Pacific Library Partnership

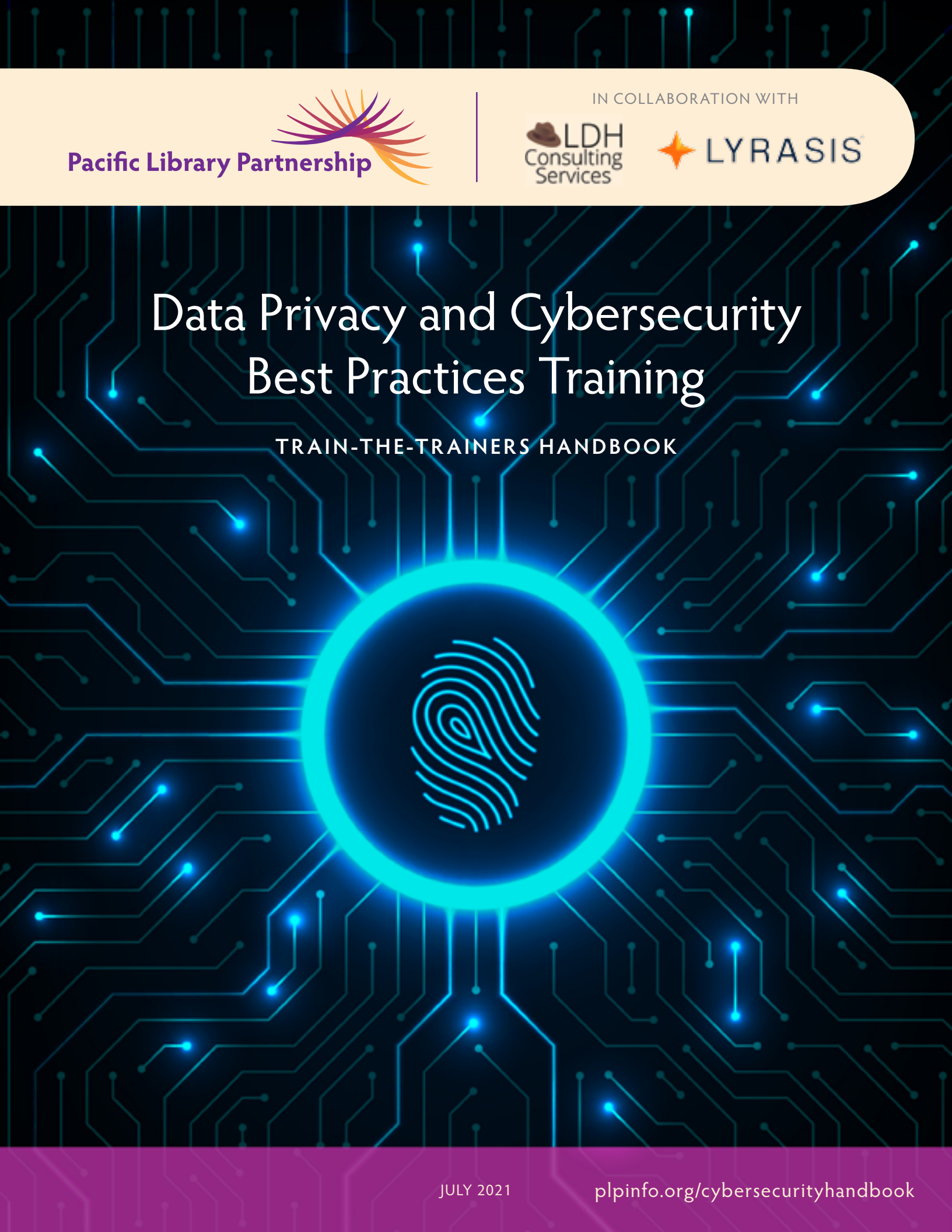
IN COLLABORATION WITH

LDH Consulting Services

LYRASIS

Data Privacy and Cybersecurity Best Practices Training

TRAIN-THE-TRAINERS HANDBOOK



JULY 2021

plpinfo.org/cybersecurityhandbook

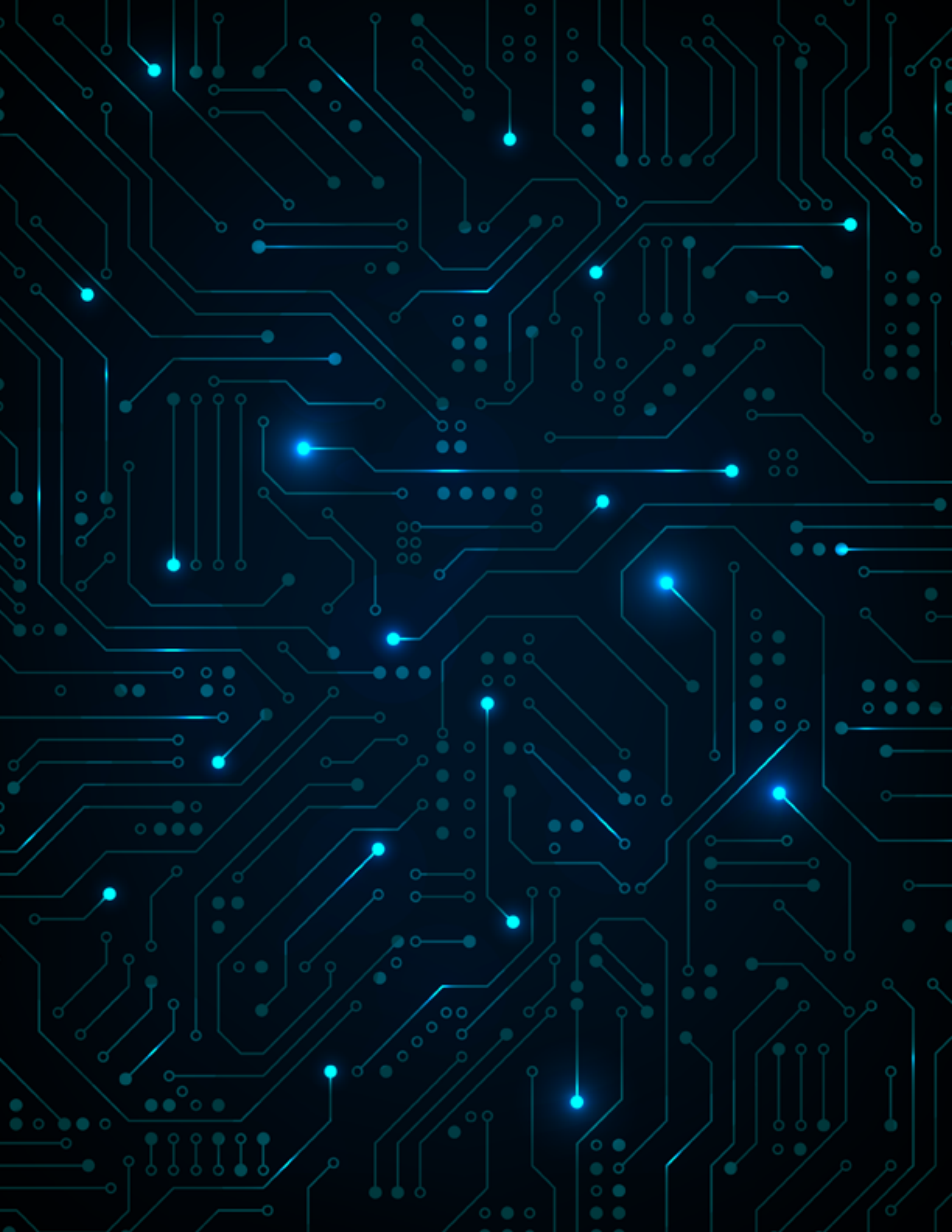


Table of Contents

SECTION 2

SECTION 3

SECTION 4

SECTION 5

This page intentionally left blank

SECTION 1

Introduction and Training Best Practices

SECTION 1.1

INTRODUCTION TO THE HANDBOOK

Library privacy and cybersecurity training is a critical component in giving library workers the knowledge and skills needed to protect patron privacy in the workplace. Alongside applicable policies and procedures, training serves a variety of functions: orienting new workers into the concepts of library data privacy and security, highlighting specific patron data considerations, and exploring different digital privacy and security tools. Training provides a dedicated space for people to explore and practice the skills needed to achieve privacy and security goals in the library—a space that allows for questions, open discussion, and practice in applying new or expanded skills and knowledge.

Developing training can appear to be deceptively simple—all training requires dedicated resources, time, and staff. More often than not, library workers charged with creating and conducting training might not have extensive experience in training preparation or delivery. Other library workers might not have much confidence in their teaching skills, or do not know how to go beyond a readthrough of the privacy or security policy to the training class. Even library workers with some training experience might want to find teaching methods and tools to expand their training repertoire.

This handbook is a guide for library workers interested in creating library data privacy or cybersecurity training programs that are both effective and designed to meet their library's needs. This handbook helps library workers through the training development and teaching processes, providing methods and skills to improve and expand training skills. The handbook also provides information about the training planning process as well as how to support learners outside of the training room.

How To Use This Handbook

The handbook contents range from creating your training program to training planning and logistics. Trainers of any skill level can use this handbook based on their current needs. While this handbook contains information about creating and maintaining privacy and cybersecurity training programs, some trainers might opt to skip that section and work on individual training development. Therefore, trainers can and should focus on the sections in which they need the most guidance at that time.

The handbook is a guide, and not a declarative document about which methods are right and which are wrong. Each method and strategy have strengths and weaknesses, which the handbook will try to highlight for the trainer. Trainers should use their best judgment in choosing which methods and strategies to use in their training development and program building.

Resources For More Information

As a part of the PLP *Data Privacy Best Practices For Libraries* project, the handbook complements the Train-the-Trainer workshop series conducted in Spring 2021 and expands on the workshops created in those series. Trainers are highly encouraged to review the Train-the-Trainer workshops, as well as the PLP *Data Privacy Best Practices Toolkit for Libraries* published in 2020. The 2020 Toolkit also contains references to other privacy training created by libraries that trainers can review and adapt for their training. Trainers are also encouraged to review the PLP *Data Privacy Best Practices for Libraries* training conducted in 2020 for training ideas and examples.

SECTION 1.2

MAKING THE CASE FOR TRAINING

Libraries talk about privacy as a core tenet in professional standards and ethics, but when it comes to practicing privacy in the field, libraries sometimes struggle in prioritizing privacy practices. Similarly, security is often overlooked, particularly if organizations are relegated to rely on other departments outside of the library to provide these services. Training is not exempt from these struggles. Trainers might find themselves coming up against an invisible wall when trying to get organizational support and resources for staff training. Alternatively, some organizations may have the resources, but library staff or administration may be ambivalent about training or there may be limited interest to get through an hour training session.

The latter situation can be addressed with buy-in strategies using some of the arguments about why privacy is important in the 2020 Toolkit and the strategies discussed later in this section. Trainers hitting the invisible barrier no matter what they try, however, might be encountering a barrier by organizational culture.

