OFFENSIVE security

How to Identify the Cybersecurity Skills Needed in the Technical Teams in Your Organization

Author: Heather Monthie, PhD

TABLE OF CONTENTS

BRIEF

To protect your organization from potential information security threats, you must understand the cybersecurity skills gaps in your Information Technology (IT) and Information Security (InfoSec) teams. Cybersecurity skills gaps can affect your organization in many ways. By identifying the gaps, you can make a plan for skills acquisition to close the gap and better protect your company. If you know the skills needed on your technical teams and prioritize them by job role, you can ensure that your team has the skills necessary to combat cyber threats. This white paper is the first in a series on best practices to develop internal cybersecurity talent in your technical teams, such as IT, Information Security, DevOps, or Engineering. In this paper, these teams are collectively referred to as “technical teams.”

HOW TO IDENTIFY THE CYBERSECURITY SKILLS NEEDED IN THE TECHNICAL TEAMS IN YOUR ORGANIZATION

This paper is the first in a series to help human resources and hiring managers identify cybersecurity skills needed among the technical teams within an organization. By understanding the different areas of cybersecurity and the corresponding skills required for each, you can begin to map out the gaps in your organization's technical teams. Cybersecurity is a complex field that covers various topics, from network security to incident response. It can be challenging to identify which specific skills your technical teams need. However, by understanding the different types of cybersecurity skills and the tasks, you can determine which skills are needed on your teams.

It can be challenging to identify which specific skills your technical teams need.

The steps to identify required cybersecurity skills on technical teams are:

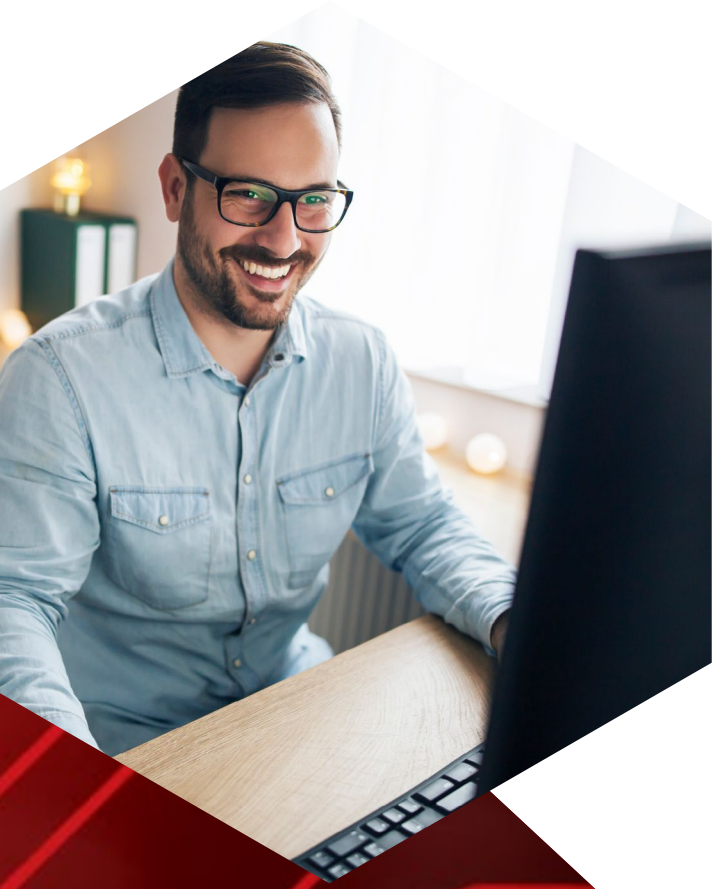
1. Build a cybersecurity competency model by job role that indicates the required skill and the associated proficiency level. The model should include skills currently needed and skills needed for the future.

2. Evaluate and measure the cybersecurity competencies of the individuals on your technical teams using the cybersecurity competency model.

3. Identify areas where your technical team has strong cybersecurity skills and areas where there are skills gaps or skills silos.

4. Develop a strategy and track the effectiveness of your efforts to close the cybersecurity skills gaps on your technical teams.

