organization approach to integrating cybersecurity and data security into the work you do every day.**

Consider the idea that a cybersecurity awareness program should include more than just training people about phishing emails or providing checklists of do's and don'ts. Phishing is an essential topic, as is communicating best practices. However, if there isn't a general awareness of the resources (software, hardware, networks, processes, data, and compliance responsibilities) that are most critical to your organization, it can be difficult to prioritize what's most important to protect and what kinds of training is most relevant.

Generating an asset or resource inventory is key, but it can be a time consuming and lonely task for one person. A structured, whole-organization approach enables deeper learning and greater awareness through crowdsourced, hands-on discovery and analysis. It also puts the security needs of a specific program or dataset into a wider context, opening opportunities to both streamline and secure shared data and processes.

Working together, leadership and staff develop the awareness and understanding of the cybersecurity risks unique to your organization, as well as the methods to actively mitigate them. Because a whole organization approach encourages data security ownership, it facilitates the integration of cybersecurity readiness into daily business. Over time, new software, external relationships, and procedures can be routinely considered through the lens of safe data handling standards and practices.

5. **Purchase, curate and/or develop cybersecurity training that covers general "cybersecurity 101" topics to function as a foundational training.**

Whether or not you build your own trainings or buy a training package, curate your own content, or subscribe to a training service will depend on many factors. Chief among these factors is the availability of the time and resources. While it is tempting to completely outsource your awareness program, it is not recommended**.** To be effective, awareness trainings and activities must be tied to the specific data, software, networks, processes, and compliance responsibilities unique to your organization. As your program develops, you'll likely use a combination of sources. Initially, you can start with free and low-cost options as needed.

Low-cost Learning Delivery Methods

- MS Forms
- PowerPoint
- Adobe Express
- Viva Learning
- MS Sway
- Google Sites
- Google Forms

Intermediate-cost Content Vendors

- Articulate 360 (Rise and Storyline) – Provides high quality training content and tools to build trainings. (Includes LMS to host SCORM trainings)
- SANS (provides deeply discounted government/nonprofit rate)
- Phishing simulation and awareness training vendors – (monthly rate per user) (e.g., KnowBe4, PhishingBox, Wizer, CanIPhish, Right-Hand Cybersecurity)

Free or Low-cost Content Sources

- MS Defender (requires MS365)
- Free vendor promotional explainer videos on YouTube
  - @NetrixGlobal – Netrix on Youtube
  - @EyeonTech – Tech Target on Youtube
- Free content from Cybersecurity and Infrastructure Security Agency (CISA)
- Free content from Federal Trade Commission (FTC)
- Free LinkedIn Learning accounts for Washington State residents (non-WA residents check with your local library system for availability)
- National Cybersecurity Alliance
- The National Cyber Security Centre (UK)
- Summarize content from webinars and cybersecurity newsletters and make it relevant to your organization.
- Use the NIST CF 2.0 Framework for topics or to structure a training plan; also see the NIST Small Business Quick-Start Guide

Topics appropriate to include in a general cybersecurity training.

A comprehensive first training should cover a range of cybersecurity 101 topics. One hour of interactive learning content with quizzes will create a foundation upon which future trainings can be added. Once created, purchased, or curated, this can also serve as cybersecurity training for new hires.

Plan on providing at least one major cybersecurity training annually. As your program develops, supplement annual trainings with 5 to 10-minute trainings and information monthly.

The topics below are provided for reference only. The first three topic area include content detail for illustration purposes. You can find a list of recommended general training topics and subtopics in the NIST Special Publication 800-50.

Suggested Topics	Content Detail
Why Is Data Security Important? What are cybercriminals seeking? What is my role in protecting data?	• Data safety Fundamentals • What is sensitive information? • Data classifications • What is PII? • How to determine how data should be classified?
Valuing and Protecting Data What is the difference between confidentiality, privacy, and data security.	• What are data breaches? • Do's and don'ts of data handing • Categories of compliance regulations
Using Mobile Devices	• Why are smartphones a risk? • What are the threats to mobile devices? • Personal devices • Public wifi • Bluetooth • IoT
Using Social Media Using the Cloud Social Engineering Malware Ransomware Password Protection Protecting Yourself Online Protecting Yourself at Work Protecting Yourself When Working Remotely	

6. **Launch your program with an announcement by your ED to all staff. Follow that up by assigning a general cybersecurity training (cybersecurity 101) that introduces concepts and a shared language around cybersecurity, privacy, and data security.**

See step 5 above for detail on options for general cybersecurity training.

