CYBRARY

How to Build a Future-Proof Cybersecurity Skills Development Program

The Complete Guide for Organizations Looking to Build High-Performance Cybersecurity Teams

2023

Cybersecurity Training Has Become Mission-Critical

In February 2021, a series of supply chain attacks involving software vendor SolarWinds compromised several US Government agencies. The company's executives blamed the data breach on an intern for using the password 'solarwinds123' which, aside from being extremely weak, had been made publicly accessible via a GitHub repository.

Later in 2021, a highly targeted phishing campaign against employees of Sacramento County intercepted their login credentials via a fake login page. The attack ultimately led to the hackers gaining access to thousands of confidential health records.

In January 2023, popular email marketing platform vendor MailChimp disclosed a data breach due to a social engineering attack that granted hackers access to an internal customer support tool. In doing so, they were able to steal private employee information and credentials.

All these incidents, among thousands of others over the past few years, have one thing in common – they were a direct result of human error. In fact, Verizon's latest Data Breach Investigation Report found that 82% of breaches involve a human element, such as falling victim to a threat actor posing as a trusted figure in the case of business email compromise (BEC) attacks. According to the FBI's Internet Crime Report, BEC alone cost US businesses $2.4 billion in 2021. There is no doubt about it: people are invariably the weakest link in information security.

Human error comes in many forms, including both skill- and decision-based errors. While we cannot eliminate human error entirely, we can mitigate it. With the right approach, we can transform our workforce from the weakest link into the first and last lines of defense against malicious actors.

To mitigate the risks of human error, most forward-thinking organizations have cybersecurity awareness programs in place, but they are not always enough. Teams directly involved in the development, deployment, and management of a company's technology systems and products need cybersecurity-specific knowledge and skills to do their part in protecting your organization.

Our recent report, developed with leading research firm Omdia, found that executive leadership increasingly views cybersecurity training as a key factor in their organizations' ability to prevent data breaches. However, the benefits do not stop there. Successful programs also lead to many indirect benefits, such as enhanced operational efficiency and increased brand trust. They add value to a business at a time when security has become an inseparable part of the relationships between businesses and their customers.

In this guide, we will explore the best practices for building a high-performance, leading-edge training program that will help secure and future-proof your business. We will cover the entire cybersecurity training lifecycle, from getting executive support to achieving long-term success.

Table of Contents

4 Getting Executive Buy-in and Alignment

4 Build a Business Case

5 Define the Scope and Plan

6 Identify Success Metrics

7 Developing a Training Curriculum

7 Assess Current Knowledge

8 Align With Business Needs

9 Review Standard Curriculum Models

10 Choosing the Right Platform

10 Develop Platform Selection Criteria

12 Increasing Adoption and Engagement

13 Adopt a Sales and Marketing Mindset

13 Build a Continuous Communications Plan

14 Leverage Gamification and Rewards

14 Monitoring for Continuous Improvement

14 Set and Track Team and Individual Goals

15 Review Organization-Level Success Metrics

15 Understand the Impact of Your Training Program

Getting Executive Buy-in and Alignment

Corporate executives are concerned with the bottom line and manage many projects and people simultaneously. Today's business leaders might take cybersecurity more seriously than ever before, but rarely is it consistently top of mind. Moreover, there is a common misconception that cybersecurity is a largely technical discipline and the sole responsibility of IT. As such, it may take some convincing to get their support and secure funding for cybersecurity training programs. In this section, we'll explore how to overcome those barriers.

Build a Business Case

Today's security leaders need to become agents of change and champions of innovation, and that demands a keen awareness of business needs. In today's business climate, it is essential for CISOs to align cybersecurity initiatives with business needs. As a first step in building a cybersecurity training program, security leaders need to build a business case to convince hesitant executives and leadership stakeholders.