WHY IS IT IMPORTANT TO UNDERSTAND THE CYBERSECURITY SKILLS GAPS ON YOUR TECHNICAL TEAMS?



Before we get into the methods for detecting skills shortages on your technical teams, let's first understand why this is significant when it comes to cybersecurity in today's society.

There are many reasons why it is essential to understand the skills gaps in your technical teams. By understanding the skills needed on your teams, you can:

- Ensure that your team has the necessary skills to prevent, detect, and respond to cyber threats
- Ensure that your development teams have the necessary skills to develop secure software by design
- Reduce the impact of a cyber attack on your organization or the organizations that use your software products
- Reduce the risk of your organization or the organizations that use your software products being the victim of a cyber-attack

THE SOPHISTICATION AND COST OF CYBERSECURITY THREATS ARE INCREASING

In 2021, the average cost of a ransomware breach was $4.62 million, with an average cost per lost or stolen record of $180, a 20% increase from 2020, according to the 2021 IBM Cost of a Data Breach Report.[1]

In addition, the Cost of the Data Breach report found the top initial attack vectors in 2021 were:

20%
Compromised credentials

17%
Phishing

15%
Cloud Misconfiguration

14%
Vulnerabilities in Third-Party Software [2]

Business email compromises were responsible for the smallest overall number of attacks but had the highest average total cost of all attacks at $5.01 million per attack.[3]

[1,2,3]https://www.ibm.com/security/data-breach

As cloud misconfiguration is one of the most frequent initial attack vectors, proper training and education for your cloud engineers could help reduce the cyber risks associated with a cloud misconfiguration. According to the IBM Cost of a Data Breach Report, it took organizations an average of 252 days to identify and contain a breach in organizations in the mature stage of cloud modernization. Organizations in the early state of cloud modernization took an average of 329 days or nearly 11 months to identify and contain a breach. Organizations with a high level of cloud migration had an average cost of a breach of $5.12 million and $3.46 million for organizations with a low level of cloud migration.[4] With proper training on cloud security, your organization can be better prepared to prevent cloud breaches and detect and respond to a breach more quickly.

Vulnerabilities in third-party software continue to rise as a top initial attack vector. Integrating security in the development process (DevSecOps) was associated with a lower-than-average data breach cost.[5] Providing learning opportunities for your DevOps team in secure software development can help identify insecure code in several ways.

As a customer purchasing third-party software or creating requests for proposals (RFP) to create customized software, you may incorporate policies and/or procedures to identify software security issues in third-party applications. These policies may include a requirement for the software vendor to have appropriate secure development practices in place when responding to an RFP.

As a vendor responding to RFPs to create custom software or developing commercial software for resale, policies and procedures can be implemented to identify insecure development practices early in the software development lifecycle. In addition, processes should also be established to analyze the existing software that is currently in use by customers use to identify vulnerabilities and develop a remediation plan.

ORGANIZATIONS ARE AT A HIGHER RISK OF A CYBER ATTACK WITHOUT THE PROPER CYBERSECURITY SKILLS.

The 2019 IBM cost of a Data Breach Report showed that employee training was an effective cost mitigator when evaluating the cost of a data breach.[6] Without the necessary skills to protect your organization from a cyberattack, it takes longer to identify and contain a data breach. To protect your organization from potential information security threats, it is crucial to understand the skills gaps in your technical teams.

[4,5]https://www.ibm.com/security/data-breach
[6]https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.148238199.1762516747.1577395260-1128561362.1577395260

STEP 1 Build a Cybersecurity Competency Model By Job Role

One of the most effective approaches to reducing the level of cybersecurity risk for your organization is to train your staff on the cybersecurity skills they'll need for their job responsibilities. It takes time to evaluate every team member and create a training plan to increase their cybersecurity skills and is well worth the extra effort.

The first step is to build a customized cybersecurity competency model for each job role within your technical teams for your organization.

Competencies describe the knowledge, skills, and abilities (KSA) required to excel in a given position. A well-designed competency model identifies the necessary KSAs and the associated behaviors that indicate the progressive level of proficiency: beginner, intermediate, or advanced.