7. **Work your plan. Create sustainable structures (Incident Response Team, regular progress reporting, action learning teams) and procedures. Document them and make sure they can be easily accessed by everyone in your organization. Support policies and procedures with role-based trainings.**

If you are an IT professional who supports a nonprofit and you find yourself tasked with creating a cybersecurity awareness program, it may feel like a heavy lift to add to your infrastructure support responsibilities. Taking a whole organization approach by forming small teams and leveraging the staff expertise (HR, learning development, content creation, database management, etc.) distributes the workload and promotes engagement and learning. Instead of passive-learning exercises assigned to meet compliance requirements, aim for engaged program building and participation. For example, if you already have an asset inventory, form a cross-functional Incident Response Team and systematically review it with them to determine which items are critical. Add to the list as needed. It should also include processes and compliance responsibilities.

8. **Growing your program for the long-term. It is practical and efficient to use a combination of action-learning and custom and purchased training to communicate policies, support behavior change, and grow awareness. Methods of cyber-attack constantly change, communicating new threats is a critical aspect of any awareness program.**

Aim initially for generating conversation and inquiry through general cybersecurity and data security best practices training. Add action-learning to assist with developing an asset inventory and evaluating how critical each is to your organization. Create policies and procedures to protect your critical resources. Create, purchase, or curate role-based trainings unique for your organization to communicate policies and procedures.

Trainings should describe how particular attacks can happen using real-life examples. You can increase the specificity and degree of technical information as staff understanding increases. Keeping up on the latest trends can be time consuming but necessary. If you don't have a dedicated IT support team to assist with this, here are some additional options.

- Outsourcing some of your awareness program to a qualified vendor
- Purchase content
- Signup for cybersecurity newsletters or threat alerts relevant to the technologies your organization uses.
- Read popular annual cybersecurity reports released by major software companies such as Verizon, IBM, and Microsoft.
- Get familiar with OWASP.org

To track your program’s impact, consider using the SANS Institute cybersecurity awareness model. For more information on this, see the “Cybersecurity Awareness Assessment Tools” section below.

Integrating Action Learning into Your Cybersecurity Awareness Program

Use action learning to maximize your awareness training efforts. Some ideas for action learning projects are crowdsourcing information gathering, policy and procedure development, or completing a post-training checklist to confirm that security standards have been met. A well-structured, hands-on learning project can demonstrate for the learner how awareness training directly applies to daily work.

Action learning can be team based or completed by individuals. It can be focused on solving a problem (e.g., creating a business continuity plan) or implementing a series of recommended security actions. A great example of action learning is a tabletop exercise to test a cybersecurity incident response plan.

You can integrate action learning into trainings or develop separate projects to meet awareness program milestones more quickly and efficiently. Participants must be adequately prepared through prior trainings. Activities should be structured and include a schedule of meetings, deliverables, and deadlines. Written instructions should be provided that clearly explain the rationale, purpose, and end goal. Map action learning activities to learning outcomes. What you want participants to learn should map directly to your awareness program goals.

Teams can be formed on a voluntary or assigned basis. When appropriate assemble teams from different programs or departments. Be prepared to motivate participants throughout the project. They will need help mapping their activities to organizational goals and the security of the data they use in their daily work. Teams should be small with the skills and experience relevant to the purpose. All participants should have the opportunity to contribute, collaborate, and direct their own learning process.

Cybersecurity Awareness Training and Incident Response

Awareness training is important to incident response planning because it helps staff identify and report security incidents quickly. When staff is aware of the latest threats and vulnerabilities, they can take steps to protect themselves and the organization from attack.

Cybersecurity awareness training also helps staff to understand their role in the incident response process. For example, staff may be responsible for reporting suspicious activity, isolating infected devices, or backing up data. By understanding their roles and responsibilities, staff members can help to minimize the impact of a security incident.

Cybersecurity awareness training can support:

- Reduced risk of data breaches
- Faster detection of security incidents
- Improved response effectiveness
- Promote a shared security language and ethic

Who should receive training?

Anyone with access to your information systems should get training:

- Staff
- Contractors
- Volunteers
- Board members
- IT

Evaluating Program Impact

While cybersecurity awareness training is a must-have, using an awareness framework to assess cybersecurity awareness maturity is a nice-to-have. However, a maturity framework can assist you with informal, qualitative efforts to identify areas for improvement, manage organizational change, and improve employee morale. A framework can be helpful for identifying and interpreting common indicators of low awareness and recognizing indicators of improvement. A framework can be useful for communicating program progress to leadership.