Equipped with a compelling business case, security leaders will greatly increase their chances of acquiring the necessary budget. A strong business case highlights both the benefits of training and the costs of not training. At the same time, the need to invest in cybersecurity training should never be communicated as a necessary evil, but as an enabler of innovation that adds value to the entire enterprise. Therefore, focus on the benefits of adopting such a program.

Here are some of the most important benefits to highlight:

Positive impacts on the efficiency of new and existing cybersecurity roles and initiatives include having a more secure and accessible asset inventory and enhanced threat intelligence.

73% *of business leaders have reported improvements in efficiency after rolling out a cybersecurity training program.**

Positive impacts on the effectiveness of cybersecurity training include a lower number of attempted attacks leading to breaches, and a marked reduction in the number of security events when compared to industry averages.

62% *of business leaders reported an increase in the effectiveness of their cybersecurity programs after investing in training.**

Providing training as part of the job, particularly when paired with internal career development opportunities, encourages employee retention, while also making the company's employment brand more attractive to new recruits.

90% *of business leaders reject the popular myth that training encourages existing employees to start hunting for jobs elsewhere, and nearly half believe training decreases the likelihood that cybersecurity professionals will leave the organization.**

* Statistics are from our research report with Omdia, "The Myths of Training Cybersecurity Professionals",based on a survey of nearly 300 cybersecurity leaders.

When building your business case, emphasize the indirect and nuanced benefits as well. There are many ways that rolling out a security training program adds business value. Not only does an engaging training program help fortify corporate culture; it enhances the overall business acumen of employees and increases productivity. It also reduces risk to the business across multiple domains, such as brand reputation and legal and compliance.

While focusing primarily on the business benefits of security training helps avoid a more doom-laden message, you still need to highlight the potential costs of not implementing a program at all. These include direct financial costs associated with breach remediation, fines for compliance failures, and costs racked up by unscheduled downtime. On top of that are the indirect costs, such as brand damage and reduced customer loyalty, which are often even greater. According to IBM's Cost of a Data Breach Report, on average a data breach costs $4.35 million, and 83% of organizations experienced more than one breach in 2022.

Define the Scope and Plan

Ideally, you should define the scope of your cybersecurity training program while building the business case, or immediately afterwards. After all, every organization has limited resources, which is why it is important to prioritize the most impactful components rather than pursue perfection. Most importantly, training should be treated as an ongoing program rather than a one-off project. The benefits of training accumulate over time, and a constantly evolving threat landscape requires continuous learning.

To secure an appropriate budget for training, security leaders must consider budget limitations and realities. For example, for companies on leaner budgets, it may be necessary to identify a subset of users who need training the most, such as those who routinely handle sensitive information or have high-level access to network and computing infrastructure. Ideally, basic training should extend to all knowledge workers in the organization, while advanced training should be provided to those involved in high-risk areas like IT, governance, risk management, and compliance (GRC), finance, or software development. Defining the reach of your program will also be an important factor when selecting a training platform or vendor.

Companies that currently lack any kind of security training program should start small, with a focus on expanding later on. Such a plan might involve equipping employees with the basic knowledge and skills they need to move on to higher-level topics further down the line. On the other hand, companies that already provide basic or ad-hoc training may want to formalize the process to maximize (and track) its benefits.

Finally, regardless of the scope, you should plan on integrating training with on-the-job tasks and responsibilities. This will further maximize the program's effectiveness, while reducing costs associated with traditional learning formats like bootcamps and seminars like boot camps and seminars that require staff to take large blocks of time off solely for training.

Identify Success Metrics

Key performance indicators (KPIs) are the success metrics that you will use to evaluate the performance of your training program. It is important to establish these early on, ideally when building your plan. While most of these will only be relevant to specific departments, such as IT or GRC, incorporating one or two as organization-level objectives and key results (OKRs) can help when seeking executive buy-in. Here are a couple of possible OKRs:

- Employee onboarding cycle: This is the time it takes for a new security employee to attain optimal productivity. A formal training program should reduce this timeframe.
- Employee retention (or conversely, turnover): This refers to the percentage of staff who stay with the company over a given period versus the percentage who leave (or vice versa). A 90% retention rate is normally a good baseline. However, remember there are many possible factors influencing retention and turnover, so it is helpful to conduct exit interviews and engagement surveys to determine the extent to which training plays a role.