To identify any cybersecurity skills gaps you have on your team or gaps you may have in the future, it is essential that you understand the responsibilities and required cybersecurity skills of each job role on your team.

Step 1a. Identify the cybersecurity Knowledge, Skills, and Abilities required for an individual work role within your technical teams

The following sub-sections describe how to gather the necessary information and organize it into a cybersecurity competency model customized for your organization. These steps provide a framework for you to use internally. This framework is written so that an external consultant might work with your organization's Human Resources, CIO, CTO, or CISO to gather this information to build a competency model. As a manager, you can use this framework to develop your own competency model customized for your industry and organization. These steps are not mandatory and should be modified accordingly to your industry, organization, or individual teams.

Review Your Organization's Strategic Plan

The first place to identify specific cybersecurity skills is your organization's strategic plan. This document can help you identify the required skills over the upcoming years. If you are increasing your web applications, you need strong web application security skills. If your company is adopting an expanding cloud strategy, you may need to boost the security skills of your cloud team.

By understanding what your organization needs to achieve within the next few years, you'll be better able to figure out the cybersecurity skills needed to support and protect your company's future growth.

Review Existing Job Descriptions

Another resource to help you identify cybersecurity skills needed on your technical teams is to review existing job descriptions and highlight the specific security skills.

By going through this exercise, you will have a good idea of your technical team's cybersecurity skills and any existing gaps. You may also find that you are not requiring any cybersecurity skills and need to update existing job descriptions.

This whitepaper, **How to Write Effective Entry-Level Job Descriptions** may help you craft well-written cybersecurity job descriptions by providing some sample language.[7]

Individual Surveys or Interviews

After you have assessed your strategic plan and existing job descriptions, it is crucial to gain insight into what the individuals on your technical teams think is necessary to be successful in their job roles. One way to do this would be to have each individual on your technical team answer a survey or interview questions about the required cybersecurity skills to protect your organization.

Without the required cybersecurity knowledge, some team members may not be aware of the cybersecurity skills they'll need for their work responsibilities. Technical staff not on the security team may incorrectly assume that security is the security team's job. This exercise may also help you see the need to impart a "cybersecurity is everyone's job" culture.

Occupational Information Network (O*Net Online)

Organizations can leverage the existing information provided by O*Net Online, which offers occupational information from the US Department of Labor. The O*Net website offers a comprehensive database of occupation descriptions to help you identify the cybersecurity skills required for specific job roles. You can use this information as a starting point to define the security-related skills needed for particular job roles[8] in your organization.

[7] https://learn.offensive-security.com/free-job-descriptions-whitepaper
[8] https://www.onetonline.org/

Align to the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity

The National Initiative for Cybersecurity Education (NICE) created the Workforce Framework for Cybersecurity (often referred to as the NICE Framework) to help organizations identify, develop, and retain professionals with in-demand cybersecurity skills.[9] The skills you've identified in the exercises above can be aligned to the NICE Framework to create a customized competency model for your organization.

Using the National Initiative for Cybersecurity Careers and Studies (NICCS) website, you can identify specific job (work) roles that closely align with your organization. You can review the associated KSAs and choose those relevant to that particular work role.[10]

For example, suppose you are creating a cybersecurity competency model for a Software Developer in your organization. In that case, you can select the "Secure Software Assessor" work role to review the associated cybersecurity KSAs for that role. You can select the KSAs that are relevant to that role within your organization and industry.

Completed List of Cybersecurity Skills by Job Role

Once you've identified the skills needed for a particular job role, you can start a table listing the identified skills. This list is the starting point for developing a customized competency model for your organization.

For the purposes of this white paper, we'll use a software developer as an example to build a cybersecurity competency model. These example skills were derived from the NICE Framework using the "Secure Software Assessor"[11] work role. You may have more or fewer skills identified for your particular work role, and you may have different levels of software developers (I, II, III, IV). This is for informational purposes only to guide you through this process. Table 1 shows an example of what a list of cybersecurity skills for a software developer looks like.

