The Enterprise Guide to Establishing a

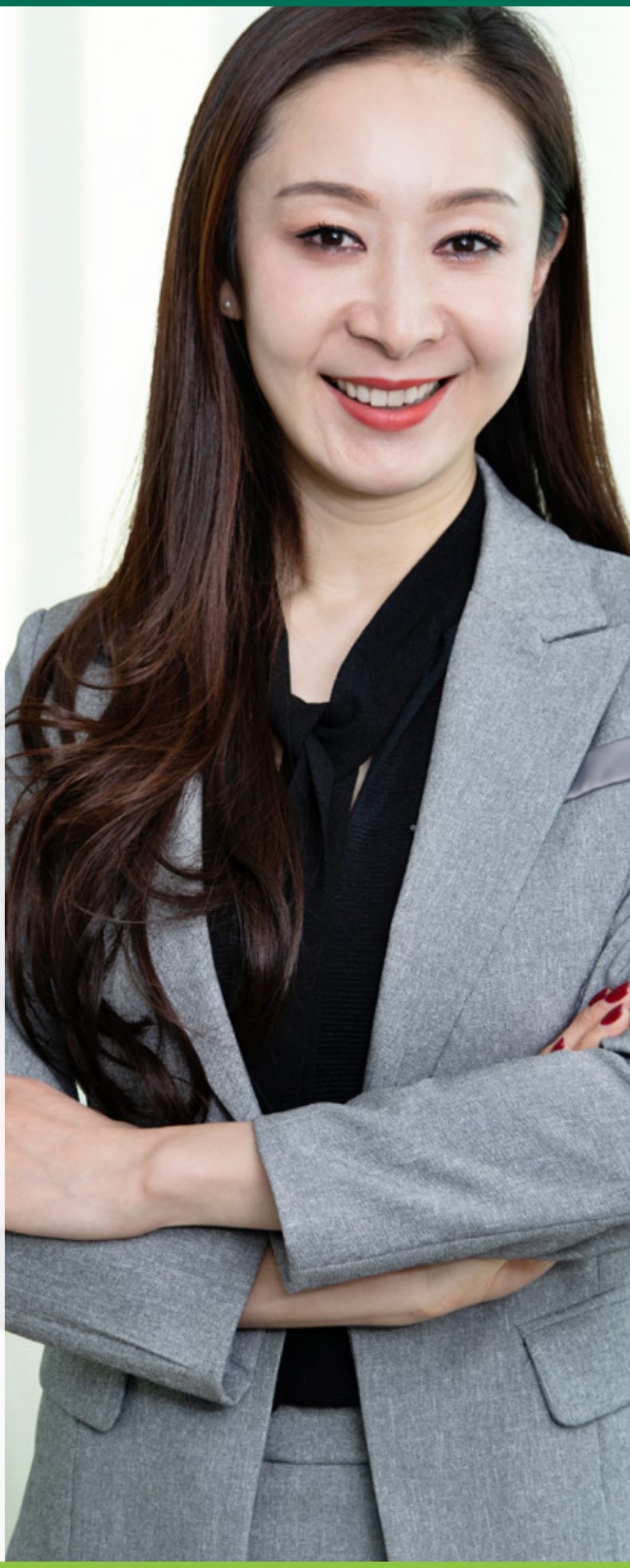
CYBERSECURITY TRAINING PROGRAM

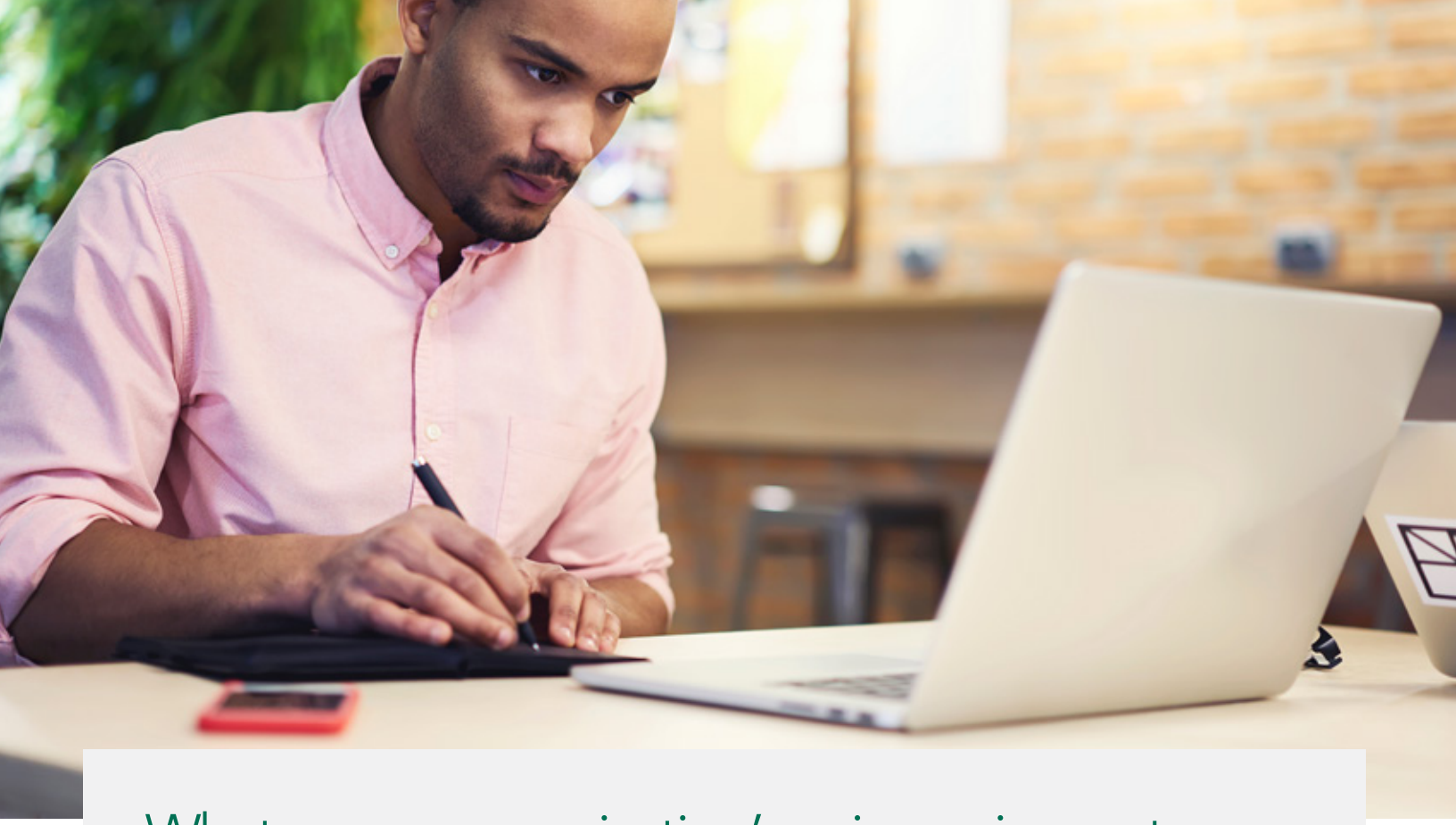
If it's true the best employees never stop learning,

then the best employers must never stop investing in their people. Nowhere is this more critical than in the cybersecurity field, where talent is scarce and employers have to keep existing teams engaged in their profession, and current on the latest threats and defenses.

Cybersecurity professionals must keep learning if they are to reach the top levels of their field, and effectively perform in today's business and technical landscapes that constantly change. Learning on the job is certainly part of the process, but it takes more than that to refine skills, acquire the latest knowledge, keep up with current best practices and demonstrate proficiency. That's why every organization needs a formal, standards-based cybersecurity training and education program for the employees responsible for securing their digital assets.

It's difficult to prescribe a one-size-fits-all approach to training your cybersecurity team. While cybersecurity training needs to be structured and adhere to industry standards, it also must be purposeful and tailored to the organization's needs. No one organization has precisely the same security needs as another. However, many of the fundamentals of a training and education program apply across different organizations and sectors, and that is what this guide will explore.