Additionally, there are several important success metrics that point to the role of training in advancing your organization's security posture. These security-centric metrics should improve with the implementation of a formalized cybersecurity-focused training platform:

Mean time to detect:
The average time it takes to discover a new threat.

Mean time to resolution:
The average time it takes to resolve an incident.

Volume of security events:
The total number of events, incidents, and breaches.

Security leaders should focus on some of the more important, company-level success metrics when building their business case. However, it is also important to involve stakeholders from across business departments to determine which ones are most important to your organization and its appetite for risk, regulatory obligations, and industry.

Developing a Training Curriculum

A training program should contribute to an organization's overall security posture. Applying a checkbox approach to training is not enough, nor does it respond adequately to the constantly evolving threat landscape. It is important to keep this in mind when developing a curriculum, which itself should be adaptable and centered around continuous improvement.

Cybersecurity skills iterate and build on one another, much like the inner workings of a flywheel, with knowledge of essential concepts enabling intermediate and advanced skills. For example, any security practitioner will need at least a baseline knowledge in areas like networking, hardware, and cloud computing. As a security leader, you should plan to address the full skills spectrum over a reasonable length of time and continue monitoring and reinforcing skills thereafter.

Assess Current Knowledge

Cybersecurity training should follow a learning continuum that begins with building awareness before blending into training and developing into continuous education. However, before you can establish that continuum, you need to benchmark your team's current skills and knowledge. You can use a globally recognized framework like the NIST SP 800-16 or NIST SP 800-50 to establish your team's training requirements based on specific roles.

There are many ways to assess your team's current knowledge, but by far the easiest are tests that align with an industry-standard framework like those mentioned above. Skills assessment tests are valuable for HR teams carrying out pre-employment screening, as well as for security leaders wanting to evaluate the knowledge and skills of their existing teams.

More generalist cybersecurity functions, particularly in the case of organization-wide training programs, should start with the basics, while those in IT and cybersecurity roles will need more specialized and targeted training. Awareness training should apply to all knowledge workers in the organization, simply because security is everyone's business. For example, employees need a baseline knowledge of things like password hygiene and how phishing scams work. However, those in IT roles will need a baseline knowledge of cybersecurity concepts, such as incident response and contingency planning. There are several proven tools and techniques for evaluating these baseline skills:

- **Launching surveys to determine current security perceptions**
- **Running skills assessment tests, exercises, and simulations**
- **Monitoring access points to record instances of tailgating**
- **Performing unannounced checks for things like unlocked devices**

Every organization should take the above steps regularly. This will establish the foundations for developing a training curriculum that aligns with unique business needs and environments.

Align With Business Needs

While awareness training encompasses the baseline set of skills and knowledge that every business needs, a cybersecurity skills development curriculum should be closely aligned with the unique needs and conditions of the business. For example, if your business provides SaaS products, you will need people who are familiar with topics like application security, IAM, and cloud computing security.

There are many possible use cases, simply because every organization faces different priorities, risks and obligations. Here are some examples:

GDPR

Your business is expanding into the EU and therefore needs to become compliant with the General Data Protection Regulation (GDPR). In this case, your team will need to follow the concepts and best practices of GDPR, such as data classification, privacy impact assessments, privacy policies and procedures, and subject access requests.

HIPAA

Your business is expanding into the healthcare sector, and therefore must comply with the Health Insurance Portability and Accountability Act (HIPAA). In this case, all security practitioners, as well as anyone else with access to systems that hold private health information, will need additional compliance training.

SIEM

Your business's infrastructure is facing more frequent and advanced attack attempts. In this case, you will need to prioritize advanced blue-teaming skills, including threat profiling, attack modelling, and intimate familiarity with SIEM tools. You might also consider purple- or red-teaming skills to better understand adversaries and proactively prevent attacks.