Table 1. Identified Cybersecurity Skills

Identified Cybersecurity Skills (Software Developer)
Knowledge of secure coding techniques
Knowledge of Payment Card Industry (PCI) data security standards
Knowledge of penetration testing principles, tools, and techniques
Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems
Skill in designing countermeasures to identified security risks.
Develop threat model based on customer interviews and requirements
Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change

[9,10]https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework
[11]https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework/workroles?name=Secure+Software+Assessor&id=All

Step 1b. Prioritize the cybersecurity skills needed for that particular job role

Now, you may have a long list of cybersecurity skills for one particular job role within your organization, and the next step is to prioritize them by importance. Using this process, you can make sure that the cybersecurity skills needed on your technical teams are prioritized by importance and align with your organization's needs.

The skills should be prioritized on a defined scale. It's important to remember that nothing is the priority if every skill here is a top priority. A sample scale that may be used is Low, Medium, or High or even 1, 2, 3 if you prefer to quantify the level of importance.

In our example for the software developer, you use the list of cybersecurity skills and add a column to prioritize accordingly.

Table 2. Prioritized List of Cybersecurity Skills

Identified Cybersecurity Skills (Software Developer)	**Priority** (1= Low, 2 = Medium, 3 = High)
Knowledge of secure coding techniques	3
Knowledge of Payment Card Industry (PCI) data security standards	2
Knowledge of penetration testing principles, tools, and techniques	1
Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems	2
Skill in designing countermeasures to identified security risks.	3
Develop threat model based on customer interviews and requirements	2
Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change	3

Step 1c. Rate the Proficiency Level Required on a Defined Scale

The next step would be to rate the proficiency level required for each identified skill on a defined scale.

To create a well-defined scale, you can use NICE Workforce Framework for Cybersecurity as a starting point. Your organization could use this scale to define the skill level required. The NICE framework uses entry, intermediate, and advanced.

1 = entry | 2 = intermediate | 3 = advanced

The NICE Framework provides some guidance to standardize the scale.[12] Each of these items on the scale should be clearly defined for more objective measurement.

When you get to the point of evaluating individuals on your team, you may find that some individuals have no experience at all in that particular area, and some may be recognized experts outside of your organization. For more specificity, your organization could use a scale of 1-5. A 1 is no experience at all, and a 5 is an expert or authority on the topic and is well-known outside your organization for that particular skill.

This is a suggested scale that provides a detailed definition of each proficiency level.

Table 3. Proficiency Level Scale

1 = No Experience or Training	2 = Entry-level abilities	3 = Intermediate	4 = Advanced	5 = Expert
Individual has no prior exposure in training, education, or experience in the topic.	Individual has some exposure to the topic and is able to complete basic tasks on their own. Requires substantial support to complete more advanced tasks.	Individual has previous training, education, or experience in the topic and is able to complete more advanced tasks on their own.	Individual has significant work experience in the topic and is able to lead projects, communicate effectively on the topic, and is a top internal resource on the topic.	Individual is well-regarded in the industry outside of the organization for this topic, has given multiple presentation, written papers or books, or has patents related to this topic.

[12]https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework/workroles?name=Vulnerability%20Assessment%20Analyst

When you are completing your competency model, you can use this scale to determine where it is that you need the individuals on your team to be. Not all software developers need to be experts in threat modeling. This scale helps you identify clearly where you need the individuals on your team to be.

You may also have different proficiency levels based on the level of the software developer work role. For example, you may need to build a different competency model for Software Developer I, II, II, IV since you may need a level IV developer to be a 4 on PCI but a level I may be a 2.

The table below shows a completed cybersecurity competency model for a level II software developer. The proficiency level may look very different for a level IV software developer.