Whatever an organization's unique circumstances, three major tenets must guide any training effort:

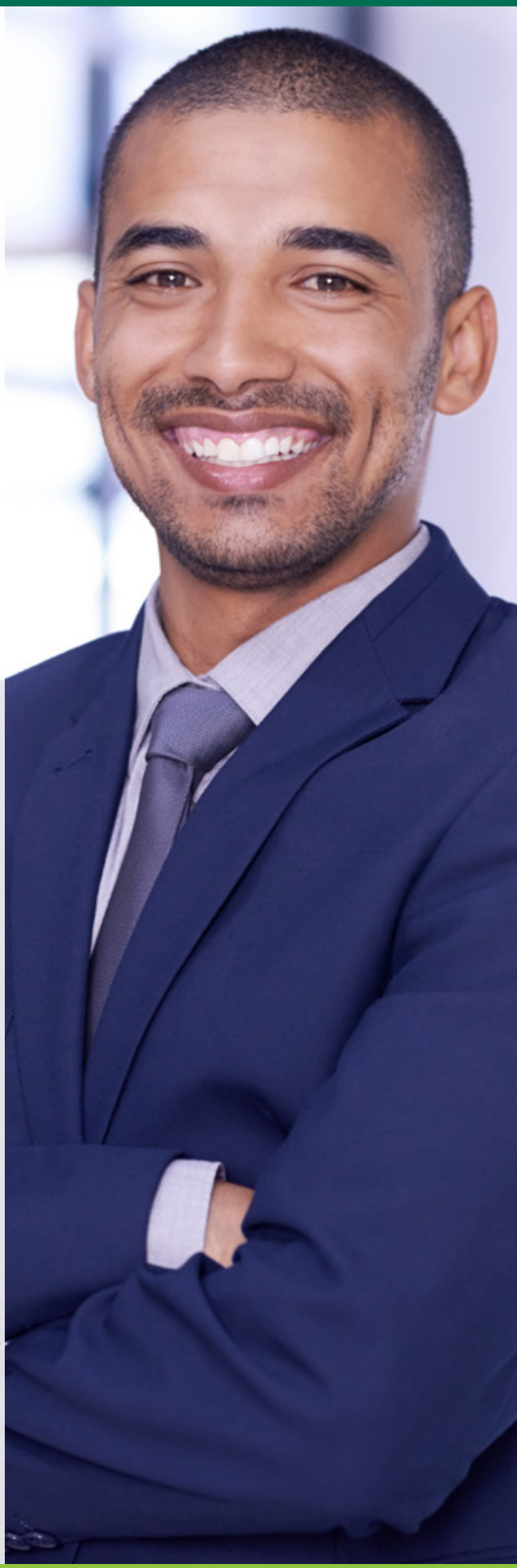
1. Security is an obligation, not an option. Your investment in security hardware, software and services must be complemented by strategic investment in the education of your cybersecurity professionals.

2. Evolving technology and constantly changing threat landscapes require a long-term, agile commitment to security, which starts with ensuring your IT/ICT and cybersecurity teams have access to the training they need to develop, evolve and refine a wide range of skills and experiences.

3. Skills development should be measured for effectiveness, so it's necessary to have a process for team members to demonstrate proficiency of the security principles they've learned.

Who Needs Training?

The answer to who needs cybersecurity training in the organization may seem obvious – the cybersecurity team. However, cybersecurity is a shared responsibility not just conceptually but often in real-world practice. It isn't the sole province of a Security Operations Center (SOC) or your Governance Risk and Compliance (GRC) team. Some organizations don't have a formal security team, instead addressing security – at least from an implementation standpoint – as part of IT's responsibility. Figuring out who needs training starts with identifying those responsible for protecting the organization's critical assets.



CIO

An organization's chief information officer (CIO) or someone in a similar capacity – chief digital information officer or information technology director – sits atop the security hierarchy in many organizations. Even if a company employs a chief information security officer (CISO) or chief security officer (CSO), the position may still report to the CIO. According to **(ISC)²'s 2019 Cybersecurity Workforce Study**, 57% of organizations have CISOs managing security assets, while at 29% of organizations, the responsibility falls to a senior IT executive such as a CIO.