CLOUD

Your business is migrating its legacy IT infrastructure to modern, cloud-based systems. In this case, those involved in the migration will need a robust understanding of cloud-specific AWS security risks, as well as the risks associated with the migration itself. Further, you may need to provide platform-specific (e.g. Azure or AWS) security training.

The potential use cases for providing more specialized or advanced security training are practically limitless. However, the above examples should help provide a sense of direction to inform the development of your training program.

Review Standard Curriculum Models

While every training program should be tailored to the unique needs of the business and existing employee skill sets, it helps immensely to have a standard curriculum model to build upon. That way, you can pick and choose what makes the most sense based on the above considerations. A good starting point is NIST, which regularly publishes guidelines for cybersecurity curricula. These are based on globally adopted frameworks like the NICE Workforce Framework for Cybersecurity and the National Centers of Academic Excellence in Cybersecurity.

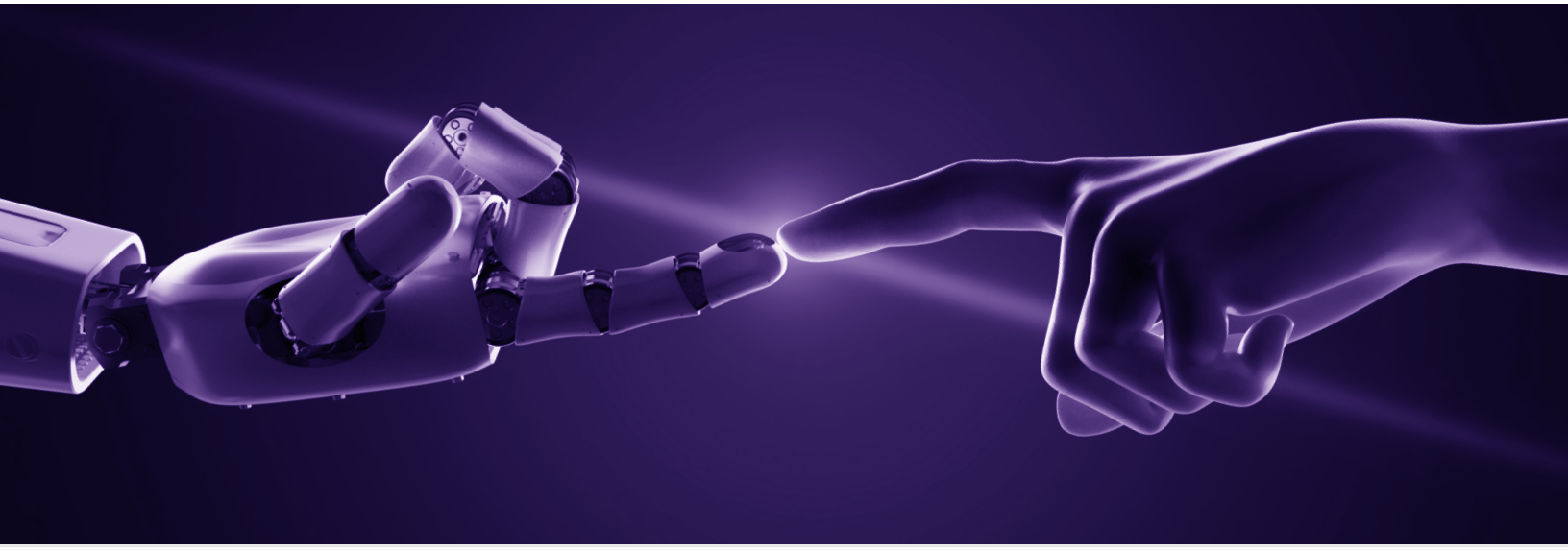
Many training vendors provide customizable curriculum models based on these guidelines and frameworks. At Cybrary, we focus on a few high-level concepts when recommending curriculum to our members:

Career Development:
Content that orients learners to the basic functions within cybersecurity roles and career paths, helping them advance in maturity and evolve their skills:

Foundations | **Offensive Security** | **Defensive Security** | **Engineering, Operations, and Architecture** | **Governance, Risk, and Compliance** | **Leadership and Management**

Certification Preparation:
Content that prepares learners to attain key industry certifications across all skill levels, and also relates concepts in the exams to practical, on-the-job skills.