Organizational Culture Issues And Strategies

It's hard to change organizational culture. Unaddressed organizational culture issues often turn minor barriers that could be addressed with time and resources into barriers that require substantially more resources to address with little chance of successful resolution. Identifying organizational issues will not guarantee that you will succeed, but you will at least be able to anticipate and plan around these issues when they arise.

Common Organizational Issues

Some common organizational issues are:

- **Communication —** every organization has some form of communication issue, including:
  - Lack of established communication lines and processes, particularly between departments, administration, and staff
  - Convoluted communication practices, such as a process that requires an excessive number of staff to approve an internal announcement or communication
  - Deliberately withholding information from other library workers needed to perform their daily duties or to make operational decisions in a timely manner
  - Communication bottlenecks
- **Interpersonal relationships —** fraught relationships between departments or offices, or between key individuals in the organization

- **Interpersonal or interdepartmental struggles** around budget, resources, and staffing
- **Exploiting uneven power dynamics** through further marginalization of minoritized people in the organization

How To Cope

Trainers coming up against any of these issues can plan and cope with these issues in a couple of ways while trying to secure support and resources for their training:

- **Spend political capital wisely —** How much political or professional capital you have in the organization? How much you can realistically spend in addressing these issues? If you have very limited capital in the organization, picking what to push on becomes even more important if you want to at least have some privacy or security practices and training at your organization.
- **Choose your battles wisely —** You can fight every fight, but you will find that approach will easily eat up time, resources, and motivation. Strategically choosing what issues to address can help reserve political capital and energy in the long term.
- **Failure can happen anyway —** Sometimes things fail due to factors out of your and the organization's control (case in point – the COVID-19 pandemic). The best you can do is to regroup and determine your next actions.
- **Fight the temptation to fix everything —** You might be successful in creating small spaces that function better than the overall organization, but remember that organizations have a life of their own, and can be resistant to large long-term changes. Focus on what you realistically have the power to influence your organization. Small acts can lead to the biggest changes in an organization.

Buy-in Basics

When we advocate for our training needs to others, we can bring research, professional standards and codes, and examples of libraries "doing it right" to the conversation; however, these can only go so far. People are not persuaded by reason or facts alone. There needs to be a connection between your audience and the topic. This requires understanding your audience's motivations, concerns, and needs.

Understanding Your Audience

Two questions will help understand your audience:

1. What are their motivators and concerns?
2. What can they relate to in terms of interests, beliefs, and experiences?

Some motivations and concerns can be:

- Compliance with regulations, organizational policies, or professional codes
- Financial or reputational liability surrounding library data breaches or leaks
- Professional, personal, or civic pride
- Pressures — work, life, state of the world
- Organizational culture — collaborative, competitive — as well as organizational issues
- Personal or professional curiosity and challenges

Finding out what your audience relates to can highlight certain barriers, including:

- **Lack of (strong) ethics codes —** some library workers or partner departments and organizations may come from other professions that do not have strong ethics codes and might not understand why librarianship's ethics codes are as strong as they are and why these codes should inform library work.
- **Social or organizational privilege and power —** some folks can only relate with others with the same backgrounds, beliefs, and experiences, which can make it difficult to make the case for privacy or security that benefits others outside of that small circle.
- **Learned versus lived experience —** While knowing something is valuable, there is still a disconnect between knowing something and experiencing it which leads a person to develop different understandings of something depending on how they know of it.

Learning more about your audience's motivations, concerns, and experiences can help you create a narrative that ties together the facts in such a way that the audience can both understand and relate to.

Before creating the pitch, you also need to understand your audience's needs. In the case of privacy or cybersecurity training, making a pitch that doesn't reflect the library's needs can cause the pitch to fail. There are several ways you can gather this information:

- Department or workgroup meetings and listening sessions
- Informal meetings, such as coffee chats
- Internal discussion boards, email groups, and shift logs
- Privacy and security audits
- Data inventories

You can also use surveys, but be mindful of survey fatigue. Like not everything has to be a meeting, not everything has to be a survey.

Creating The Pitch

Pitches can take different forms, depending on the location, time limits, and other logistical factors in the delivery of the pitch. Sometimes you have time in a meeting, other times you only have a minute in the hallway. It's worthwhile to spend some time working through the following exercises to break down the components of your pitch and refine them to accommodate the different situations where you might need to give your pitch:

Three-minute Story — You only have three minutes to give your pitch to your audience. What are the most important points that you need to cover to give your audience the information they need and to support your proposal? Create a three-minute pitch with those points.

The Big Idea — This is similar to the three-minute story exercise above, but reduced down even further. You only have one sentence to make your case. Create a sentence that articulates your proposal as well as what is at stake.

Storyboarding — This exercise can help build the narrative structure of your pitch and can incorporate the pitches created in the previous exercises. Take some sticky notes and create an outline of your pitch, using one sticky note for every point or idea you want to communicate to your audience. This could also include your Big Idea, or multiple Big Ideas (if you want to have a Big Idea for each slide in a presentation, for example). Move around the notes as needed until you find a flow that best suits your audience.

Getting Buy-in — Strategies

Having a solid pitch is a major component in gaining buy-in for training, but it is only one part of the process. What other ways can you increase your chances of getting buy-in and for your training proposals to succeed?

- **Have vocal allies in the organization —** The more organizational influence and power they have, the better; however, do not discount the influence that strong allies in the front lines can have in an organization. A bottom-up approach can be as effective as having a strong advocate in administration. Allies are also very good people to get feedback and perspective on proposals or potential problems that you otherwise wouldn't think of.
- **Make a place for yourself at the table —** Some of us have a spot on the table in organizational discussions and decisions. If that's not the case for you, find someone (such as an ally mentioned above) who can negotiate a place for you. This way lessens the chance of others at the table feeling threatened in terms of possible changes to organizational power balances.

- **Come with a story that aligns with their motivations and concerns —** Show that you know your audience by reflecting their concerns, motivations, and needs in your proposal.
- **Come with a realistic actionable plan or outline —** Bring an actionable plan that is within the means of your organization. An example of this is how your proposal can use available resources. However, don't forget to make the argument to shift responsibilities if you are proposing staff time and changes in duties for existing staff so that they have the dedicated time to work on the projects you're proposing.
- **Strive for positive-sum outcomes —** If you think of this conversation as a "winner takes all" or "everyone loses," then you will most likely end up with that result. Reframing your conversations as a "how can this plan benefit everyone" talk can help you determine which areas in the plan are most important to prioritize, and which areas are the most important to your audience.

SECTION 1.3

THE "WHEN," "WHERE," AND "WHO" OF PRIVACY AND CYBERSECURITY TRAINING

When To Train

Training can be proactive, reactive, or somewhere in between.

Proactive training is training that is regularly scheduled or is part of an established process. Scheduled training will help make sure that all workers will at least have a passing familiarity with data privacy and security practices at the library. This includes onboarding training, annual refresher training, and other routine training and scheduled opportunities for open discussion (such as monthly coffee or lunch gatherings) and professional development (such as staff day programming). You can cover the basics and also take deep dives into particular aspects of library data privacy in these scheduled trainings.

Reactive, or event-based, training occurs when a privacy-related event calls for additional training support for the library. This doesn't have to be limited to events at your library, either. You can use other library privacy incidents to provide training for your staff before the same incident happens at your library.

Even when policies are followed, event-based training can positively reinforce behavior and knowledge. Think of a law enforcement request for patron data —that event in itself can make staff anxious about making sure that they are following policy, and training can be one way to help with that anxiety. The event is fresh on everyone's minds and there's an incentive to talk privacy or security while you have their full attention (that otherwise might not be there with scheduled training).

You'll find that several types of training can be both proactive and reactive. These could include implementing new processes, working with vendor products and services, and major changes to policies and procedures. Ideally, you want a mix of scheduled training, impromptu training, and refreshers in your data privacy or cybersecurity training program. There's no magic ratio, but the one thing you want to avoid is to have your training be all reactive training. Train early and train often.

Exercise — When Do You Train?

- How many of the privacy/cybersecurity training at your library are scheduled training, such as onboarding?

- How much of the privacy/cybersecurity training you have held was the result of privacy or security-related incidents, such as ransomware or a possible data leak or unauthorized access?

- How can your library schedule training to minimize gaps in knowledge about privacy and security practices in the library?

- What types of event-based training seem to work well at your library? How can they possibly be modified into either scheduled training or asynchronous, self-paced training for staff?

Where To Train

Training can take place in person, online, or as a hybrid of both.

In-person training can create unique learning environments depending on the mix of people in the room. While lecturing is common at in-person training, group discussions and activities are common active learning methods for in-person training. One particular mode of learning that can't be easily replicated online is the "hallway track" or the conversations that come up in breaks, or before or after the training session. In-person training is limited by where and when they are held.

Online training can get around these limitations through asynchronous content delivery. You can pre-record lectures, assign readings, and have participants take quizzes or answer questions in discussion forums. You can build some opportunities for big and small group discussions, but most likely not replicate the hallway track mentioned earlier. Online training sessions can be synchronous, but you will run into the same schedule limitations as in-person training. Depending on resources, the software used for training can be a limitation for both the instructor and learner. One common example of this limitation is software or training materials that are not usable with screen readers. Another limitation comes with captioning. You can create a transcript of what you will say, but transcriptions only capture a portion of what everyone says in a synchronous training session if the session does not have live captioning.

There is training that supplements in-person classes with online quizzes and discussions. Some use online training or in-person group discussions as a way to build relationships between people. It is as easy to combine the worst of both modes of training as it is easy to combine the best. If you decide to create a hybrid training, be aware that there will be some who will not be able to participate in certain parts of the training, particularly if you do an in-person component to online training.

Exercise — Where Do You Train?

- Where does the majority of your library's privacy/cybersecurity training happen — in person or online?

- What would happen if your library's in-person privacy/cybersecurity training was adapted online? How would that change the content, the people who take the training, and when the training happens?

- What would happen if your library's online training was adapted to an in-person training? How would that change the content, the people who take the training, and when the training happens?

Who To Train

Train everyone who comes into contact with patron or library data. This includes working directly with data as well as working directly with patrons.

Library staff and administration both work with patrons and with patron data. So do your library volunteers. Volunteers might not be aware of the patron's right to confidentiality and privacy, including the privacy and confidentiality around patrons' questions about materials and resources, as well as their attendance at programs and events. Volunteers also get questions from patrons about other patron's checkout records, and they might even get asked for information from a law enforcement official.

Library board members and other external library governing bodies are other groups that should be considered for training since they might have access to patron data through

reports and discussions with the library. They too might be asked for patron information from others, such as a local politician who requests a list of library patrons for a campaign fundraising event.