With that in mind, senior IT executives and CIOs should receive an appropriate level of training. How much depends on the extent of the CIO's involvement in cybersecurity. Many CIOs have had security responsibilities as they moved up through the ranks but may not be directly involved in cybersecurity in their current position. Even so, they need a baseline of current security knowledge so they can relate to the cybersecurity team and ensure the organization's security needs are properly addressed. If ever questioned about security in the boardroom, the CIO needs to be able to speak authoritatively. The same goes for the CIO's staff – everyone should have appropriate levels of cybersecurity knowledge in order to fulfill their duties.

CIO's Staff

Some larger organizations have an Office of the CIO (OCIO), which includes a team of leaders for specific IT functions, including security. Members of the OCIO may include:

- Deputy CIO
- Chief Technology Officer
- Chief Development Officer
- Chief Data Officer/ Data Protection Officer
- Compliance Officer
- Application Development Manager
- Help Desk Director
- CISO

IT Department

Organizations without an OCIO, or even a CIO, are still likely to have an IT department and IT director with roles similar to the ones in the list above. Whatever the nomenclature, it's important to understand each role's responsibilities and its relationship to the organization's security in order to map a training plan for each. IT teams may not be formally responsible for setting up cybersecurity programs and policy, but they often implement and maintain them. This means IT teams often play a critical role in securing the organization. They should not simply be viewed as implementing policy, but should also be empowered to contribute to strategy with their unique perspectives, while honing their technical, hands-on skills securing systems and responding to incidents. Providing them with the training shows you are willing to invest in your teams to make them successful in their work and that you recognize the valuable role they play in the broader cybersecurity practice within your organization.

CISO and Cybersecurity Specialists

The CISO and the cybersecurity team are the primary candidates for cybersecurity training and certifications. The same is true in organizations where the IT team is responsible for setting, implementing and maintaining cybersecurity practices. These organizations may treat cybersecurity as its own vertical silo that acts as a check and balance to the office of the CIO. Security teams are structured in various ways according to an enterprise's specific needs, but generally they are subdivided into several functional areas, including:

- **Risk Assessment and Management** – Determines the level of risk the organization can sustain. Develops and maintains risk-based strategies based on assessments, intelligence collection and ongoing updates on the threat landscape and the company's security posture.
- **Policy and Compliance** – Ensures that processes, practices and technologies meet industry standards and adhere to internal requirements, as well as external mandates such as industry-specific regulations and federal and state laws.
- **Security Operations** – Develops and enforces security policies and processes, managing security tools, and monitoring operations to detect and respond to threats.
- **Security Administration** – Implements security strategy and process, including hardening systems, and defending endpoints and networks against threats, performing initial threat assessments, patching applications and maintaining security solutions.
- **DevOps** – Develops or modifies new and existing applications, heading up many systems integrations within an organization, requiring strong security awareness and knowledge of best practices for secure software development.

People to Train

(ISC)² research has determined that a wide array of positions have cybersecurity responsibilities to varying degrees. Consider the following roles and functional areas within your organization for your training program:

Security Administration	Security Operations	Risk Assessment & Management
Security Specialist	Security Analyst	Risk Manager
Security Administrator	Incident Responder	Information Assurance
Security Engineer	Forensic Analyst	Specialist/Administrator
Security Architect	Malware Researcher	Pen Tester (Red Team)
Data Recovery Specialist	Pen Tester (Blue Team)	Vulnerability Specialist

Policy & Compliance	DevOps
Business Continuity Manager	Application Developer
User Awareness Manager	Database Architect
Security Auditor	Database Administrator
Data Privacy Officer	Cloud Architect
Governance, Risk and Compliance Officer	

Who Is Responsible for Training

In-house training teams typically are attached to human resources. Often, they have numerous responsibilities – sometimes shared with other departments – including employee onboarding, training for specific jobs, workplace behavior instruction, compliance with company rules and employee evaluations. However, cybersecurity is a very specialized, dynamic discipline, requiring a focused, expert-led approach. When HR is in charge of training as a function, cybersecurity or IT leadership must be engaged and remain involved in cybersecurity training by assuming the responsibility of creating a curriculum that maps to its needs.