Mission-Readiness:
Content that keeps working cybersecurity professionals informed on the latest threats and vulnerabilities, honing their problem-solving skills and sharpening their cybersecurity instincts.



Choosing the Right Training Platform

The traditional approach to cybersecurity training is to send employees off to bootcamps or seminars. These training formats take a one-to-many approach and often lack customization and alignment with specific business needs and use cases. The programs themselves are costly, and employee travel and related expenses pile up quickly. As such, employees undergoing traditional training tend to spend longer periods away from work, potentially leaving you short-staffed.

Choosing an online learning platform is a far more appropriate and cost-effective approach, since it can facilitate on-demand, self-paced learning, hands-on skills development, and customization. Online learning has become the gold standard for learning on or off the job. That said, there are many platforms and vendors to choose from, all of which cater to different needs and audiences. In this chapter, we will look at the most important considerations when choosing a platform that will work for your business both in the short and long term.

Develop Platform Selection Criteria

Below are some of the most important selection criteria to consider when choosing a platform that will work for your business both in the short and long term.

Depth and Breadth

Your training platform must be able to meet the demands of the scope you defined previously, and then some. Cybersecurity concepts build on one another as needs evolve and new threats and measures to counter them emerge. Consequently, your training platform needs to cover a broad range of topics, including foundational IT knowledge areas needed to pivot into cybersecurity-specific roles as well as more specialized skills like red-teaming and SIEM application workflows.

Large enterprises, particularly those with workforces scattered across countries and regions, face a broader range of threats and must also adhere to a wider variety of compliance regimes and standards. By contrast, smaller organizations will want to focus more on the specificity of the training content available rather than its extent. Always choose a platform that provides sufficient scope to meet the needs of an increasingly diverse workforce.

Centralized Content

One of the most important considerations is the availability and accessibility of the content. You should avoid having multiple, ad-hoc training resources since this diminishes their value and makes it difficult, if not impossible, to comprehensively track progress and performance. This is a common issue if you end up using multiple vendors to accommodate your training goals. Instead, having a one-stop shop for all your training resources ensures standardization, alignment with your training curriculum, and complete trackability.

The best training platforms have extensive partner ecosystems to seamlessly integrate essential functions. For example, an integrated training platform should provide a unified user experience across skills assessment solutions. Choosing a platform that integrates skills assessment and virtual labs vendors allows learners and administrators alike to easily track progress from a single, centralized interface.

Cybersecurity Focus

Online learning has become a vast and highly diversified industry with numerous options to choose from. The best known vendors are enormous platforms like Coursera and Udemy, which provide thousands of courses spanning virtually every industry vertical. However, these are aimed more towards individual learners pursuing online degrees and enterprises seeking educational development across a very broad range of areas.

When it comes to putting your cybersecurity training curriculum into action, generalist learning platforms can be overwhelming for learners and administrators alike. As such, it is usually best to choose a platform that specializes in cybersecurity and its related disciplines. The platform you choose should cover generalist IT skills as well, especially if you have employees on your team who currently lack the foundational skills needed to take on security-oriented roles.

Timeliness and Relevance

The ever-changing nature of the cybersecurity landscape is precisely what makes traditional forms of education, such as formal college degrees, less relevant than they are in other fields. It is also why most IT- and cybersecurity-related certifications need to be renewed once every three years. When it comes to certification-aligned training, it is vital that learning materials align with the latest edition of the certification in question.