One area that is overlooked for library privacy and security training is IT. The IT people you work with might not be in the library, but instead, campus IT or city IT. The IT workers might not be aware of the privacy policies, procedures, and practices around patron data. If any of your library's computer or network infrastructure, web applications, or any productivity software and applications are maintained by external IT departments, a conversation with key IT staff is a starting point in determining the shape and form of training for the IT department.

Exercise — Who Do You Train?

- What groups of people in your organization receive some form of library privacy/cybersecurity training? What type of training does each group receive?

- Who works with patrons or with patron data in your library? Include both internal and external workers, such as external IT departments and organizational administration.

- Take the answers from the above two questions and compare them. Which groups are working with patron data but are not included in library privacy/cybersecurity training? How could they be included in library privacy/cybersecurity training?

SECTION 1.4

THE "HOW" AND "WHAT" OF LIBRARY AND CYBERSECURITY TRAINING

Please visit Section 4 for more information about the resources referenced in this section.

It's tempting to let your privacy or cybersecurity training consist of policy readthroughs. This section will push past that temptation. Training cannot be "one size fits all." Training needs to consider the target audience and their needs. The trainer needs to set out learning objectives for the training and how these objectives will be met. While we won't have definitive answers for all of these questions for your specific situation, you will have a sense as to how to either create new training or revise existing training that meets the audience where they are.

Training Content

Before deciding what content to include in any library training, consider the following factors:

Audience — Your audience will affect what type of content you include in the training, such as the level of depth into the content and the shared level of knowledge or experiences with a particular topic. For example, you might have board members who are new to the library and are unsure how to articulate why people should care about privacy while at the same time not understanding why the library can't report on detailed demographic patron data. In this situation, you might want to start with the foundations of library privacy and introduce the board members to high-level concepts of data privacy in libraries (such as data minimization and the avoidance of collecting non-essential data to prevent harm to patrons). Library workers have more exposure to library privacy and security practices, and training sessions outside of onboarding can delve into specific issues like how to help patrons with data privacy and security questions and working with vendors particularly in contracting and auditing.

Time — The amount of content covered in a training is partially decided by how much time you have for the training session. Short training sessions can be opportunities to talk about one major topic or a small set of interconnected topics leading up to one or two conclusions, but may not allow for much time for interaction between trainers and learners. Long training sessions have more room to cover more topics and to create spaces for interaction, but carry the risk of losing learner motivation and attention if the training goes on for too long or if too many topics are covered at once without a chance to digest the content. We will cover additional time considerations in Section 1.5 on training logistics.

Format — Where the training will take place could also affect the content you choose to include. This will particularly affect the level of interactive training in certain training around digital tools. Training on specific digital tools will require access to specific equipment and software if you want learners to work with the tools in the session. Examples include access to computer labs for in-person training or providing access to the tool through the online training environment.

Training needs — If you aren't sure what your library or your audience's training needs are, there are a few ways you can solicit feedback. Surveys can gauge what topics to train on, but surveys should be supplemented with other methods, such as meeting with library staff and administration about their training needs. Coffee chats can be another option to talk one-on-one with an individual about their concerns about privacy at the library. You can also gather information from staff discussion areas, such as group email lists, discussion boards, and logs, and track any reoccurring themes and issues for possible topics.

Possible Training Topics

The most common privacy and security-related training topics are privacy and security policies and procedures. While this is appropriate for scheduled training such as onboarding new library workers and training for when policies change, you'll quickly find that this only captures a small portion of your library's training needs:

- How to teach patrons about protecting their data privacy and security
- Strategies in preserving data privacy and security when working with vendor products and services
- Specific patron concerns or considerations, such as library surveillance practices or law enforcement requests for patron or library data
- Specific privacy and security tools, such as privacy-preserving web browsers, browser plugins, and apps
- Information security best practices, such as password/passphrase management and how to identify phishing or scam emails
- How to respond to privacy or security incidents

Sections 2 and 3 cover additional training topics specific to data privacy and cybersecurity.

Learning Objectives

Learning objectives are measurable outcomes that state what learners should know or be able to do by the end of your training session. These objectives can help with prioritizing which content is covered in the training session and what content is covered in other sessions or outside training. Learning objectives provide structure to both the trainer and the learner,

providing a structure for trainers to follow and providing a means of assessment for learners to determine their progress in achieving the objectives.

Let's create some learning objectives for a library privacy training covering the policies and procedures around law enforcement requests for patron data. Some learning objectives for this library training could be "By the end of this training, library staff will be able to…":

- Identify which library policies and procedures apply to law enforcement requests for patron data
- Determine which procedures to follow based on different types of law enforcement requests
- Explain library policies and procedures to law enforcement when questioned during a request
- Understand the connection between the patron's right to privacy and library privacy and procedures around patron data requests

Each learning objective follows a particular structure:

- Begins with an active verb
- Lists one main action, be it skills, knowledge, or values, to obtain
- Aims to be measurable by the learner and trainer

EXERCISE — CREATING LEARNING OBJECTIVES

Take proposed or existing library privacy or cybersecurity training and create up to three learning objectives that start with "By the end of this training, participants will be able to…" following the structure outlined in our previous example.

1. _____

2. _____

3. _____

After creating the learning objectives, answer the following selected questions from Cornell University Center of Teaching Innovation's Learning Outcomes Review Checklist:

1. Is the learning outcome measurable? _____
    a. How can you measure the outcome? _____

_____

_____

2. Does the learning outcome use an effective, action verb that targets the desired level of performance?

3. Does the learning outcome specify appropriate conditions for performance?

4. Is the learning outcome written in terms of observable, behavioral outcomes?

Training Methods

Once you decided what topics to cover, how you will teach these topics? The teaching methods we choose affect the learner's relationship with the topic, including how they understand it and the motivation to understand it in the first place. Each method has its own set of strengths and weaknesses but you can use multiple methods in the same training to mitigate these weaknesses.

Passive And Active Learning

The two types of learning you might be most familiar with are passive learning and active learning. Passive learning allows trainers to present information in a controlled environment, such as a lecture with slides and handouts. Trainers need to prepare these materials and talking points in advance to ensure that they cover key points and concepts. While trainers

have greater control over the training session when using passive learning methods such as lecturing, there are limited opportunities for engagement outside of questions or short discussions. Passive learning can quickly turn into an information dump if there is no chance for learners to process and apply what they learned.

Some examples of passive learning methods include:

- In-person and video lectures
- Readings, including books, articles, and online posts
- Podcasts
- Recorded interviews, demonstrations

With active learning, learners can apply what they learned in the training environment and get immediate feedback from both the instructor and from their peers. This allows learners to gain experience that they can then draw on when they go back out to the field. Active learning gives learners the chance to reflect and apply what they just learned; however, it's only as effective as the most motivated learner. There can be times where no interaction happens and other times where interaction overtakes the training plan – it depends on who is in the audience, and how motivated they are to learn.

Active learning can take many forms, including:

- Hands-on demonstrations and labs
- Big and small group discussions
- Games
- Exercises
- Quizzes
- Roleplay and scenarios
- Self-reflection (journaling, self-assessment, etc.)

Trainers should incorporate both types of learning, choosing the specific methods based on the topic and learning objectives. To avoid the information dump pitfall that comes with passive learning methods in a training session, structure the training to include active learning methods between periods of passive learning, such as a group discussion after covering one or two main concepts in a lecture, or after watching a video. This can serve as a progress indicator for the trainer to determine if learners will be able to achieve the learning objectives or if the trainer needs to spend more time on a concept or topic before moving on in the training. This alternating passive-active learning structure also gives learners time to process what they learned into manageable chunks instead of waiting to the very end to apply what they learned.

Regardless of what methods the trainer chooses, each method requires careful planning and structure before the training:

- **Mapping back to training learning objectives —** Active learning methods need to be chosen with the learning objectives in mind. For example, if one of the learning objectives for privacy training is explaining and demonstrating to patrons how to navigate privacy settings when using a vendor ebook service, trainers can create an exercise where pairs of learners take turns to practice this navigation and explanation with their partner who plays the role of the patron.
- **Timing —** How much time will learners have to complete the activity? Make sure to give enough time for not only the activity but for debriefing after the completion of the activity.
- **Ground rules and guidelines —** Having ground rules for discussions can mitigate conflict and power imbalances within the training room. Some examples include the Recurse School's Social Rules and the University Corporation for Atmospheric Research's "Ground Rules + Tools: Facilitating Productive Discussions" both of which can be found in Section 4 of the handbook.
- **Resources and materials —** What resources will be available for the activity? This can range from sticky notes and pens for an in-person exercise to online tools to create quizzes and exercises.

Sometimes trainers will need to create activities from scratch, such as the creation of interactive quizzes and exercises that tie back to the training material, but other times trainers adapt activities from existing training. Trainers searching for activities from other staff-oriented library privacy training can use some of the in-person and online activities from the Data Privacy Project and the NYC Digital Safety Training. Other activities can be found in the PLP Data Privacy Best Practices Training for Libraries training from 2020 and 2021. There are additional library privacy training available at a cost from various training and professional organizations.

Trainers can incorporate activities from other sources, including training targeted toward patrons. Examples of patron privacy training that uses active learning are the Cybersecurity Training for Youth Using Minecraft Field Guide and the training materials available on the Library Freedom Project. Additional general privacy and security training activities can be found at EFF's "Security Education Companion" as well in training provided by the overall organization or local government (depending on the library).

Trainers should not limit their search for example activities to privacy or security-related training. Resources such as Liberating Structures and classroom activities found in many K-12 and college teaching resources can be adapted to library training activities.

ACTIVE LEARNING METHODS — CONSIDERATIONS

Each method has specific considerations for trainers to be aware of when choosing training activities. While not an extensive list of considerations, the following list can provide some guidance for trainers who have limited experience in training.

Discussions

Randomly assigning people to small groups and ensuring that people talk to different people instead of staying in the same small group are a few strategies to work through some of the pitfalls of group discussions. Ground rules (mentioned earlier) can mitigate group conflict and power imbalances. Small groups should not exceed five per group to provide a better chance for everyone to participate. Assigning a leader to take discussion notes and to report out to the larger group can avoid a lack of discussion when everyone comes back from small group discussions.

Games

Games can be as simple as a custom board game similar to Candyland or as involved as a pub trivia-style event or escape room. These games can be team-based to encourage cooperation between learners. Several published games in the marketplace are specific to cybersecurity and can be incorporated into training. Games will motivate folks who like competition, but be aware that some folks might get too competitive even with the simplest of games.

Question-based Discussions, Exercises, and Quizzes

Writing questions for exercises and quizzes can be deceptively simple. Sometimes questions can be too broad or narrow, or questions can be leading or loaded, steering learners into one prescribed answer or view. Use the following list from the Cornell University Center of Teaching Innovation on strategies in writing effective questions in writing questions for your training activities:

- Ask students to explain the cause of an event or why a given situation or condition has arisen. These usually begin with “Why” (open-ended question).
- Ask students to explain their reasoning for a multiple-choice answer and explain why the other answers are incorrect.
- Ask students to compare and contrast situations, cases, ideas, people, or objects.
- Ask students to explain how to do something.
- Ask students to use their reasoning to predict something.