Table 4. Completed Cybersecurity Competency Model

Cybersecurity Competency Model (Software Developer II - EXAMPLE)		
Identified Cybersecurity Skills (Software Developer)	**Priority** (1= Low, 2 = Medium, 3 = High)	**Proficiency Level** (1 = No experience, 5 = Industry-recognized expert)
Knowledge of secure coding techniques	3	3
Knowledge of Payment Card Industry (PCI) data security standards	2	3
Knowledge of penetration testing principles, tools, and techniques.	1	2
Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	2	2
Skill in designing countermeasures to identified security risks.	3	3
Develop threat model based on customer interviews and requirements.	2	2
Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	3	3

STEP 2 Evaluate and measure the cybersecurity competencies of the individuals on your technical teams using the cybersecurity competency model.

Once you have identified the cybersecurity skills required for an individual job role, the next step is to evaluate and measure the proficiency of each individual on your technical teams. You can identify individual skillsets through a few types of evaluations:

- employee self-assessments
- surveys or interviews
- cybersecurity skills assessments
- observation with a scoring rubric
- performance reviews
- work products

Following this procedure will help you obtain a clear view of the cybersecurity skill gap and what actions need to be taken. This involves determining which job functions require more training, where resources should be allocated for growth, and how to prepare proactively for future threats.

Employee Self Assessments

Employee self-assessments are one method to measure skillsets for individuals on your team. Using the list of cybersecurity skills you've created and the scale to define the proficiency level, employees can assess their skills and rate their competence levels for each. Self-assessments should only be one part of the process used to identify skills gaps on your team, as there is a growing body of research that shows evidence that men overrate their skills and women underrate their skills.[13] [14]

Surveys or Interviews

Having a conversation with individual employees to gather information about their skillset is another way to measure your team's current skillsets. This process can provide valuable insight into the current skill level of individuals on your team and job roles within your organization.

Surveys can be completed online anytime by all team members and can provide valuable data to identify skills gaps.

Interviews are 1x1 conversations that allow you to probe deeper into areas where skill gaps may exist.

To create effective surveys or interview questions, try asking questions like:

- What is your familiarity with all top priority skills?
- Do you consider yourself an authority or expert on any of these skills?
- Is this a topic you could teach someone learning for the first time?
- Do you have any experience with these types of skills?
- What are the most desirable skills you wish to obtain?

These are questions managers can use to get a clear picture of their technical staff's current cybersecurity competence level.

[13]Nowell, C., & Alston, R. M. (2007). I thought I got an A! Overconfidence across the economics curriculum. The Journal of Economic Education, 38(2), 131-142.
[14]Admiraal, W., Huisman, B., & Pilli, O. (2015). Assessment in massive open online courses. Electronic Journal of E-learning, 13(4), pp207-216.

Cybersecurity Skills Assessments

Skills assessments are another great way to identify the skills needed on your information security team. You can perform a skills assessment with individuals on your team by either asking individuals to complete a skills checklist or using a pre-designed hands-on skills assessment.

For a more effective assessment, it may be helpful to create questions around scenarios or examples. This provides more real-world context for the skills assessment and helps ensure it evaluates the right cybersecurity skill.

Performance Reviews

Reviewing previous performance reviews is another method of keeping track of individual cybersecurity skills and growth. You may or may not have access to prior performance reviews, and if you do, you can look for any statements of professional development goals.

In the future, adding cybersecurity-related professional development goals in the performance review process helps clarify the individual employee on what areas to focus on developing.

When developing performance reviews, consider including questions like:

- What are your current top 1-3 goals for growing your cybersecurity skills?
- What areas in cybersecurity do you consider to be your greatest strength?
- What have you struggled with so far in achieving your goals?

How would you rate yourself on a scale of 1 - 10 in each skill area, based on the list of skills needed for your job function?

As good management practice, performance reviews shouldn't have any surprising information for the individual. The performance review should be a formality of defining professional goals for the following year.

Work products

Evaluating work products is another way to assess the skills of your technical team.

This can be done by collecting work product samples from each team member. For example, you can ask employees to submit an incident report or presentation they have completed for a previous customer engagement. This will give you a clear picture of how skilled they are in their job function and what kind of work they create.

By closely reviewing all of these resources, you can identify gaps in skill development on your infosec team and make a plan to ensure that every member is knowledgeable and prepared for any potential threats to your organization or customers.