The training platform you choose must take these factors into consideration. It should regularly update not only its standard training content, but also regularly add courses and materials to address new vulnerabilities. Moreover, new vulnerabilities and threat actor campaigns arise daily. For example, many training programs rely on MITRE ATT&CK, a global knowledgebase collating the latest adversary tactics and techniques based on real-world observations.

Hands-On Skills Development

No one can expect to become a cybersecurity practitioner, or even a security-conscious team member, if every team member's learning materials follow the same format. While everyone has a preferred way of learning, the only way to validate the skills and knowledge acquired is to put them into practice in a real-world scenario. Therefore, virtual labs and up-to-date skills assessments are a critical part of the process.

A large part of cybersecurity training involves learning by doing. For example, cybersecurity skills that deal directly with data breaches and ethical hacking cannot be learned solely by passively consuming training content. Virtual labs allow trainees to put their skills to the test in the safety of virtual machines that accurately replicate the real-world environments they are likely to encounter in their jobs.

Variety of Content

Variety is a critical enabler of knowledge retention, while also helping to accommodate a broad range of learning styles and preferences. For example, training modules of various lengths will make the program more accommodating to employees' schedules and allow training to fit in between meetings.

Your training platform should incorporate a variety of text- and video-based learning materials to help learners get up to speed with the various concepts and knowledge areas of the topic. Just as important is accessibility to interactive components like hands-on labs that use real virtual machines where people can put their newly acquired skills to the text. Similarly, a variety of content lengths, with long form, deeper dive activities mixed with shorter, bite-sized modules, give learners options when trying to fit training into a busy schedule.

Increasing Awareness and Adoption

Once you have a training curriculum and a platform, the next step is to communicate it to your employees. Ideally, you should start building awareness a few weeks before rolling out the program, much like a marketing team does ahead of a new product launch.

When enrolling employees in cybersecurity training, you also need to make clear the goals and expectations for each job role, since not everyone will need the same degree of training. Everyone who works with a computer should have at least a baseline knowledge of common security threats and the ways to counter them, while IT practitioners themselves will need a more extensive set of knowledge and skills.

You will also need to factor in employees' time and availability. For mandatory cybersecurity training, be sure to schedule time blocks during employees' current work schedules. That said, you might also want to encourage employees to learn off the clock, especially when it comes to ancillary skills that support career development. Some learning platforms provide subscriptions that grant access to their entire content portfolio which, for employees and new recruits alike, provide a substantial extra job benefit. This is even more attractive in the era of widespread layoffs, where employees are increasingly concerned with their job security.

Adopt a Sales and Marketing Mindset

Ask almost any employee what they think about training, and there is a high chance they will respond unfavorably. The first thing that may come to mind is more work and a greater burden on their already busy schedules. This is even more likely if communicating your training program revolves around the needs of the business rather than the benefits to your employees. Focus instead on the benefits for employees, which extend to both their professional and personal lives.

Creativity and thinking outside the box can also go a long way towards fostering engagement. Security leaders can learn a lot from high-performance marketing teams. For example, making your internal campaign thematic adds an element of fun and helps overcome the widespread perception that cybersecurity training is just for IT professionals. Consider incorporating elements of pop culture and other shared interests across your organization and weaving them into the messaging promoting your training.

You should think of it as an internal campaign that centers around the value training offers to your employees, not just to the business. Benefits for employees might include internal career development opportunities and greater workplace morale. After all, a security-aware employee is more likely to confidently engage with innovative new projects. Of course, the business benefits are already clear, but centering your communications around the needs and desires of your employees will make your training program vastly more accessible.

Build a Continuous Communications Plan

A continuous communications plan takes a structured approach to prioritizing key topics and reaching the KPIs and objectives established at the onset of the project. It is a vital component of any formalized training program, since it keeps everyone on track and provides the means to monitor performance and drive a culture of continuous improvement. Start by outlining the what, why, and how of the program, and build reminders and nudges throughout the various stages of the training lifecycle. Remember, while specific projects might have a finite lifespan, cybersecurity training overall is never a one-and-done process.