Scenarios and Role Playing

Building scenarios can an enjoyable experience if you like creating word problems or stories; nonetheless, you will need to put some structure into their construction. What are the learning objectives, how does this tie back to the training material, and what is the main takeaway for the participants?

If you are stumped about what scenarios to create for your training, you can check shift logs and other library discussion forums for inspiration and examples of past incidents. You can also model scenarios off of incidents that happened in other libraries. If you're still not sure about what to write, or if you are not sure about your writing skills, several training resources use scenarios that you can study and adapt for your training.

Your scenario framework will differ depending on how you plan to use scenarios. Creating a scenario for word exercises will differ from creating a scenario where in-person participants assume a role. While assigning roles for in-person scenarios, one option is to assign one or two group members to be observers of the scenario, taking notes. Creating material for the scenario includes the base text for everyone to read, specific text based on role, accompanying materials, and debriefing questions at the end for each group to discuss after they reached the time limit.

You can also bring the debriefing session one level higher by having an open discussion for the entire training class. Groups can then learn from each other and cover points or issues that other groups didn't consider.

Context And Reinforcement — A Short Case Study

You might have heard about people at other workplaces receiving questionable emails, only to find out that these were sent as a test to find out how many employees can spot phishing emails and other scams. These simulated tests seem like a good idea because they can identify if there is a need for additional training; however, these tests can spectacularly backfire. Here is a real-world example — a library employee who is advocating for library workers to get the COVID-19 vaccine receives a phishing email about available vaccine appointments, only to find out that their library sent out the phishing test. If there's one way to make your workers distrust IT or management, this example is most likely it.

The main takeaway from these stories of phishing tests gone wrong and other types of simulated tests:

- **Context and methods matter —** Simulated tests can be effective, but the test's logistics — including timing and content — can work against training outcomes. Trainers should also consider the current state of the organization, such as staff morale and major events in the organization, in developing and teaching privacy training. Another thing to consider is the effectiveness of training methods, including how often training has to be repeated to mitigate evolving privacy risks.
- **Positive reinforcement over negative —** Negative reinforcement can demotivate people to report suspicious emails or other possible security or privacy issues when they experienced punitive actions for past mistakes. Positive reinforcement, such as awarding staff members who do not click on the test phish email, can help with creating a more security-conscious organization.

Training Room Strategies And Issues

Many trainers find themselves teaching training because they are the most knowledgeable person in the library about data privacy or security. Some trainers might not have extensive experience in training or teaching in an in-person or online format. This section is a starting point for trainers who want additional support in handling common training session issues and developing teaching skills.

Practicing And Learning From Others

The best way to develop teaching skills and strategies to handle common training issues is through practice. This practice can come in the form of conducting more training, but it can be supplemented by learning from more experienced trainers or teachers in the organization. Trainers can learn from more experienced colleagues in several ways:

- Observe a training conducted by the experienced trainer and take notes about what went well and how you can incorporate that into your training
- Ask the experienced trainer to observe one of your training sessions and provide feedback on what went well and what can be improved
- Ask for feedback on draft training materials, including slides, handouts, and activity plans
- Set up a regularly scheduled time to talk about teaching and training methods and issues — this can start with a meeting between you and the experienced trainer but can be xpanded to others in the organization who want to create a community of practice around training pedagogy
- Schedule a practice training session where you and the experienced trainer can critique and tweak the training before teaching in front of learners

Trainers can also learn from pedagogical resources and courses for school teachers and college instructors. Several higher education institutions have centers for teaching that have information about strategies for in-person and online teaching, as well as information about active learning methods. Trainers might also find materials around facilitation helpful for conducting in-training discussions and other activities. You can find some examples of these resources at the end of the handbook.

When Things Don't Go As Planned

Trainers can create detailed training plans, but sometimes the training doesn't go as planned. Sometimes trainers can recover from these deviations from the plan. For example, if the training comes to the point where learners are discussing everything except what you hoped they would learn from the training, that doesn't necessarily mean that the training failed. It went in a direction that your learning objectives didn't plan for. You can bring up some of the

uncovered topics through open questions to the learners. This is also an opportunity to learn from observations and discussion to revise the learning objectives or the training materials for future training.

Trainers might have a session where no one is participating in training activities or discussion. Restructuring discussion questions and activity plans can address some of these issues, such as breaking learners into smaller groups for the first part of the discussion or activity. Be aware that sometimes the silence that comes after asking a question does not necessarily mean that no one will answer. Learners need time to process and reflect on the question and what they just learned in the training. Resist the temptation to fill that silence. If the silence continues beyond a few moments, ask open follow-up or related questions that shift the level of reference, context, or angle to the original question.

Sometimes the conflict between learners can derail training. Setting guidelines and ground rules at the start of the session can mitigate the chances of conflict, but a gentle reminder is sometimes needed. Address the problematic issues at the moment through the gentle reminder about what is and is not allowed according to the ground rules. Sometimes the conflict continues, in which at that time a trainer might need to call a “time-out” to re-assert the ground rules to the training room.

SECTION 1.5

LIBRARY PRIVACY AND CYBERSECURITY TRAINING LOGISTICS

The previous sections covered the who, when, where, what, and how of training. This section covers the practical logistics of training that sometimes are left out of training outlines and plans until the last stages of planning. Incorporating logistics throughout the training planning process will address common issues trainers encounter, such as equipment and scheduling issues. Logistics also shape the training in terms of class size and the amount and type of activities included in the training plan and the type of assessment processes to obtain feedback for future training sessions.

Scheduling And Timing

Timing is a perennial issue with scheduling in-person and synchronous online training. Scheduling training is a juggling act with the trainer navigating through people's availability, particularly for longer training or training that takes place during busy periods. For incident-based or "one-off" type training, offering repeating sessions at different times of the day provides more options for staff who work different hours or shifts that make it difficult to attend the first training date. Regular training, such as onboarding training or privacy refresher training, can avoid some of the scheduling issues through having dedicated training times. The frequency of these scheduled training will depend on the size of the library and the rate of onboarding — it might make more sense to train new employees or volunteers as soon as possible if there are only a few starting hires every few weeks or months, but libraries who hire a constant stream of workers or volunteers might find it more efficient to have a privacy and security orientation training every month or couple of weeks. Asynchronous training avoids scheduling issues on the trainer's side, but library workers will still need dedicated time in their workday to complete the training.

The training schedule itself is as important as when the training is scheduled. Trainers new to the training world might find themselves going over their allotted time, or find that learners run out of motivation or energy after hitting a particular point in the training. Here are some considerations for the training schedule:

- **Length of training —** in-person training can be as short as a few minutes and as long as multiple days. While longer training means that the trainer can cover more material, it can also lead to learner burnout if there are little to no time for breaks, activities, and reflective/self-

assessment time. The nature of online synchronous training accelerates learner attention span burnout. Synchronous online training should be limited to 90 minutes, with scheduled breaks if going longer than 60 minutes. Trainers recording lectures for asynchronous online training should aim for lecture videos no longer than 10 or 12 minutes to avoid similar learner attention span issues as in-person and synchronous online training.

- **Cushion time —** Trainers sometimes create content for the full training time, but end up running over due to the training sessions not starting at the posted start time or the need to make unplanned follow-up announcements at the end of the session. Trainers should leave cushion time at the beginning and end of their training schedule (around five minutes each) to accommodate any delays or announcements at the beginning and end of the training session.
- **Evaluations and feedback forms (in-person training) —** Trainers should provide time for learners to fill out evaluation forms at the end of an in-person training session for the greatest chance of a high feedback response rate.
- **Introductions —** Similar to cushion time, trainers who create content for the full training time might go off schedule when group introductions take longer than expected. If trainers plan to have learners introduce themselves in an in-person training, creating a small ice-breaker exercise — such as asking learners for their name, their work title, and one "what is your favorite_____" question (example: non-alcoholic drink) — can keep the introductions part of the training on schedule. Online training can have learners introduce themselves in advance if there is a place dedicated to training discussions.
- **Housekeeping —** This time at the beginning of the training should be used to go over the training schedule, ground rules, and other logistics learners need to know, such as where the restrooms are for learners who had to travel to a different location for the in-person training or where to ask questions in an online training platform.
- **Breaks —** Trainers are strongly encouraged to incorporate breaks into synchronous training sessions. The length of the break depends on the location; online training breaks can be a short as five minutes while in-person training non-meal breaks can be as long as 15 minutes for people to use the restroom, get something to eat or drink, spend time outside the training room, and so on.

Training Class Size And Space

Trainers will quickly find themselves overwhelmed if the in-person training session is overcrowded and the trainer is the only one facilitating the entire training session. In-person training class sizes can vary depending on the structure and content of the training. A training that is a mix between lecture and discussion can accommodate more learners in one session than a hands-on workshop that requires special equipment. The number of learners in an in-person session also depends on

the number of trainers and assistants in the session. Hands-on sessions or in-person training with intensive technology-related activities should consider enlisting one or two training assistants to help learners with the labs or activities. Online synchronous training sessions encounter similar issues of overcrowding in activity-intensive training if there are no training assistants in addition to the trainer.

The training space also determines how many learners are in one training session. Online training needs to be aware of license restrictions on the number of users in an application or web conferencing space. In-person training needs to ensure that the training room can adequately accommodate the expected number of learners for the session, including making sure that there is enough special equipment for learners such as computers.

One aspect of training logistics that is sometimes left out of space considerations is accessibility. The choices in online and in-person training spaces have the potential to exclude learners from training. Online training spaces should meet, at minimum, the Web Content Accessibility Guidelines (WCAG) version 2.2 at the time of publication of this handbook. In-person training spaces need to consider the accessibility of the space, as well as how accessible it is to get to and from that space. Training must also consider captioning for lectures and discussions. Trainers can learn more about planning for more accessible in-person training by contacting organizational staff responsible for accessibility at their organization, as well as reading more about accessible meeting requirements such as https://accessibility.cornell.edu/event-planning/accessible-meeting-and-event-checklist/ and other resources in Section 4.

Equipment And Materials

Equipment and material choices will depend on the type of training and where the training takes place. Training materials for learners can include:

- Slide outlines and transcript
- Exercise workbooks
- Resource or reading lists
- Training handbooks
- Additional resources or publications from outside sources

Training activities will need additional materials, ranging from activity instruction worksheets to props and game materials for training games or exercises. Sticky notes, poster paper, pens, and markers are also material to provide to learners for in-person discussion group note-taking.

Equipment needs for in-person training can include:

- Laptop or desktop computer
- Projector
- Microphones — wireless if possible so the mic can easily be passed around the training room
  - Even if the training space is small, everyone — the trainer and the learners — must use the mic. Using the mic is about accessibility for all in the room, not about the person speaking at the time.