In this scenario, the HR and cybersecurity/IT teams should decide together what areas of training and assessments are needed, as well as which cybersecurity team members should be trained and certified, at which point in their tenure, and for what applicable skill or domain. Consider appointing a cybersecurity training officer who runs the training team and oversees the following responsibilities:

- Managing the budget
- Organizing training schedules by individuals, groups of individuals
- Identifying specialist training providers to supplement in-house capabilities
- Organizing training delivery method:
  - Online Self-Paced
  - Online Instructor-Led
  - Classroom-Based
  - Private On-Site
- Maintaining the training schedule, keeping track of each individual's progress
- Tracking certifications, certificates, assessments and other proof of accomplishments or course completions earned by each individual

Determining the Curriculum

Developing a cybersecurity education curriculum requires proper planning, starting with a thorough assessment of the organization's needs.

1 Assessment

A comprehensive assessment is likely to uncover needs that an organization may not have recognized yet. Here is an example of which areas an assessment should cover:

- Which systems, platforms and applications are in place, inclusive of IT and Operational Technology (OT) systems
- Which changes, updates and upgrades are planned
- Which data and assets need to be protected
- Who runs which systems and applications
- Existing levels of security proficiency
- Existing security knowledge and skills gaps
- Projection of future security needs based on planned technology implementations, ongoing threat assessments and cybersecurity advancements
- Future strategic plans for the organization, including acquisitions and international expansion
- Potential external factors that may require time and investment from the security team, including new data privacy and protection regulations
- Crisis response capabilities and the need for a secure remote workforce
- Geographic distribution of systems and people

In assessing training needs, planners must take care to focus on the organization's needs – both immediate and long-term – and resist being pulled into irrelevant areas. Identify your organization's most pressing needs and plan the training curriculum accordingly. Since security is so broad, it's easy to lose sight of what is mission-critical to the organization and to employee development. This is why having a formal plan is essential.

If you leave this responsibility to your teams, they may focus on areas that interest and challenge them but do not necessarily align with what you need them to be learning. Further guidance on assessment and curriculum planning is available from the National Institute of Standards and Technology **(NIST) 800-50 Framework**. Guidance is also available from the **U.K.'s National Cyber Security Centre (NCSC)** and the **European Union's ENISA**.

2 Third-Party Training

Training that originates outside the organization typically is built around certification and certificate programs, and the development of specialized security skills. Industry standards training falls into three primary categories – vendor-specific, specialized skills like penetration testing and forensic investigations, and vendor-neutral certifications. Each has its rightful place in the program.

Vendor-specific certificates demonstrate proficiency in an individual vendor's products, systems, solutions and platforms. Earning vendor-focused certifications is recommended for team members who work with or specialize in the vendor's technology. A multitude of vendors offer training and certifications with the most common coming from industry stalwarts Microsoft, Cisco, Check Point, IBM, RSA, McAfee, Symantec and Fortinet.

A comprehensive curriculum also should include pathways to earning relevant vendor-neutral certifications built around standards developed by security professionals themselves. Vendor-neutral certifications prove the ability to implement, monitor and administer IT infrastructure using information security policies and procedures regardless of the vendor. Moreover, this vendor-agnostic approach is extremely valuable as it enables you to identify the information security leaders who understand cybersecurity strategy and who can design, develop and manage the overall security posture of your organization.

When pursuing vendor-specific training, understand that your employees are going to learn about that vendor's specific software and hardware, which is advantageous if those solutions are part of your defenses. A vendor-neutral course or training focuses on developing more comprehensive and wide-ranging skills that can be applied to multiple disciplines and across product sets.

Vendor-neutral certifications are available from various providers, including (ISC)², ISACA, SANS Institute, EC-Council, CIW, Global Information Assurance Certification (GIAC) and CompTIA. **(ISC)² offers a full complement** of certifications, including some of the most sought-after and respected in the industry.

3 Internal Training

A comprehensive cybersecurity curriculum should include internal training components as well. To add to the knowledge gained through third-party programs, cybersecurity and IT security professionals should have opportunities to learn from their colleagues and senior team members who are familiar with the organization's specific environments and practices.

Cybersecurity professionals may learn from senior team members in various ways:

- On-the-job learning with guidance from senior peers
- Manuals and documentation on the organization's systems, configurations and security policies and procedures
- Documentation of team member roles and responsibilities
- One-on-one sessions and classroom instruction
- Cross-training to round out the expertise of cybersecurity team members
- Mentoring programs

Challenge even your most experienced team members to share their knowledge and present to their peers. This not only facilitates more knowledge sharing but helps hone communications skills among your team.