Next, choose suitable communication channels for providing announcements, feedback, and support. For example, you can make major announcements at company- or department-level meetings and use email for sending reminders about upcoming projects and training goals. It is also important to have a collaborative space where everyone can share knowledge and get support. Consider creating a dedicated channel on Slack where employees can share ideas, ask for help, or simply share their latest successes. In all communications channels, include a short list of helpful and relevant resources using internal knowledge bases like SharePoint Team sites.

Finally, be sure to get executive leadership as involved as possible. Not only is their initial buy-in important – their direct and ongoing involvement is just as crucial. By having them participate in communications and formal recognition of employees' milestones, they can lead by example and greatly boost engagement.

Leverage Gamification and Rewards

Adding interactive components to your training program can take engagement to a whole new level. Gamification is a proven strategy that involves tactics such as developing points systems, using badges to recognize achievements, and publishing leaderboards to add a competitive element. In fact, gamification is the reason why apps such as Duolingo, Elevate, and Lumosity have become enormously popular in everything from language learning to brain training. There is no reason why cybersecurity training should be any different.

By introducing gamification, you can make your training program go viral within the company. For example, introducing leaderboards provides visibility into progress and public recognition for your best performers, keeping the program top of mind by stoking friendly competition between teammates. This also encourages employees to stick to the training and even go above and beyond expectations.

Rewarding employees for their efforts will keep them coming back for more. Structure rewards for top-performing teams and individuals. While gamified rewards like points and badges grant recognition, physical rewards are important for showing appreciation for big accomplishments, such as meeting a major training milestone or earning a certification. For example, you might offer employees gift cards, a donation to a charity of their choice, swag bundles, or tech gadgets. At the team level, you might host a special outing for the winning team at a highly-rated restaurant or sports event. Finally, at the organization level, you might provide a company-wide reward for meeting a specific OKR.

Monitoring for Continuous Improvement

The ever-changing threat landscape demands an ongoing training program that continually adapts to the new reality. You also need to be able to answer questions like who has learned what and whether there are any trends that can help you boost adoption.

This is an iterative process that will inform the optimal frequency and most suitable topic areas to focus on. You should also keep a close eye on the latest events in the security field in order to respond quickly to new threats and the measures needed to mitigate them. Sometimes changes to the program will need to be introduced quite suddenly, while others, such as the launch of new certification-based courses, take a more gradual and structured approach.

Set and Track Team and Individual Goals

It is important that you have the means to monitor and track progress and that you regularly review your goals and tweak them as required. Moreover, setting individual goals and checking monthly progress is a good starting point, allowing you to make informed adjustments to said goals thereafter.

The most basic metric to monitor is the completion percentage of an assigned curriculum or course. Higher-level results and outcomes, such as passing certification exams, are also vital. However, it is important to start small by focusing on baseline training. Equipped with a robust foundation, some of your employees – particularly those who are already directly involved in IT – will progress easily, which tells you it is time to up the ante. In other cases, expectations may prove to be unrealistic due to things like a lack of pre-existing knowledge or available time. If this happens, you may want to set more modest goals in order to keep employees motivated and engaged with the program. After all, cybersecurity training should never become a burden.

Review Organization-Level Success Metrics

At the beginning of this guide, we talked about getting buy-in from executive management. Just as important is retaining their support and involvement. That means keeping training initiatives top of mind among your stakeholders. As such, you should review organization-level success metrics multiple times every month. This will help sustain the program and secure the longer-term support you need to make it thrive.

More exhaustive reviews and retrospectives should be held once every three months or more, depending on your organization-level goals and priorities. These reviews should take into account both individual and team goals as well. If you are frequently missing your targets, it is important to understand why.

Sometimes the goals themselves might not be the issue, but the conditions for attaining them are, such as not having enough time available or a lack of supporting materials. On the other hand, if you frequently exceed your goals, it might be time to challenge the team with loftier targets. Keep stakeholders informed and involved with any adjustments, as this helps to build a virtuous cycle that promotes ongoing improvement.