- Speakers, for both microphones and the computer (if the trainer needs sound for a video or other multimedia file)
- Whiteboard or poster paper and easel with markers

Online training equipment follows a similar needs list for both learner and trainer:

- Computer with the required web conferencing or broadcasting software installed
- Headset with microphone
- Webcam — while the trainer should appear on video sometime during the online training, learners should have the option to turn the web camera off during the training to avoid internet connectivity issues.

Trainers who are interested in creating more polished training videos or an upgraded physical web conferencing space can read more about lighting, equipment, and space arrangements from remote teaching sites like https://teachremotely.harvard.edu/video-and-audio or general advice sites around video conferencing or livestreaming listed in Section 4.

Training Tools And Applications

PowerPoint, Keynote, or other presentation slide software tend to be the go-to for trainers; however, there are a variety of other tools and applications trainers can use for training sessions and activities, particularly online training. Some tools and applications include:

- Learning management systems, such as Moodle
- Screen and video recording software, such as Camtasia
- Web conferencing software, such as Zoom
- Online discussion and workgroup apps, such as Microsoft Teams
- Online collaboration tools, such as Microsoft 365 and Google Workspace
- Various apps for creating forms, quizzes, exercises, and other interactive activities

Trainers might already have access to specific tools and applications through their workplace and trainers are encouraged to make use of existing resources. Before use, talk to the appropriate staff to assess if there are license restrictions on use, particularly the number of concurrent users for a training session. Trainers are also highly encouraged to assess the privacy policies of third-party applications for problematic data privacy or security management practices, including problematic vendor privacy practices highlighted in the PLP *Library Privacy and Vendor Management* 2020 training.

Feedback And Assessment

Trainers need feedback to assess the effectiveness of the training and if the training met the needs of the learners. The learning objectives created during the planning process are one measurement to use in gathering feedback from learners, usually edited into "I" statements and placed on a Likert scale. Other aspects of the training (length of training, training space,

materials, tools, activities) and training goals beyond the learning objectives can also be measured for effectiveness with a Likert scale or another rating system.

Another measurement is the use of free text fields for learners to expand on their thoughts of the training, including:

- What actions they will take in their daily work based on what they learned in training
- What went well in the training
- What could be improved, or done differently
- What topics they wish to cover in future training

Trainers should collect the least amount of identifiable data possible from learner feedback forms, particularly if there are outliers in the training group, such as only one person from a particular department attending a training. Tying names or identifiable demographic or work information to feedback forms will limit honest feedback on a training session.

Some organizations have generic training assessment forms that collect data for all types of training in an organization. Trainers should work with the organizational assessment staff to customize the form if desired. If the generic form requires identifiable information to be attached to the feedback, discuss with organizational staff about possible ways the assessment form can be modified to not collect identifiable data that is not needed for critical organizational reporting needs.

Trainers do not have to limit themselves to feedback forms for assessment. Other assessment options include observations of training sessions and review of training material by peer trainers or others with training or teaching experience.

SECTION 1.6

SUPPORTING LEARNERS OUTSIDE THE TRAINING ROOM

It is impossible to teach everything there is about library privacy or cybersecurity in a single training session. Training is limited by time, resources, and staff availability. Trainers need to prioritize which topics are covered in particular training, resulting in leaving out topics that otherwise would be covered if there were more time or resources for more training. In addition, the topics covered in training will need to be reinforced and updated with the latest developments or changes in privacy practices, but again, reinforcement and update training sessions are limited by organizational constraints.

Trainers are not limited to the training room when it comes to raising awareness and teaching library workers about library privacy and security. This section contains several ideas in providing spaces and professional development opportunities for learning about library privacy and security topics and updates.

Communities Of Practice And Communities Of Interest

Communities of Practice (CoP) provide a space where library workers can come together discuss how they practice privacy or security in their library work. The main focus of the CoP is to provide peer support and knowledge to others with implementing data privacy or security concepts in their daily duties. Members have the chance to contribute and shape the CoP, such as how the group meets and organizes activities within the library. This includes the relationship between the CoP and the more formal data privacy or security management structures at the library. The members of the CoP have experience that can be used to revise or address potential risks in library operations. The CoP can provide informal training or workshop opportunities around specific topics and tools outside of more structured training environments. Library workers primarily interested in learning or discussing about library privacy/cybersecurity in general might be better suited for communities of interest.

Communities of Interest (CoI) focus on bringing together people who are interested in a particular topic. Library privacy and security CoI spaces include both practitioners and those who are interested in the topics in general. The types of topics in a library privacy CoI could range from privacy or security news and regulations to issues around privacy and equity — it depends on what the members of the CoI bring to the group's attention, as well as the interest level of the group to discuss particular topics. A typical library has several

spaces in which a CoI can flourish, such as an internal discussion board or group email list. The CoI might also hold informal in-person or online discussion sessions on a particular topic of interest to others in the library.

Both CoP and CoI offer a space for library workers who respond well to the motivation and accountability that a group of like-minded individuals provides. The community members will need to provide some structure and facilitation of their groups, which requires member motivation and time. This might mean that some communities will become dormant if there is little motivation or available resources to keep the group active. Some libraries might have their CoP and CoI merge into one overall community if the individual groups have a heavy overlap in membership or if one group becomes dormant.

Documentation And Knowledge Bases

Training library workers on policies and procedures needs to be accompanied by written documentation. Without documentation, library workers have to rely on tacit knowledge from others or try to remember what was taught in a training. Neither situation is ideal for library workers or patrons alike; that is why privacy and security policies, procedures, and practices should be documented and readily accessible to library workers for consistent implementation outside the training room.

Documentation and other information about library privacy and security should be accessible to all library workers through a centralized knowledge base (KB). A KB manages and organizes an organization's knowledge assets through intranets, internal wikis, and other internal areas for retrieving and accessing organizational knowledge. Trainers can post training modules, materials, and additional readings or resources related to the training alongside policies and procedures or other privacy-related library documentation or practices in the KB.

Documentation and KBs are only as reliable as the oldest document or knowledge asset. Any documentation or resources posted will need regular updating and review to ensure that the information provided is not out of date or otherwise does not reflect current organizational policies, procedures, or practices. One thing to be aware of is if there is a culture or practice of printing out documentation and training materials among library workers. Clearly dating the documents or materials with the date of creation or revision mitigates some of the confusion if someone is referring to a different version of the document than others in a work discussion. Any notices sent to library workers about updates to any privacy policy and procedure documents could also include a reminder to workers to replace printed versions of the document with the latest version.

Professional Development

Trainers and library workers both benefit from professional development resources and opportunities. The rapid pace of change in privacy and security regulations, practices,

and risks in libraries makes it all that more important to provide ways to keep up to date. Trainers can create a clearinghouse in an intranet site page or another section in the KB that contains a list of library privacy and other privacy-related training, classes, presentations, interest groups, and websites. The CoP and CoI mentioned earlier in this section can also provide professional development opportunities in tandem with the clearinghouse. In addition, all library workers can contribute to the clearinghouse by adding any resources or materials gathered from external training, presentations, or classes they attended.

Section 7 of the 2020 Toolkit provides several professional development opportunities, including training and websites tracking the latest developments in library privacy as well as the privacy field in general.

SECTION 2

Data Privacy Training

SECTION 2

DATA AND PRIVACY

What We Mean By "Data" And "Privacy"

Talking about library data privacy can take a variety of forms, depending on the context of the conversation. All of us have varying definitions, knowledge, and experiences with data privacy in our personal and professional lives. This section briefly explores some of the concepts behind data privacy in libraries, and how trainers can navigate different approaches to data privacy to create a baseline to ensure that everyone in and outside the training room is on the same page in library data privacy conversations.

Privacy

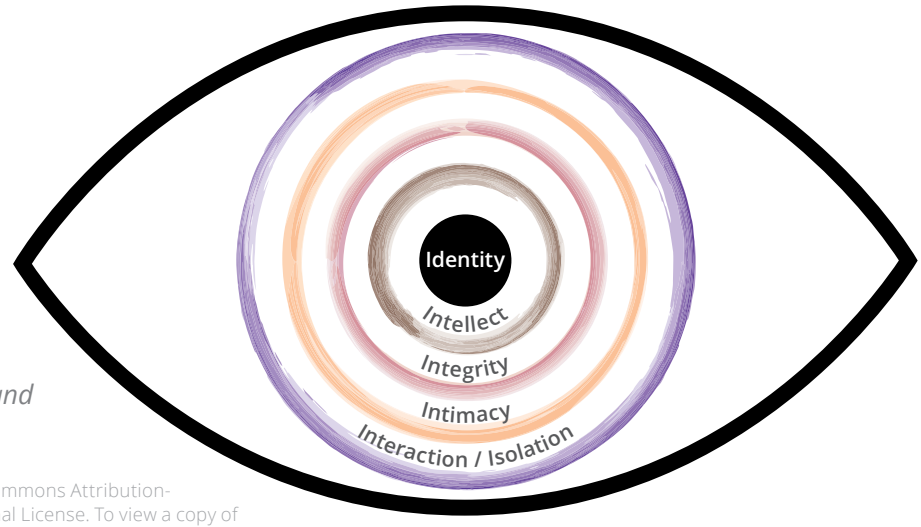
We might have different definitions for privacy if we're asked to define the term for ourselves and in our professional work. You can break privacy down into different types:

- *Bodily privacy* refers to genetic information and certain actions or choices that the person makes about their physical body.
- *Information privacy* refers to personal data, such as financial and medical records.
- *Communication privacy* differs from information privacy in that the former pertains to all forms of correspondence, including mail, phone and video calls, and email.
- *Territorial privacy* refers to a person's environment, be it at home, work, or another space.

We all might have these types of privacy in our definition, but these definitions might change based on the context of the question or the setting in which the question is asked. In addition, breaking down privacy into categories reveals not only the complexity of privacy but also the interconnectedness between categories. Libraries primarily work in *information privacy* but what we do affect other privacy categories:

- A person's *territorial privacy* in the physical library space
- Using library public computers to send correspondence *(communication privacy)*
- Search and circulation history containing information about a person's physical body in the form of medical research or health resources *(bodily privacy)*

You can use these definitions as a starting point when discussing privacy with others. Another approach that takes the different types into account is the Six Private I's framework created by Sarah Hartman-Caverly and Alexandria Chisholm. This conceptual framework represents the various layers or zones in which privacy protects: identity, intellect, bodily/contextual integrity, intimacy, and interaction and isolation.