There are several different maturity models available. The SANS Security Awareness Maturity Model is a researched framework developed by a respected for-profit cybersecurity training organization. SANS provides certifications and advanced training for cybersecurity professionals. Their professional development courses are quite pricey. However, they have made their framework tools and some learning content available for free.

Free leadership training and security awareness content
https://www.sans.org/cybersecurity-leadership/

SANS Security Awareness Planning Toolkit
https://go.sans.org/lp-kit-security-awareness-planning

SANS Security Awareness Roadmap
https://sansorg.egnyte.com/dl/zLpElKi24l

Example Free Trainings

Security Awareness and Training
Created by Department of Health and Human Services (HHS)
https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/security-awareness-training/index.html

Free and Low-Cost Online Cybersecurity Learning Content
https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content

Cybersecurity Training & Exercises
https://www.cisa.gov/cybersecurity-training-exercises

Top 10 Free Cybersecurity Training for Employees
From edapp.com
https://www.edapp.com/top-10-cyber-security-training-for-employees/

NIST Special Publication 800-16 Revision 1 (Draft)
https://www.niatec.iri.isu.edu/(S(5pvzas455hrdzsrxbwh1ndqb))/GetFile.aspx?pid=379

NIST Special Publication 800-50
Building an Information Technology Security Awareness and Training Program
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf

Recommended Reading

Web Article, "Why Employee Cybersecurity Awareness Training Is Important"
From Center for Internet Security
https://www.cisecurity.org/insights/blog/why-employee-cybersecurity-awareness-training-is-important

Web Article, "Sizing Up Your Cyber Risks"
From Harvard Business Review
https://hbr.org/2019/11/sizing-up-your-cyberrisks

Web Article, "Cyberattacks Are Inevitable. Is Your Company Prepared?"
From Harvard Business Review
https://hbr.org/2021/03/cyberattacks-are-inevitable-is-your-company-prepared

Video, "Treat Cybersecurity as a Business Investment for Better Outcomes"
From webinar by Gartner with video and presentation slides
https://www.gartner.com/en/webinar/458795/1082738

Cybersecurity Awareness Program Check List

Every awareness program should reflect the nonprofit it serves. We share the following program development steps as only one possible path to sustainable awareness. Program components and structure must align with a nonprofit's size, technology, available resources, and mission. You'll notice on the list below that awareness activities are mixed with security activities. This requires that an organization to work iteratively to update governance systems for a remote work environment. Security and governance tasks are used as learning opportunities when possible. We hope that you will find ideas, inspiration, and confirmation from reading development journey in checklist form.

Year 1:

_____Select staff member to serve as security program lead (at least half time during initial development).

_____Obtain executive leadership support and approval for the program

_____Write project charter (1 to 2 years for foundational program development) with the intent of building a sustainable, on-going awareness program

_____Obtain an internal program sponsor

_____Identify and recruit external cybersecurity expertise (consultant or volunteer) ***501Secure can connect nonprofits with external cybersecurity experts for projects or quick consults.*

_____Obtain project charter approval from program sponsor and executive leadership

_____Executive leadership announcement about project launch to staff and board

_____Cybersecurity awareness research and self-education by program lead

_____Draft 12-month cybersecurity awareness training plan for organization and content calendar

_____Establish human resources standards and procedures for assigning and tracking training completion

_____Draft general cybersecurity policy (privacy, confidentiality, and data security)

_____Draft general IT policy (how to request IT support, care for organization devices)

_____Create IT policy summary guide with link to full policy and require that all staff read and sign

_____Create cybersecurity policy summary guide with link to full policy and require all staff to read and sign

_____Assign 1-hour of basic cybersecurity training to all staff (our first training was purchased externally and contained 12-interactive modules)

_____Assign organization-specific phishing tutorial developed in-house (e.g., how to recognize and report phishing, provide specific examples of phishing emails received by the organization)

_____Create new-hire orientation to our IT service desk and technology learning resources

_____Form cross-functional, five-member, incident response team representing business and IT support functions, e.g., chief information officer, IT Support, human resources, operations, deputy director (or equivalent), executive director (participates during emergencies only), communications lead

_____Define and formalize two security roles: Data Steward (all staff members fill this role) and Resource Owner (staff members who have statutory ownership or admin rights for IT infrastructure and cloud applications).