Since there can be some subjectivity in evaluating the quality of a work product, you can use the scoring rubric you created to be more objective in your analysis.

Assess and Measure with a Scoring Rubric

Managers can assess employees using a well-designed scoring rubric. This procedure presumes that the managers are knowledgeable on the subject area and have the skills to evaluate the employees' abilities properly.

A rubric is a tool that indicates how an employee's work products should be evaluated. They're used when there isn't necessarily a right or wrong response, and the quality of work needs to be measured. Skills measurement becomes more objective and consistent with a well-designed scoring rubric.[15] [16]

Suppose you have already created a competency model that defines the level of proficiency needed for a particular job role. In that case, you can add an additional column to rate the current proficiency level using the same scale to develop a rubric.

The example completed Cybersecurity Competency Scoring Rubric below shows an example of one individual's cybersecurity skillsets. Using this completed rubric, you can easily identify a skills gap that one individual has. In this example, the individual is expected to be at a level 3 for knowledge of secure coding techniques but is currently at a 1. Proficiency in Payment Card Industry standards is acceptable for this individual. From this evaluation, a manager and employee can work together to develop a professional development plan to upskill the employee in the necessary cybersecurity skills for the position to get them to the required proficiency level.

[15]NBrookhart, S. M. (1999). The Art and Science of Classroom Assessment. The Missing Part of Pedagogy. ASHE-ERIC Higher Education Report, Volume 27, Number 1. ERIC Clearinghouse on Higher Education, One Dupont Circle, Suite 630, Washington, DC 20036-1183.
[16]Moskal, B. M. (2000). Scoring rubrics: What, when and how?. Practical Assessment, Research, and Evaluation, 7(1), 3.

Table 5. Cybersecurity Competency Scoring Rubric - Individual

Cybersecurity Competency Model (Software Developer II - EXAMPLE) – Individual)			
Identified Cybersecurity Skills (Software Developer)	**Priority** (1= Low, 2 = Medium, 3 = High)	**Expected Proficiency Level** (See Table 3 for definitions)	**Current Proficiency Level** (1 = No experience, 5 = Industry-recognized expert)
Knowledge of secure coding techniques	3	3	3
Knowledge of Payment Card Industry (PCI) data security standards	2	3	3
Knowledge of penetration testing principles, tools, and techniques.	1	2	2
Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	2	2	2
Skill in designing countermeasures to identified security risks.	3	3	3
Develop threat model based on customer interviews and requirements.	2	2	2

STEP 3 Identify areas where your technical team has strong cybersecurity skills and areas where there are skills gaps or skills silos.

Once you have completed the individual competency models for all individuals on your team, you can look at your team as a whole to identify any skills gaps and/or skills silos.

Table 6. Cybersecurity Competency Scoring Rubric - Team

Cybersecurity Competency Model (Software Developer II - EXAMPLE) – Team)					
Identified Cybersecurity Skills (Software Developer)	**Priority** (1= Low, 2 = Medium, 3 = High)	**Expected Proficiency Level** 1 = No experience, 5 = Industry-recognized expert)	**Employee A**	**Employee B**	**Employee C**
Knowledge of secure coding techniques	3	3	3	3	3
Knowledge of Payment Card Industry (PCI) data security standards	3	2	3	3	3
Knowledge of penetration testing principles, tools, and techniques.	2	1	2	2	2
Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	2	2	2	2	2
Skill in designing countermeasures to identified security risks.	3	3	3	3	3
Develop threat model based on customer interviews and requirements.	2	2	2	2	2

One of the most important things you can do as a technical manager is to evaluate the skills gaps and identify skills silos at the team level. By identifying and addressing these gaps and silos, you can help improve your team's efficiency and effectiveness.

Skills Silos

In this example of a software developer, we have identified a potential skill silo for knowledge of PCI standards. It has been identified as a top priority for the team, yet only one developer has any knowledge of the topic. As a result of completing these activities, you have identified a skill silo that puts your team (and organization) at risk.