*The **Six Private I's** framework created by Sarah Hartman-Caverly and Alexandria Chisholm represents the various layers or zones in which privacy protects: identity, intellect, bodily/ contextual integrity, intimacy, and interaction and isolation.*

People's definition of privacy is also shaped by the legal system through legal opinions, regulations, and case law:

- Legal review articles influence how the US defines privacy. One of the greatest influencers of US privacy regulations, "The Right To Privacy" (published in 1890 in the *Harvard Law Review*), states that individuals have "the right to be let alone."
- The interpretation of the Fourth Amendment in cases plays a pivotal role in privacy. An example of this that influenced privacy in both general and library spaces is Katz v. United States in 1967. The Supreme Court expanded the amendment's protections in their ruling, stating that the amendment grants people a reasonable expectation of privacy even in public spaces.

Lastly, sometimes people use "privacy," "security," and "confidentiality" interchangeably. While there is some overlap between the three terms, ultimately these terms mean different things:

- *Confidentiality* refers to a party trusted with personal or sensitive information refraining from disclosing this information to unauthorized third parties.
- *Privacy* refers to the right from intrusion from any party, even trusted ones.
- *Security* is the protection of assets, including data.

Security can tell you how to protect the data, but *privacy* will ask you if this data should be collected and retained in the first place.

Data

The definition of data can also confuse people depending on the context of the term's use. We'll start with the definition of "data" from Merriam Webster, where data is one of these three things:

1. Factual information
2. Digital form of information
3. Information output that has to be processed before it can become meaningful

This definition, however, does not capture the reality of data. Data is not an unrefined resource to be processed into meaningful information. We create data in our everyday life, from using our smart devices at home to the various tools we use for our work. We also create data when we shop, when we travel, and when we browse online. Some of this data is needed for operational purposes — the credit card company needs information to process the payment, for example. However, a lot of the data we generate is *data exhaust.* This exhaust trail of data reveals who we are in terms of our behaviors, interests, and habits. The data could be collected and used by third parties without prior consent or awareness from the people generating that data. It's very hard to separate the person from the data they generate. Even when we talk about the aggregation of data, or when we describe data through metadata, we can still get a relatively accurate picture of the person generating the data.

In summary — When we talk about data privacy, we are not only talking about informational privacy but ourselves as a whole. Our approach to data privacy needs to reflect that we are the data that we create.

Privacy In Libraries — Resources For Training Topics

It is nearly impossible for a library to not collect and use patron data. Your library's integrated library system is the main database for patron data — like name, address, age — but other systems collect and store patron data, such as your catalogs, discovery layers, and digital resources. Your physical environment also collects patron data, such as copiers, public computers, and devices that circulate, such as hot spots and laptops.

Some of this data is needed for library operations — for example, a record of who currently checked out a library resource. Other data is not essential for operations, such as keeping a record of individual patrons who accessed an electronic resource during a specific span of time. This creates a tension between the need for data (operations, assessment, evaluation, and justification of library operations) and respecting patron privacy.

Because libraries collect and use patron data in many ways, it can be difficult to determine what library data privacy basics, issues, and considerations should be included in privacy training beyond the privacy policy. Trainers can use the strategies outlined in the first section of the handbook as well as the information covered in the 2020 Toolkit to identify possible privacy training topics. Trainers are encouraged to review the 2021 Train-the-Trainer webinar series materials for additional ideas.

For trainers who might need additional guidance or structure in planning and conducting privacy training, the 2020 privacy training series can be modified and adapted for the trainer's needs. Section 7 of the 2020 Toolkit also contains example privacy training targeted toward library workers that can be adapted for other libraries.

This page intentionally left blank

SECTION 3

Cybersecurity Training

SECTION 3.1

SECURITY AWARENESS TRAINING

The ultimate end goal of security training is to make your library Defensible & Resilient. Defensible does not mean secure — it means you are making your library able to be defended. There are more things to defend than there are resources to defend with. Defensibility focuses on what, why, how, when and from whom. Making your staff aware of security and making your library defensible means considerable work. It means a lot of hard, detailed work. Our work on training means a change in mindset through increased awareness of threats and an admission of inconvenience. Closely related to defensibility is Cyber Resilience. Being resilient means your library will have an ability to keep operating when bad things happen to your IT. It means the ability to withstand all types of cyber events. In the end, we want to have trained people, following safe practices, using solid technology.

Base Your Training On Solid Policies And Procedures

Security and security awareness training depends on well documented policies and procedures. It's important to have detailed, solid documentation. This will build a solid foundation four improving security culture at your library. The policies and procedures are useful as evidence of compliance, training, and general support of day-to-day safe and secure operations. Make sure the policies are available for review and use for anyone who wants to take a look. As much as possible these documents should be front and center for everyone. The policies and procedures should be par of all your trainings. What we want is policies that reinforce good security principles that will foster over time a new instinct in people, a new way of looking at things, a new way of acting in a more secure way. Your policies are only as good as the least aware employee. Last, and not least, schedule time to update them regularly.

Keep It Fresh

This probably goes without saying for any type of ongoing, regular training. To keep users interested in what you're trying to teach them, they can't be expected to sit through the same material more than once or twice at the most. Though the topics will be the same, the details and examples need to change each time. When you recycle old material and using a long, boring, annual course you'll end up just teaching them your library is just apathetic about security.

Keep It Short

We're all busy and if we expect everyone to set time aside from daily responsibilities to complete their awareness training, we need to respect their time and make it short and interesting. We don't need to make everyone an expert, but we need to make sure they know what to do when things go wrong.

Make It Focused

Library employees all perform different tasks and that means they face some different threats. That means we can't train them all on the same types of risks. Tailor your training based on age, role, department, groups and anything else that might change their risk profile.

Make It Happen Regularly

Security awareness training needs to be done more than just once a year. One annual training is probably not enough to see any real improvement in awareness. Our ability to identify threats fades over time, so libraries who conduct trainings only once a year will rarely see positive user behavior changes.

Don't Shame Failures

Training should always be an experience that helps employees learn without feeling bad. And if mistakes are made after training, use them as an opportunity to help workers understand. We all make mistakes, and it's important that people report their mistakes, not try to hide them.

Never Without the "Why"

Why are we doing this training? Employees should not only understand the attack vectors they face, but why security is so essential to a business. The goal is to make doing things the right way become the default in your library. If everyone knows all about the "why" they will be more likely to accept changes and inconviece that comes with making things more secure. One of the most important things they need to know is why we're a target. We (libraries) are targets because we can be large (ish) and complex (ish) and we are hard to defend, and we are often part of larger organizations, (city/county, campus). Those larger targets could have much more value than what we have in the library.

Let Them Know How Important They Are

End users are much more than just a security liability. Let them know how important they are in defending the company from attacks and breaches. Focus on getting everyone — from employees to executives — to believe in your efforts. If everyone isn't convinced of the importance of awareness, few people are going to support your mission.

Make It Entertaining

Make at least part of the training a game. Ask everyone to "think like a bad guy" and show them safe ways to attack the library, or maybe attempt to phish another employee. Challanging them in a controlled and safe manner will help them better understand the types of attacks they will see.

Onboard Employees Along With Training

New employees go through many different types of training when they are hired, make sure security awareness is part of that.

Mix It Up

Along with regular short training, try different training mediums as well. Use short videos, industry articles, emails, Microsoft Teams messages, Slack and whatever else your library uses to keep in touch. Making the training modules short digestible and educational. It may be possible to expand the program to include SMS messages by using contact center technologies, knowledge bases, and artificial intelligence to be faster and more targeted with the information.

Find Security Champions

Find enthusiastic employees who will help the security team evangelize security's message. Large library have fire drills and "fire marshals" and it's a good idea to have "security marshals." The marshalls are the knowledgable people who can work as contacts to help their team mates to ensure quicker response.

Train Up The Chain Of Command

All the way up. Your bosses, the director(s) and even the board. Is your boss/director/board/dean/whatever aware of IT Security? If they were, would that help make the library more secure? They (board/boss/whatever) all need to know about your training and technology. When it comes to technology, they should be away there's other costs attached to new technology that will need to happen in order to keep things secure. Make sure everyone understands that we are all targets. If they ask "How secure are we? What's this going to cost?" the answer will most likely scare them. It may be up to you to help everyone, top to bottom, at your library become Security Literate.

Remember What This All Means To Others

It is important to remember that security can mean barriers to getting work done. Security can get in the way for patrons & mean extra work and trouble for administrators. At the same time, it's critical. So it's important for us to remember what others think. We need to keep in mind how security affects our patrons and work environment.

Ask Them How You Did

So what did employees think of the training? If you don't ask, you're missing an important part of awareness.

SECTION 3.2

THREAT MODELING

There's something called "Threat Modeling" in IT Security. Think of it as just taking a step back and looking at the big picture. It doesn't necessarily take an expert, but it takes time, and patience and some training. In libraries, it helps us align our limited resources, work, money, defenses with the threats that pose the greatest risk. That is, those threats that are the most likely to occur and those that could be the hardest to recover from.

Our risks need ranking and working through some Threat Modeling lets us do that. Sure, we need to lower all risks, but all risks aren't equal. We want to know what our biggest threats are. Those that are likely to be attacked and those that are easy to be exploited. What's most valuable and hardest to recover from. We need to make sure we know what's around and how it can be exploited.

Where Do We Focus?

Where do we even start? It's probably not easy, and looks overwhelming. We need to find ALL the things to defend and decide how to best defend them. Then, take a look at what we have and rank them. All those things on your list are not equal. Start with the highest risks. The things most easily exploited. The most valuable things.

We have limited time/people/money, and we need to have priorities because there is SO much to worry about, so we need to know our threats RANKED and how we're going to defend them. We want to make sure we're able to focus what we have in the right place, and that's what this is about. Going from overwhelmed, to a starting point, a place to focus. All the many threats we face are not equally dangerous, and our defenses are not all equal. A good starting point is knowing what's been hit before and what caused that breach/exploit/hack (Patches, social engineering, passwords, misconfiguration).

How Do We Rank All These Things?

What do we have to protect?

Everything with an IP needs some type of protection, though everything with an IP address isn't necessarity equal. Considerations:

- How likely is each thing to be attacked?
- Has it been attacked before?
- Is it a commonly found in other places?
- Is it easy to run common tools to test for exploits?
- How easy is this thing to find/exploit?
- Does it contain valuable patron or library data that can be sold?
- Has it ALREADY been exploited in this OR another library?
- Can people touch this thing?

Chances are good your library's IT team has a tight budget and the general chaos of 2020 probably even moved security

to a lower priority as work-from-home arrangements quickly became top priority. Libraries large and small are just as at risk from cyber security threats as large businesses and other businesses. Your library is NOT too small to be a target. As attackers have increasingly automated their attacks, it's very easy for them to target thousands of places at once. Libraries can often have smaller budgets, less stringent technological defenses, less awareness of threats and less time and resource to put into cybersecurity. This makes our libraries an easier target for automated attackers to find a way in. The largest threats to libraries right now are ransomware and business email compromise. A well trained group of employees at your library will reduce the chances of these attacks succeeding.

Phishing

So many common threats to libraries now start with email. There is even a dedicated hacker group known as "Silent Librarian" known to be actively targeting academic libraries.