The training officer, or team in charge of training, should identify internal experts to impart knowledge on specific areas, from endpoint protection to database security and network security to threat analysis, risk assessment, auditing and incident response.

Knowledge Transfer

Internal training also can serve the purpose of cross-pollinating knowledge in the cybersecurity team. For instance, firewall and endpoint security experts may teach penetration testers and threat analysts about their functions and responsibilities, and vice versa. This should not be an attempt to teach everyone everything. Rather, the goal is to share foundational knowledge to develop a well-rounded, cohesive team. Ultimately, this team may respond faster to incidents because it works better together, understanding the roles each team member has day-to-day and in a crisis.

Cross-pollination and more open communication also help with problem solving; someone with fresh eyes may view an issue from a different angle and suggest new solutions. In addition, the practice prepares the cybersecurity team for future changes, making it easier to assign team members to newly vacated or created positions

Mentoring

Mentor programs benefit individuals with skills development while elevating the entire cybersecurity team. To set up mentoring relationships, identify senior members who have the enthusiasm and aptitude to teach others. Pair them with less-experienced colleagues who are studying for certifications, looking to round out their skills or need to learn about specific areas of cybersecurity. Successful mentoring programs contribute to participants' career advancement while building rapport among team members.

4 Industry Conferences and Events

Industry events provide a wealth of knowledge and information to cybersecurity professionals. In addition to general sessions about industry trends and technology advancements, some events and conferences include sessions that fit into specific certification curricula, providing opportunities for individuals to advance their studies.

Identify which members should attend which events and decide with them what sessions are "must attend." To foster enthusiasm and creativity, make room in conference schedules for individuals to choose seminars and sessions that specifically interest them. Travel to a conference also is viewed as your investment and trust in your team members. Many will appreciate the time away from the office to learn and will often return to enthusiastically share what they learned with the broader team.

5 Training Delivery

Different individuals learn in different ways; some prefer self-paced study with a strong emphasis on online courses and materials, while others thrive in traditional classroom settings. Whenever possible, try to match delivery methods that best suit individual learning styles and the material to be learned. Whether vendor-specific or neutral, education and certification programs typically include one or more training methods, including self-paced online sessions, virtual classrooms and onsite sessions. Some individuals also may benefit from participating in cybersecurity labs as well as the virtual training environments of cyber ranges. Seek out these alternatives and evaluate them for your program's needs.

6 Technology Advances

One of the greatest challenges cybersecurity professionals face is the relentless pace of technology evolution. It is one of the main reasons ongoing education and skills development is so critical to keeping cybersecurity environments up to date. Vendor-neutral certifications are designed to ensure cybersecurity workers stay current with technology by learning practices, procedures and programs that focus on technologies as opposed to specific vendor products. However, ensuring that systems are kept current also makes it necessary to keep up with the vendors who make them.

Security vendors typically are good about communicating changes, updates and plans for new technologies. To ensure team members keep up with technology changes:

- Identify which team members are affected
- Plan training/skills updates accordingly
- Maintain close ties with your vendor reps and/or solution providers
- Determine if you should assign "ownership" of specific vendors to team members, so they are responsible for staying ahead of all changes to your security solution stack

Training and Certifications

Cybersecurity training is a multifaceted endeavor, and certifications are an essential part of the curriculum. Certifications demonstrate proficiency in different areas of security, providing demonstrable value to the enterprise. Having certified professionals builds confidence that an organization has a knowledgeable cybersecurity team with the necessary skills to create and maintain a robust security culture.

A strong security culture is key to minimizing security incidents and knowing exactly how to react if one occurs. Implementing a formal training and certification program helps attract and retain top talent, while demonstrating the operational value and investment in cybersecurity by the organization. When the program is fully endorsed by leadership and receives proper funding, cybersecurity professionals feel supported and appreciated. As such, they are more likely to stay with an organization for the long term because they see a pathway to progress in their career.