Skills Gaps

In addition to identifying skills silos, you may have identified an area where you require some cybersecurity expertise but no one on the team has the skills at the skill level you've identified. You have identified a cybersecurity skills gap on your team. In the example in table 6, we have identified that knowledge of penetration testing techniques is required yet no one on the team has this knowledge. This exercise has helped to identify a skills gap that puts your team (and organization) at risk.

To build a strong technical team, it is essential to have a diverse group with technical, cybersecurity, and professional skills. This will help ensure that your team can handle any situation that arises. It is also important to remember that not every team member needs to be an expert or advanced in every area of cybersecurity.

By evaluating the skills gaps and skills silos at the team level, you can make more informed decisions about training and development for your team members. This will help you prioritize the skills they need and better equip them to protect your organization against potential cyber threats.

Putting it all together

In the example above, we have identified that only one software developer on the team has the expected proficiency level for PCI standards. We have identified a skills silo and in order to mitigate the risk associated with only having one person on the team well-versed in PCI standards, it is imperative to either add additional people to the team with the expected proficiency level or upskill existing employees to get them to the expected proficiency level.

In addition to the identified skills silo, a skills gap was identified in "knowledge of secure coding techniques" where the expected proficiency level is a 3, yet all the software developers only have a level 1 proficiency. Managers and employees can work together to develop a professional development plan to upskill the employees to reach the expected proficiency level.

Skills Management Software

Skills management software can also help identify the cybersecurity skills gap in your technical teams. This software allows you to input all the relevant job functions and prioritize each skill by its level of importance. The software then calculates a Demand or Need score for each skill, giving you a clear picture of the overall demand for that particular skill. Several options are available, but this is out of scope for this paper.

STEP 4 Develop a skills acquisition strategy and track the effectiveness of your efforts to close the cybersecurity skills gaps on your technical teams.

There are two strategies managers can use to close cybersecurity skills gaps on their teams:

- hire new team members
- train existing team members.

These two methods for skills acquisition is essential for closing the cybersecurity skills gap. Hiring new team members can be expensive for acquiring new cybersecurity skills on your technical teams, yet it is very effective if you want to build out and grow your team.

This paper addresses methods for how to train existing team members. For information on hiring new team members, see the paper **"Writing Effective Entry-Level Job Descriptions."**

Cybersecurity Skills Training Strategy

Cybersecurity skills training can be done in person, online, or self-study and can cover a range of topics such as cloud security, penetration testing, and incident response. Offering training and education benefits to employees can also attract and retain top cybersecurity talent since at least 37% of the global workforce desires a position with a company that provides additional training.

If an organization does not provide additional training and education opportunities for its employees to acquire essential cybersecurity skills, the lack of training may lead to the failure of the team to defend against cyber attacks.

Given the rise in the number and complexity of cyberattacks, it's critical to have a well-equipped staff knowledgeable about how to defend your business. Some of the most common methods for implementing a training and education program for cybersecurity skills acquisition include:

- instructor-led training (virtual or face to face)
- self-paced online learning
- peer learning
- webinars
- mentor programs
- job shadowing/job sharing

Instructor-Led Training (Virtual or Face-to-Face)

There are many online and in-person cybersecurity training programs to choose from. Instructor-led training sessions are a great way to improve the cybersecurity skills of your team members, regardless of their level of knowledge. Instructors may deliver virtual or face-to-face classes that teach the necessary cybersecurity skills for a specific job role within your company.

Self-Paced Online Learning

There are a variety of cybersecurity training courses accessible online that enable employees to learn at their own pace and when it is convenient for them. This is useful for individuals who require more flexibility while studying materials or completing coursework. Self-paced online learning can be a more affordable alternative to face-to-face instructor-led training since no travel costs are involved.

Peer Learning

This is a fantastic method to acquire knowledge and information about topics unique to your business. Furthermore, it allows employees to share ideas and best practices. You may collaborate across functional areas to establish peer learning opportunities beneficial for individuals at all proficiency levels. Peer learning includes mentor programs, employee-led webinars, and job shadowing.

Employee-Led Webinars

Employee-led webinars or Lunch-N-Learns are informal training where an employee gives a presentation on a specific topic to their colleagues. This is an excellent way to cross-train on any cybersecurity skills gaps or silos you have identified. Colleagues can also share best practices and learn from each other's experiences.