A recent study by the Association for Computing Machinery (https://dl.acm.org/doi/10.1145/3415231) asked experts how they deal with email. They found an expert will examine an email by first trying to make sense of the email, and understand how it relates to other things in their life. As they do this, they notice discrepancies: little things that are "off" about the email. As the recipient notices more discrepancies, they feel a need for an alternative explanation for the email. At some point, some feature of the email — usually, the presence of a link requesting an action — triggers them to recognize that phishing is a possible alternative explanation. At this point, they become suspicious (stage two) and investigate the email by looking for technical details that can conclusively identify the email as phishing. Once they find such information, then they move to stage three and deal with the email by deleting it or reporting it. Training employees to be suscipiscous and carefully examine all email is critical. It may also be useful to send test phishing email to employees as training.

Technical defenses that are very effective include powerful spam filters, disabling Microsoft Office Macros, and using a second factor of authentication.

Business Email Compromise

Phishing attacks, and Business Email Compromise (BEC) in particular are extremely dangerou. They've become very sophisticated in recent years, with talented and dangerous attackers becoming more convincing in pretending to be legitimate business contacts. In particular, Business Email Compromise is on the rise. This type of attack involves bad actors using phishing campaigns to steal business email account passwords from high level executives, and then using these accounts to fraudulently request payments from employees. Part of what makes phishing attacks so damaging is that they're very difficult to combat without proper training. The attackers are talented social engineers and target employees within your library, rather than targeting technological weaknesses. There are indeed technological defenses against phishing and BEC attacks, but the first line of defense is training.

Ransomware And Extortionware

Securing Computers Against Ransomware And Extortionware

Limit Users — Least Privilege / Zero Trust: This simply means that all user accounts should run with as few privileges as possible, and also launch applications with as few privileges as possible. Everything on your network should be an untrusted device, and be treated as such.

Updates / Patches: All devices need to be kept current and set to update automatically if possible. Without updates the bad guys will exploit vulnerabilities in your operating system, browser, app, antivirus tool or other software program with the help of an exploit kit. These kits make it easy to quickly find a way in with out much training or skill. The easy to use kits contain exploit code for known vulnerabilities that enable them to drop ransomware and other malicious payloads. Make sure that your updates are done on all of your connected software and hardware.

Check Your Settings: Along with updates, making sure your apps and operating system are configured correctly make your IT much more secure. The biggest and easiest wins include disabling Remote Desktop Protocol (RDP), PowerShell, and Microsoft Office macros.

Harden & Segment your networks: Network segmentation is another solid mitigation against ransomware, and other types of cybersecurity threats. In a properly segmented network, groups of end devices like servers and workstations have only the connectivity required for similar types of use. This limits the ability of ransomware to spread or an attacker to pivot from system to system.

Canaries: Canaries can be hardware or software and can detect suspicious activity in a network. They can be used throughout your network on computers, servers, and even phones. Anytime a canary is accessed an alert is sent, letting you know someone has accessed a resource that should be off limits.

Protective DNS — PDNS is a security service that uses existing DNS protocols and architecture to analyze DNS queries and mitigate threats. Its core capability is leveraging various open source, commercial, and governmental threat feeds to categorize domain information and block queries to identified malicious domains. This provides defenses in various points of the network exploitation lifecycle, addressing phishing, malware distribution, command and control, domain generation algorithms, and content filtering. PDNS can log and save suspicious queries and provide a blocked response, delaying or preventing malicious actions — such as ransomware locking victim files — while enabling an organization to investigate using those logged DNS queries. OpenDNS, Cloudflare, Google Public DNS, Comodo Secure DNS, Quad9, 7Verisign DNS.

SECTION 3.3

OTHER GENERAL RECOMMENDATIONS

Multi-factor Authentication

Multi-factor authentication (MFA or 2FA) is an additional authentication step that requires a separate additional token to be entered in addition to a password. You're able to reach your intended destination only after successfully presenting a password and a second factor, like a number. Forcing use of a second factor means that even if someone knows your password, they will not be able to login to the service. This is especially important to have on your email.

Backups

Whatever backup solution you choose, copies of backups should be stored in a different location. Send them to cloud object-based storage that can't be changed. The idea is to get your backups—or at least one copy of your backups—as many hops away from an infected Windows system as they can be. Put them in a provider's cloud protected by firewall rules, use a different operating system for your backup servers, and write your backups to a different kind of storage (immutable backup). If your backup system is writing backups to disk, do your best to make sure they are not accessible via a standard file-system directory. For example, the worst possible place to put your backup data is E:\backups. Ransomware products specifically target directories with names like that and will encrypt your backups.

Passwords

We all have been frustrated by passwords. It is important to have a strong unique password for every single account we have. That makes it impossible to remember all our passwords without using a password manager. Moving your library to password manager will go a long way to making all your services more secure.

Security Exercises

"It's Gone"

Pick a system, any system. Think of a reason why it's completely done — failure of the entire RAID array, fire in the datacenter, hacked, lost, human mistake — and see how you're library is able to function without it.

"Stowaway"

Connect an unauthorized network device into your network and let it talk to something. Practice hunting it down and how to find anything on the network that shouldn't be there.

"Evil Mailman"

A system that should never send mail starts sending mail. How do you spot and stop the spam?

"Evil Librarian"

Choose an employee, pretend he or she has been fired, and revoke all of his or her privileges. Are they still able to access anything in the library?

"Evil Patron"

You walk into your library as a patron with a Kali Linux laptop. Start exploring...

SECTION 4

Training Resources

SECTION 4.0

RESOURCES

Additional Train-The-Trainer Manuals

This handbook highlights several strategies and examples of training preparation and teaching, but trainers are not limited to the strategies covered in this handbook. Trainers might find the following trainer manuals of interest if they want to explore additional planning and teaching strategies.

Cserti, Robert. 2018. "Train the Trainer Course - A Complete Design Guide (With Examples)." *SessionLab.* https://www.sessionlab.com/blog/train-the-trainer/.

ENISA. "Good Practice Guide on Training Methodologies." https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies.

Partners in Health. 2011. "Training of Trainers." https://www.pih.org/sites/default/files/2017-07/TrainingOfTrainers_English.pdf.

University of Kansas. "Developing Training Programs for Staff." Community Toolbox. https://ctb.ku.edu/en/table-of-contents/structure/hiring-and-training/training-programs/main.

Active Learning Methods

Center for Educational Innovation. "Active Learning." University of Minnesota. https://cei.umn.edu/active-learning.

Center for Teaching Innovation. "Active Learning." Cornell University. https://teaching.cornell.edu/teaching-resources/engaging-students/active-learning.

"Liberating Structures." https://www.liberatingstructures.com/.

Learning Objectives

Center for Teaching Innovation. "Setting Learning Outcomes." Cornell University. https://teaching.cornell.edu/teaching-resources/designing-your-course/setting-learning-outcomes.

Eberly Center. "Learning Objectives." Carnegie Mellon University. https://www.cmu.edu/teaching/designteach/design/learningobjectives.html.

Ground Rules And Guideline Examples

"Ground Rules + Tools." University Corporation for Atmospheric Research. https://www.ucar.edu/who-we-are/diversity-inclusion/community-resources/ground-rules-tools.

"Social Rules." Recurse Center. https://www.recurse.com/social-rules.

Training Accessibility

"Accessible Meeting and Event Checklist." Cornell University. https://accessibility.cornell.edu/event-planning/accessible-meeting-and-event-checklist/.

"Accessible Syllabus." https://www.accessiblesyllabus.com/.

Leary, Alaina. 2020. "How to Make Your Virtual Meetings and Events Accessible to the Disability Community." *Rooted in Rights.* https://rootedinrights.org/how-to-make-your-virtual-meetings-and-events-accessible-to-the-disability-community/.

User Research Center. "Accessible Remote Instruction." Harvard University. https://urc.library.harvard.edu/accessible-remote-instruction.

Online Teaching And Recording

TeachingSupport@UMN.edu and Faculty Development for Online Teaching Task Group. *Guidelines for Online Teaching and Design.* https://pressbooks.umn.edu/guidelinesforonlineteaching/.

"Video and Audio." Harvard University. https://teachremotely.harvard.edu/video-and-audio.

Feedback And Assessment

Center for Educational Innovation. "Gathering Feedback and Documenting Professional Growth in Teaching." University of Minnesota. https://cei.umn.edu/gathering-feedback-and-documenting-professional-growth-teaching.

University of Wisconsin-Madison. "Best Practices and Sample Questions for Course Evaluation Surveys." University of Wisconsin-Madison. https://assessment.provost.wisc.edu/best-practices-and-sample-questions-for-course-evaluation-surveys/.

Example Trainings And Resources

Training materials from the 2020 *Data Privacy Best Practices Training for Libraries* PLP trainings can be found at https://www.plpinfo.org/dataprivacytoolkit/.

"Data Privacy Project." https://dataprivacyproject.org/.

Henning, Nicole. "Online Privacy & Security Course." https://nicolehennig.com/courses/privacy-security-best-practices-library-users/.

"Library Freedom Institute." https://libraryfreedom.org/index.php/lfi/.

"Main Page/Teaching Resources." Library Freedom Wiki. https://libraryfreedom.wiki/html/public_html/index.php/Main_Page/Teaching_Resources.

NYC Digital Safety. https://nycdigitalsafety.org/.

"Cybersecurity for Youth Using Minecraft." 2019. *Pacific Library Partnership.* https://www.plpinfo.org/minecraft/.

"Digital Shred: Privacy Literacy Toolkit." https://sites.psu.edu/digitalshred/.

"Security Education Companion." *EFF.* https://sec.eff.org/.

Further Reading — Data And Privacy

Anderson, Jill. 2020. "Analyzing the Foundations of the American Right to Privacy Part 3." Choose Privacy Every Day. https://chooseprivacyeveryday.org/analyzing-the-foundations-of-the-american-right-to-privacy-part-3/.

Chisholm, Alexandria Edyn, and Sarah Hartman-Caverly. 2020. "Privacy Literacy Instruction Practices in Academic Libraries." https://scholarsphere.psu.edu/resources/6e465f98-fc36-478e-bba5-3f29c52a7632.

VPRO. 2019. *Shoshana Zuboff on Surveillance Capitalism.* https://www.youtube.com/watch?v=hIXhnWUmMvw.

Swire, Peter P., and DeBrae Kennedy-Mayo. 2020. *U.S. Private-Sector Privacy.* Third Edition. IAPP. https://iapp.org/resources/article/u-s-private-sector-privacy-third-edition/.

Zuboff, Shoshana. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30 (1): 75–89. https://doi.org/10.1057/jit.2015.5.

Further Reading — Making The Case For Privacy

"Data Privacy Best Practices for Libraries." 2020. Pacific Library Partnership. https://www.plpinfo.org/dataprivacytoolkit/ (Sections One and Seven in particular).