Cybersecurity training programs also build confidence – from the C-Suite to the board room to your customers – because it helps an organization demonstrate it has the controls and skills in place to address cyber threats. Today, customers and shareholders are willing to accept that breaches happen; however, if you fail to respond appropriately and adequately, you will lose their confidence. Invest in training your team. Invest in certifications to prove your team has what it takes.

Funding Certifications

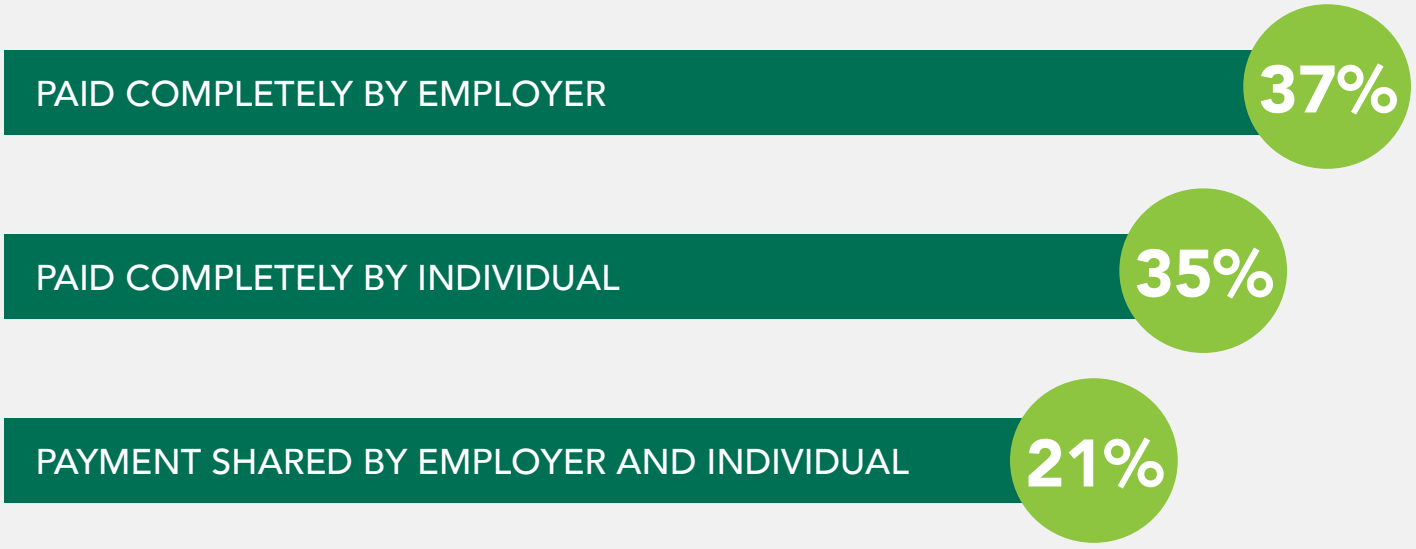
Training and education are an ongoing endeavor. If cyber threats continue to evolve – and they will – cybersecurity workers must evolve with them in order to remain effective. To ensure members of your security team acquire the knowledge they need, they need to show proof of learning. That is where certification is crucial. By earning certifications, team members demonstrate their proficiency and validate their expertise.

The question of whether employers or employees should pay for cybersecurity certifications has long been a subject of debate. Cybersecurity professionals consider the cost of certifications as the biggest hindrance to their career paths, according to (ISC)^2 research.

Employers often hesitate to fund cybersecurity team members' certifications for fear they will leave after becoming certified. As Sir Richard Branson once famously replied when someone asked him how he would feel if he trained his employees and they left his company, "What if I don't train them and they stay?"

Understandably, employers want a return on their investment. Yet, having an experienced, skilled cybersecurity team has significant value, and it's important to remember the ultimate goal is to defend against cyberattacks that can incur significant losses and damage a company's reputation.

Some employers absorb the full costs of education, while others leave it to employees to pay. Here is the breakdown of payments by employers vs. individuals, according to (ISC)^2's 2019 Cybersecurity Workforce Study:



Not all employers have the resources to fully fund their cybersecurity team members' certifications, but those that can should seriously consider it for the following reasons:

- Attract, motivate and retain top talent
- Lower costs of recruitment to fill vacancies
- Solidify career paths for team members
- Show support and appreciation for team members
- Help set security as a priority for the organization and create a strong culture of security
- Solidify the organization's defenses against cyber threats now and in the future
- Demonstrate the success of your cybersecurity training program

Although it may seem expensive to fund employee certifications, doing so can help prevent the much larger costs of a cyberattack. The better trained your cybersecurity team is, the more likely it is to prevent a debilitating cyberattack.