Mentor Programs

Mentor programs are formal programs where employees more experienced in a particular topic share what they know to help less-experienced employees develop their skills in this area. It is important to note that junior employees may have more experience with a particular topic and can help more seasoned employees learn a new cybersecurity skill. Peer mentoring has been shown to be an effective training approach to acquiring in-demand cybersecurity skills.

Job Shadowing / Job Sharing

Job shadowing is a training approach that allows employees to watch someone else do their job for some time. This is an excellent way to learn the skills needed for a specific role and understand the day-to-day responsibilities of that role. Job sharing is when two employees split the duties of a single job role. This is a great way to learn about different aspects of a single job role and gain experience in multiple areas.

By understanding the skills gaps on your information security team, you can make a plan for skills acquisition to close the gap and better protect your company. Identifying the gaps allows you to prioritize the skills needed by the job role and implement a training and education program that meets the needs of your employees. By using various training methods, such as instructor-led training, self-paced online learning, peer learning, webinars, mentor programs, and job shadowing, you can ensure that your employees have the skills necessary to combat any threat.

Measuring the Effectiveness of Cybersecurity Skills Training

One of the most important things that you can do as a manager for your cybersecurity skills training strategy is to measure the success of your skills acquisition plan. Measuring the effectiveness of your plan can ensure that your team is making progress and that the plan has a positive impact on your organization.

There are many different ways to measure the success of your skills gap closure plan, but some of the most critical indicators include:

- The number of team members who have acquired new skills
- The level of skill development among team members
- The number of threats that have been averted due to the improved skills of the team

Some of these are easier to quantify than others. You may need to use a mix of qualitative and quantitative data to get a complete view of the success of your skills training program.

The number of team members who have acquired new skills

The number of team members who developed new skills over your skills acquisition plan is a good indicator of its effectiveness. This will reveal how many individuals on your team are closing skill gaps and enhancing their performance.

The level of skill development among team members

Another way to measure the success of your skills acquisition plan is to determine the level of skill development among your team members. You can re-visit the steps you completed to create the custom competency model and re-evaluate the individuals on your team. By revisiting these steps, you may identify that you had five individuals on your team move from “beginner” to “intermediate” proficiency levels in cloud security.

The number of threats that have been averted due to the improved skills of the team

Another way to assess the success of your skills gap closure plan is to see how many security incidents have been prevented due to better training. While this number will not always tell you whether or not your strategy is working, it may help you determine which initiatives (such as training and development) should be prioritized first and which ones require more attention.

CONCLUSION

To protect your organization from potential cybersecurity threats, it is crucial to understand your technical teams' cybersecurity skills gaps and silos. By identifying the gaps and silos, you can make a plan for skills acquisition to protect your company better.

Cybersecurity skill gaps and silos can affect your organization in many ways. However, by understanding the cybersecurity skills needed on your technical teams and prioritizing them by job role, you can make sure that your team has the skills necessary to combat any threat. Once any skills gaps and silos have been identified, it is essential to create a skills acquisition plan and measure the effectiveness of implementing the plan. Measuring the success of your strategy makes sure that your team is moving forward, that the plan has a beneficial impact on your company, and that any necessary changes are made as soon as possible.

Please contact **sales@offensive-security.com** to discuss how we can assist with your training needs for your technical teams, such as IT, Information Security, DevOps, or Engineering.

ABOUT OFFENSIVE SECURITY

Offensive Security is the world's leading provider of hands-on cybersecurity training and certifications for the cybersecurity professionals. Created by the community for the community, Offensive Security's one-of-a-kind mix of practical, hands-on training and certification programs, virtual labs and open source projects provide practitioners with the highly-desired offensive and defensive skills required to advance their careers and better protect their organizations. Offensive Security is committed to funding and growing Kali Linux, the leading operating system for penetration testing, ethical hacking and network security assessments.

For more information, visit
www.offensive-security.com
and follow @offsectraining and @kalilinux