Nussbaumer Knaflic, Cole. 2014a. "Storyboarding." Storytelling with Data. https://www.storytellingwithdata.com/blog/2014/02/storyboarding.

———. 2014b. "The 3-Minute Story." Storytelling with Data. https://www.storytellingwithdata.com/blog/2014/02/the-3-minute-story.

———. 2014c. "What's the Big Idea?" Storytelling with Data. https://www.storytellingwithdata.com/blog/2014/02/whats-big-idea.

Further Reading — Security

International Federation of Library Associations and Institutions. 2020. "Awareness, Planning, Resilience: Thoughts on Libraries' Cyber Defense in 2020." Library Policy and Advocacy Blog. https://blogs.ifla.org/lpa/2020/03/27/awareness-planning-resilience-thoughts-on-libraries-cyber-defense-in-2020/

Ibrahim, Hassana Ozavize and Fatimah Abedo Umar. 2020. "Cybersecurity Threats and Its Emerging Trends on Academic Libraries." International Journal of Academic Library and Information Science. http://academicresearchjournals.org/IJALIS/PDF/2020/March/Ibrahim%20and%20Umar.pdf

Caro, Alex and Chris Markman. 2016. "Measuring Library Vendor Cyber Security: Seven Easy Questions Every Librarian Can Ask." Code4Lib Journal. http://journal.code4lib.org/articles/11413

American Library Association. 2016. "Library Privacy Guidelines for Public Access Computers and Networks" http://www.ala.org/advocacy/privacy/guidelines/public-access-computer

Kahn, Miriam B. 2007. *The Library Security and Safety Guide to Prevention, Planning, and Response.* Chicago: American Library Association Editions. https://www.alastore.ala.org/content/library-security-and-safety-guide-prevention-planning-and-response

"For Librarians." Scholarly Networks Security Initiative (SNSI). https://www.snsi.info/librarian-resources/

Additional Resources — Podcasts

"A Big List of IT Security/Cybersecurity Podcasts."
https://github.com/Blake-/cyber-security-podcasts

Additional Resources — Websites And Newsletters

Pardon the Intrusion Bi-weekly Letter About Security and Privacy (The Next Web)
https://thenextweb.com/newsletter/

SANS Reading Room: http://www.sans.org/

Sans: https://www.sans.org/newsletters/newsbites

Security Newsletter Archive: https://securitynewsletter.co/archive

Srsly Risky Biz: https://srslyriskybiz.substack.com/

tl;dr sec Newsletter: https://tldrsec.com/

This page intentionally left blank

SECTION 5

Training Plan Template

SECTION 5.0

TRAINING PLAN TEMPLATE

This general template will guide trainers through a high-level process in building a library privacy/cybersecurity training. Trainers can customize the template to reflect the needs or circumstances surrounding the specific training being developed.

Training Title:

Training Description

In 100 words or less, describe the training to your intended audience.

Date And Length Of Training Session:

Training Audience

Who is the intended audience for this training?

Why are they the audience for this specific training?

What organizational needs or issues are addressed by offering this training to the intended audience?

Learning Objectives

By the end of your training, what should learners know or be able to do?

Take the list from the last question and create at least two to three learning objectives following these guidelines:

- *Begin with an active verb*
- *List one main action, be it skills, knowledge, or values*
- *Aim to be measurable by the learner and trainer*

1.

2.

3.

Training Content And Methods

Content

What content will be covered in the training?

How does the content relate to the learning objectives?

How is the content relevant to meeting the needs of the intended audience? The organization?

If you need to trim the list of training topics, which content might be better suited to be covered outside of the training session and how can you cover them?

Activities

What types of active learning will you incorporate into your training?

How will each activity help learners achieve the learning objectives?

How does each activity tie back to the material covered in other parts of the training?

Training Location

In-person training

Where will the training take place?

What is the training room configuration, including placement of chairs, tables, podium, etc.?

Does this training take place in a different location than the learners' work places? If so, what travel information needs to be sent to learners, including directions, building entrances and room numbers, parking and public transit information, cafes or other food/drink places nearby, etc.?

Online training

What software and applications will the online training use for content delivery?

What software and applications will the online training use for learner activities?

Will the training session be synchronous or asynchronous?

If asynchronous, what content needs to be recorded?

If synchronous, when will the session take place and on what platform?

What are the equipment and software requirements for learners to access the online training?

How will learners acquire and/or access the equipment and software required for the online training? Will learners need instructions for installing specific software or other specific instructions about accessing the training platform?

Training Logistics

Schedule

Outline the training session below with approximate times for each topic/activity as well as breaks, announcements, ground rules, introductions, etc. Don't forget to schedule "cushion time" at the beginning and end of the session in case of delayed start times, unscheduled announcements, etc.

Equipment

IN PERSON TRAINING

What equipment will you need for your training session?

- Laptop
- Microphones for trainer and for audience
  - Lapel
  - Wireless
- Projector
- Speakers or A/V system for playing sound from laptop (if playing sound or video files)
- Whiteboard and markers
- Easel flip charts/boards and markers
- Easel
- Note pads, pen, pencils, markers for learners
- Clock or timer

- Other (list below)
  - _____
  - _____
  - _____

ONLINE TRAINING

What equipment will you need for your training session?

- Laptop or desktop computer
- Microphone (or headset with an attached microphone)
- Headphones
- Web camera
- Ring light or other light source
- Other (list below)
  - _____
  - _____
  - _____

Training materials

What handouts, materials, files, resources, etc. will you need to provide to learners? _____

Which materials should be sent to learners before the training, if any? _____

Which materials should be available at the time of training?

Which materials should be sent to learners after training, if any?

Ground rules

What are the ground rules or guidelines for your training session?

Accessibility

Trainers must ensure that training spaces and materials are accessible to all leaners. The following resources contain information about accessible presentations, online content, and physical spaces:

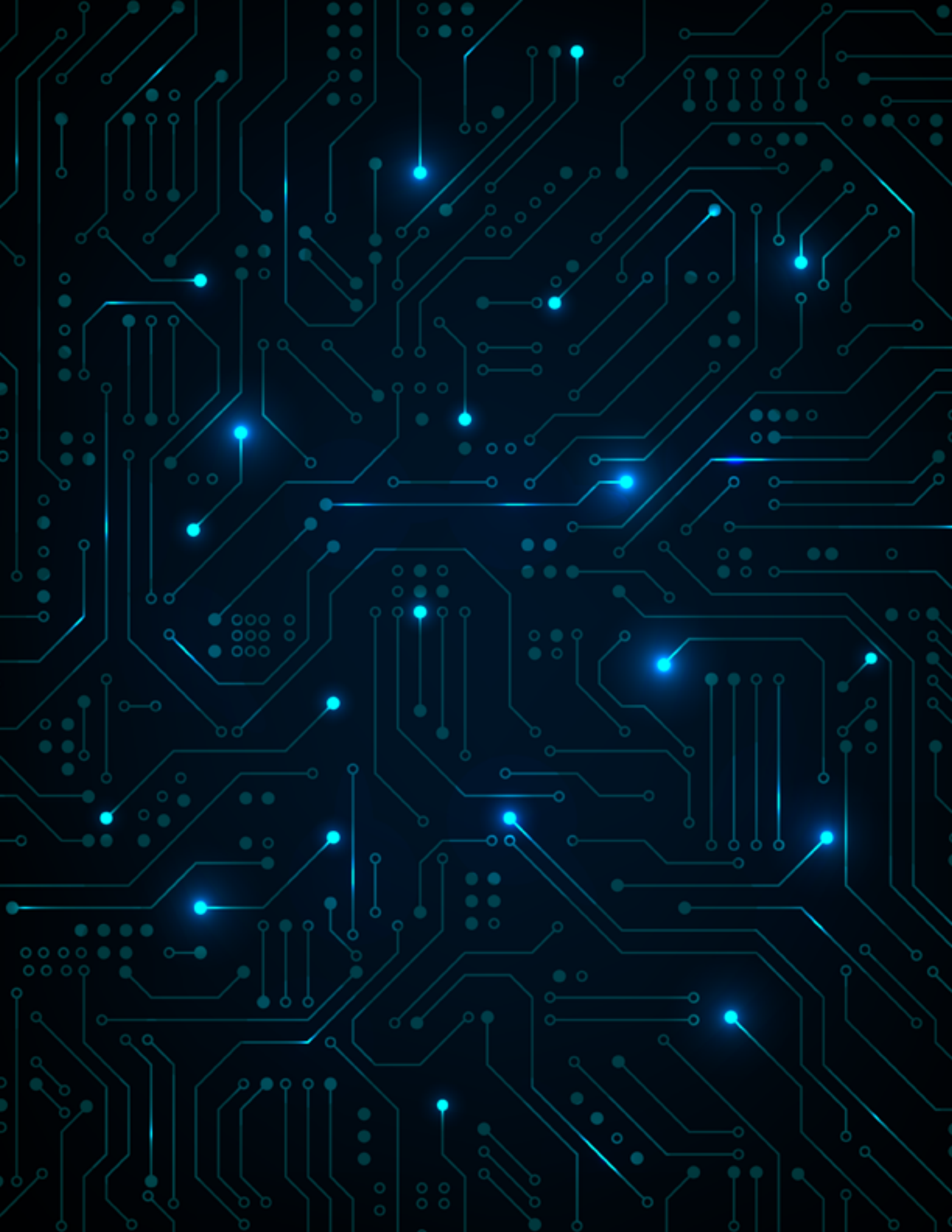
- Create Accessible Digital Products (Section 508) — https://section508.gov/create
- How to Make Your Presentations Accessible to All (WAI-W3C) — https://www.w3.org/WAI/teach-advocate/accessible-presentations/
- Making Meetings Accessible (CDC) — https://www.cdc.gov/ncbddd/hearingloss/transcripts/Making-Meetings-Accessible.pdf

Trainers can learn more about planning for more accessible in-person training by contacting organizational staff responsible for accessibility at their organization, as well as reading more about accessible meeting requirements such as https://accessibility.cornell.edu/event-planning/accessible-meeting-and-event-checklist/ and other resources listed in the 2021 Train the Trainer Handbook.

Feedback/Evaluation

How will you evaluate the training session? Evaluation surveys, feedback from peer trainer observations, etc.?

This page intentionally left blank



Pacific Library Partnership

32 W. 25th Ave., Suite 201
San Mateo, CA 94403
650-349-5538
info@plpinfo.org

Data Privacy & Cybersecurity Best Practices Train-the-Trainers Handbook *is supported in whole or in part by the U.S. Institute of Museum and Library Services under the provisions of the Library Services and Technology Act, administered in California by the State Librarian. The opinions expressed herein do not necessarily reflect the position or policy of the U.S. Institute of Museum and Library Services or the California State Library, and no official endorsement by the U.S. Institute of Museum and Library Services or the California State Library should be inferred. This document does not constitute legal advice, and is for information purposes only. Please consult an attorney or other legal counsel for legal advice.*