_____Form a NIST Cybersecurity Framework self-assessment team to review organization's current compliance with cybersecurity framework (two volunteer cybersecurity experts, program lead, and IT support lead)

_____Create IT Security SharePoint to share awareness information with staff

_____Create MS Teams channels to support work by NIST self-assessment team, asset inventory team, and incident response team

_____Form asset inventory team (managers and key business function staff)

_____Prepare instructions, training, and tools for NIST self-assessment team, asset inventory team, and incident response team. Set goals and meeting schedules.

_____Develop and provide cybersecurity training for managers and key data stewards. Training to establish shared cybersecurity language. Training includes content on cybersecurity risk, business threats, and asset inventory purpose and procedures. Training supports managers as cybersecurity champions for their teams.

____Launch asset inventory project to catalog data and cloud applications used by program teams. Team members classify data by sensitivity (restricted, confidential, internal or public). They also evaluate the potential impact that compromised data, software systems, and processes would have on programs or the organization.

____Build cooperative relationship between IT support and human resources through incident response team collaboration and action-learning projects

____Develop new-hire onboarding and device provisioning processes suitable for a 100% remote work environment.

____Develop staff separation procedures that address knowledge transfer and device deprovisioning suitable for a 100% remote work environment.

____Complete post-asset inventory interviews to review completed inventory worksheets

____NIST self-assessment team evaluates results of current security status against security framework and reports findings

____Update draft and finalize of 12-month cybersecurity awareness training plan to support security and training goals developed from the asset inventory and NIST self-assessment findings

____Incident Response Team meets monthly to complete the following tasks:

- develop team charter
- define roles and responsibilities
- develop standard meeting procedures
- develop meeting minutes procedure to ensure team meetings are documented
- determine when and under what circumstances team will be activated during an emergency
- determine what constitutes an incident and emergency
- create emergency communication plan
- draft incident response playbook (basic scenario responses for team to follow)
- assemble comprehensive list of org contractual and regulatory responsibilities
- complete team trainings and tabletop exercises to test the playbook
- establish an event reporting and logging policy and procedures
- work with program managers to develop incident response and business resiliency plans for each program

____Assemble asset list from asset inventory sheets

____Analyze asset inventory sheets and notes from follow up conversations with inventory team. Compile a list of security recommendations for policies, procedures, configurations, training, technology investments, and other actions

____Review recommendations with executive director, program managers, and IT support staff to create prioritized list of action items

____Formalize data classifications and create data handling guidelines

____Draft or update policies and security procedures based on recommendations list

____Create security action item timeline. Schedule and assign work as action-learning to increase security awareness, when possible

____Create 90-minute training and resource guide on privacy, confidentiality, data security, incident response, data stewardship, and resource ownership. Training to include data handling guidelines, a remote work security checklist (action-learning), overview of compliance responsibilities, and links to internal resources and policies.

____Establish tech support ambassador program, in which IT support staff give guest talks to program team meetings about security or give mini tech trainings

____Create monthly, quarterly and annual reporting and staff activities. Add them to administrative and staff calendars. E.g., annual trainings, October Cybersecurity Awareness Month, International Password Day.

____Create downloadable cybersecurity emergency plan for all staff that includes emergency contact plan if we lose access to our network; incident reporting procedures; and what to do during specific scenarios (e.g., lost laptop, ransomware notice, clicking on a link in a phishing email, etc.)

____Create resource owner sheets that contain master records for all hardware and software assets and audit quarterly. Include in each record account ownership and recovery information and a current list of users and permissions

____Train IT support staff on incident detection and response, and training on incident response team procedures

____Provide IT support staff access to Resource Owner sheets

____Create Software as a Service (SaaS) standards for evaluating potential cloud vendors

____Require new cloud apps to be vetted by IT support using the SaaS standards checklist

____Train Resource Owners on how to stay up to date on threat intelligence for the cloud applications they steward

____Update data retention policies based on asset inventory and compliance responsibilities

Year 2:

____Continue development of role-based trainings

____Continue working through security action item list

____Begin schedule of monthly 5-to-10-minute refresher trainings

____Continue quarterly updates of Resource Owner sheets

____Advanced cybersecurity training for IT staff and incident response team

____Tabletop exercises provided by external facilitator for incident response team

____Integrate Phishing Simulation Software into the cybersecurity awareness program