Evaluation

Any program worth implementing should be measured for effectiveness, and that includes training and education. Tracking the progress of cybersecurity team members' training activities helps create an understanding of the team's proficiency levels. The training officer, or cybersecurity training team, should set goals and review metrics accordingly. Here are some examples of metrics:

- Course completions
- Certifications earned
- Time spent by individuals on training activities
- Number of attempts to pass tests

Consider making the metrics available to supervisors to compare them against individuals' performance based on the supervisors' own observations. To verify proficiency, schedule periodic benchmarking and interviews with individuals to assess their skill levels. When doing performance reviews, education achievements and certification completions should be included in the overall assessment of each employee.

Ensuring Training Effectiveness

Evaluating individuals on their training achievements is one way to assess the effectiveness of an organization's training program, but the program itself should also be evaluated periodically. Without an evaluation mechanism, an organization may overlook gaps and opportunities for improvement. Here are some ways to assess program effectiveness:

- Evaluation forms filled out by individuals and their managers
- Surveys
- Benchmarking
- Interviews with individuals and managers
- Independent observations

> Assessment of learning is difficult and even intimidating. Activities such as Show-and-Tells or Lunch-and-Learn presentations delivered by staff can go a long way in helping you assess what was learned, as well as enhance team chemistry and communications skills.

Information compiled through these methods should help identify areas needing improvement. The need for periodic changes and improvements is a given. Remember, a cybersecurity education and training program needs to support these tenets:

1. Security is an obligation that requires education of cybersecurity professionals.
2. Evolving technology and changing threat landscapes necessitate a long-term commitment to cybersecurity.
3. A process should be in place to measure the effectiveness of cybersecurity skills development.

To satisfy these principles, the program must evolve. The better the cybersecurity education and training program can absorb changing requirements and realities, the better protected your organization becomes.

Plan Implementation and Recommendations

Part of the plan is to determine how much of your time should go into developing the curriculum, creating a training schedule for your team, staggering training sessions and obligations to avoid interference with day-to-day responsibilities, and tracking the progress of individuals and the team as a whole.

To ensure best results, consider building in incentives for reaching training milestones in the form of bonuses, celebrations, company announcements – or, in cases where major milestones are achieved – salary adjustments. Also consider setting annual KPIs and include them in yearly team performance reports and individual evaluations.

Distribute the plan to all members of the cybersecurity team, accompanied by a memo on recommended training for each individual and the organization's expectations for when to complete the training. Here is a list of recommendations to follow in preparing and distributing your plan:

1. Conduct an assessment of all existing security controls, protocols and policies currently in place to identify gaps and areas needing improvement.
2. Conduct an assessment of all systems, platforms and applications currently in place to ensure the training curriculum maps to your environment.
3. Determine who should be trained, and what levels of training each individual needs.
4. Assign a training officer who is responsible for managing the program and tracking the progress of each individual.
5. Build the program to meet specific organization needs by leveraging industry standards training combined with internal training tailored to your specific environment.
6. Engage learners in planning the curriculum and allow some leeway in the program for areas that interest them without losing sight of overall critical needs.
7. Set program goals and KPIs for the team, and specific milestones and incentives for individual learners.

Conclusion

The objective of this guide is to help you create a cybersecurity training plan that maps to your organization's specific needs. We've given you the blueprint, and now it's time for you to start developing your plan. Challenge your team. Educate your team. The investment in time and money you make today will better prepare your organization for tomorrow's threats.

For more information, visit **isc2.org** or contact our team for a consult today:

Americas
+1 866 331 4722 ext. 2
training@isc2.org

Europe, Middle East and Africa
+44 203 960 7804
info-emea@isc2.org

Asia-Pacific
+852 2850 6951
Japan: +81 3 5322 2837
China: +86 10 58732896
isc2asia@isc2.org