Understand the Impact of Your Training Program

Last but not least, it is vital to understand the ongoing impact of training on the overall security posture of the business. A successful training program will ultimately lead to shorter detection and response times, a reduced number of incidents, and greater awareness of risks facing your business. Things like employee feedback and surveys can help greatly in evaluating perceptions around security in the organization. To gain a clear picture of the effectiveness of the program, security leaders should focus on the following key areas:

> **Awareness:** Regularly evaluate what people have learned by tracking their progress through specific courses, career paths, and certifications earned.

> **Behavior:** Determine how people behave when faced with real-world threats, such as by using simulated phishing scams and enrolling them in virtual practice labs.

> **Perceptions:** Find out how seriously the team takes information security by releasing anonymous surveys, as well as by asking individuals for direct feedback.

> **Culture:** A security-aware company culture is one where employees are confident in their abilities to mitigate threats, while also being open and willing to learn more.

By measuring performance with a combination of hard data and qualitative feedback, you will be able to validate the effectiveness of your training program to executive management. You'll also keep employees motivated and engaged as they develop new skills and advance their careers.

Continuous Cybersecurity Skills Development to Future-Proof Your Business

Cybercrime will only continue to evolve in parallel with technological innovation, and with every new opportunity comes new risks. That is why future-proofing your business starts with having a mature information security posture – one that adapts and improves with support from a continuous training and skills development program. Here is a quick summary of what it takes to bring your training program to that level:

- **Build a strong business case, define success metrics, and build a plan**
- **Develop a training curriculum that aligns with business needs and realities**
- **Select a platform and vendor that provides the necessary coverage and focus**
- **Launch an internal campaign to increase adoption and raise awareness**
- **Monitor, evaluate, and optimize for continuous adaptability and improvement**

These key considerations for training program development support an overarching skills development lifecycle. They create an iterative feedback loop that scales with your organization's growth and business needs.

Cybrary's industry-leading cybersecurity training platform guides key steps of this lifecycle, equipping your team to succeed against a constantly evolving landscape while enabling business growth. With our Cybrary for Teams solution, cybersecurity and learning and development (L&D) leaders can develop critical cybersecurity skills for staff at any career stage.

The Cybrary for Teams platform covers a comprehensive curriculum:

- **Unmatched depth and breadth:** Cybrary offers over 2,000 learning activities covering virtually every cybersecurity skill set, domain, and knowledge area.
- **Centralized platform:** Cybrary is a one-stop-shop for all of your cybersecurity skills development needs, streamlining implementation and progress monitoring across your team.
- **Cybersecurity-focused:** many training platforms are more generalist or IT-focused, but Cybrary has always been laser-focused on cybersecurity skills development.
- **Timely and relevant:** Cybrary's expert instructors stay on top of the latest threats and vulnerabilities to help practitioners prepare their defenses and hone their skills.
- **Hands-on skills:** Cybrary's virtual labs and role- and skill-based assessments develop on-the-job skills that put concepts into practice and make users high performers.
- **Variety:** Cybrary offers a robust mix of content formats spanning on-demand video, multi-modal content, practice tests, labs, and assessments, with a variety of lengths to support short bursts or deeper dive sessions.

To learn how Cybrary can support your team's skills development needs, visit https://www.cybrary.it/business/demo-request-teams/ and request a demo today.

CYBRARY

About Cybrary

Cybrary is a cybersecurity and IT workforce development platform. Its ecosystem of people, companies, content, and technologies create an ever-growing catalog of online courses and experiential tools that provide IT and cybersecurity learning opportunities to anyone, anywhere, anytime. Cybrary has received numerous industry recognitions since its 2015 founding, expanding to a user base of over 2 million users with 96% of Fortune 1000 companies learning on the Cybrary platform.

Visit https://www.cybrary.it/business/demo-request-teams/ and request a demo to see how Cybrary can help you build a future-proof cybersecurity skills development program.