The challenge of addressing the skill gap in IT and security skills gap

The challenges presented by COVID-19 only validated what security professionals have long been stressing when it comes to security best practices. With the remote workforce continuing to grow, securing devices that were not previously considered from a security perspective is more important than ever before. However, we must not forget the most important security device of all: people.

As important as secure devices are, they're only as good as their human operators. More often than not, organizations either overlook this aspect of security or actively ignore it. In order to increase their security posture, organizations must understand that there's currently a massive gap between the skills they currently have and the skills they need moving forward. As such, a recent survey of more than 800 industry professionals of varying experience dove headfirst into assessing and addressing skills gap challenges.

Acknowledgement of the cybersecurity skills issue

The first step to solving any problem is to acknowledge that it exists. In years past, organizations big and small just waved their hand when it came to security issues, believing they either had enough resources or it didn't apply to their business. According to the aforementioned survey, nearly three out of four professionals routinely encounter skill gaps on their current teams and two out of three also recognize that these gaps limit their teams' effectiveness. So, why is there still such a divide between the supply of open positions and demand for security and IT professionals?

For starters, it's hard for organizational leaders to upskill their employees when they're so far underwater with current challenges, including the increasing cyber-attacks on the remote workforce. This is particularly true for organizations with limited resources. This challenge, coupled with the fact that most employees tend to wait for permission versus taking initiative themselves, often results in security slipping through the cracks until it's too late to address.

Budgetary constraints

Skills gap challenges also persist because there's been a lack of organizational funding for security training. Referencing the survey from earlier, more than a third of respondents admitted that their respective organization either decreased their training budgets or had no training budget at all. Another third also cited cost as one of the primary barriers preventing security and IT professionals from getting the skills development training they need. But at the same time, it's extremely difficult to prove the value of security unless an organization has suffered a data breach or cyber-attack.

On-premises vs. remote workers

Properly addressing these issues is much more challenging due to the ongoing pandemic forcing employees, departments, and even entire organizations to conduct work remotely. Even though many business processes aren't dramatically affected by this shift, training and learning have completely evolved.

Early on, security and IT teams were stretched so thin fighting traditional fires as organizations adopted the fully remote work model that they were forced to delay upskilling efforts on long-term issues. Also, prior to the work-from-home era, security and IT training often happened in a physical group setting. This allowed team members to "whiteboard" or interact in person to promote engagement. Now, this is nearly impossible to replicate on video conferencing platforms. Body language is impossible to read, and "Zoom fatigue" is affecting everyone.

Vetting, hiring and onboarding

Another challenge that has compounded the skills gap has been the failure of organizations to properly vet applicants and adequately onboard them. The biggest pain point for hiring and onboarding security positions is vetting the vast number of different skills new employees might have, especially when organizations often don't know the correct skills to look for in applicants. Also, once a new hire is finally onboarded, the provisioning of access for tools to perform job functions is time consuming and involves jumping through unnecessary hoops. Not surprisingly, the it is discovered that almost half of organizations do not confirm new hire skills for specific roles, and two out of five rarely or never assess the skills of newly onboarded team members.

Finding the right prescription

Assessing and addressing the security and IT skills gap is much different today than it was just six or even three months ago. Going an entire week without seeing a fellow colleague or being solely focused on fixing old problems is going to have a significant impact on almost everyone at an organization. But everything isn't all doom and gloom. There's also a handful of quick and easy fixes that organizations can implement in order to give them the opportunity to pursue long-term solutions.

Companies are desperate for cybersecurity workers—more than 700K positions need to be filled

The need for cybersecurity professionals has been growing rapidly, even faster than companies can hire—and that demand is expected to continue. The number of unfilled cybersecurity jobs worldwide grew 350% between 2013 and 2021, in India alone it grew from 1 million to 3.5 million. There are 515,000 jobs yet to be filled as of November 2021. It is only because potential workers have not acquired required skills to handle Cyber security jobs.

One contributing factor to the talent shortage is that there aren’t enough professionals who have the credentials necessary (whether it’s a master’s degree in cybersecurity or another certificate program) to get hired.

Why it’s difficult to fill cybersecurity roles

While companies are looking to hire cybersecurity professionals in droves, the industry often requires that workers have certain credentials or certifications on top of education requirements. An example is a CISSP certification, which is required for many top-level cybersecurity roles that are in high demand—and have high-paying salaries, to the tune of about $120,000. Even if you have an undergrad or graduate degree in cybersecurity, computer science, or an adjacent field, that may not be enough to land certain jobs in the industry.

Breaking into cybersecurity

Undergraduate and graduate degree programs focused on cybersecurity continue to be a popular route for entering the industry. Companies are also providing in-house training for current employees who are looking to enter the cybersecurity workforce.

If you're already in a technical role—but not specifically cybersecurity—add cybersecurity into your current role. This could involve learning a new skill set through shorter-term training opportunities or boot camps.

Another way to get your feet wet is to prepare to take one of the entry-level cybersecurity certification tests, such as Security Plus.

Cybersecurity specialists are a growing sector of IT job postings. More and more businesses are devoting resources to cybersecurity, which includes protecting network and data from hackers, viruses, and more. As technology enables more connected devices and makes it easier for people to work remotely as freelancers or contractors, the need for advanced and complex security measures has increased. No longer are all employees on site connected to hardware and all being served by data processed through a local server.

Having new technology in place, a more spread out employee base, and access to more data than ever before means that companies have to be more proactive in protecting their company data, employee devices, networks, and other cyber resources. This is where the role of a cyber security specialist comes in. Companies need dedicated employees who are qualified to handle the technology and mitigate the risk.

Cyber Security Education Requirements

Most cyber security specialists have earned a bachelor's degree level of education. Since cyber security specific jobs are fairly new, many current cyber security experts started in other IT careers with a degree in computer science. Other degree options have become available through programs and universities all over the country, including specific degrees in cybersecurity, management information systems, computer forensics and digital investigations, and others at both the bachelor's and master's level.

Cyber Security Specialist Job Description

Cyber security specialists are usually responsible for:

- Granting VPN access to remote workers
- Monitoring for malware
- Diagnosing data vulnerability
- Making recommendations for hardware and software to enhance security
- Regulating use of data, only allowing access of certain files to certain employees
- Designing firewalls
- Running data usage reports
- Training staff on current security issues
- Helping HR train other departments on safely handling data

The specific job responsibilities of a cyber security specialist will depend on the company they work for, but these duties are often seen in the role.

Cyber Security Qualifications

In addition to an education focused on computing, data, and security, cyber security experts usually also:

- Are good problem solvers and enjoy puzzles
- Have project management skills
- Have a flexible attitude
- Can work independently and in groups
- Are trustworthy

Education is a huge part of being qualified for a cyber security job, but it’s important to have other intangible skills that contribute to their qualifications.
Cyber Security Specialist Certification

Some cyber security specialists will go beyond a university education and acquire additional training and certifications. Some cyber security specialist specific certifications include:

- Cisco Cybersecurity Certificate
- Master’s Degree in Information Assurance and Cybersecurity
- CompTIA Penetration Tester Certification
- Certified Information Systems Auditor Certification
- Certified Information Security Manager Certification
- Certified Information Systems Security Professional

Having additional certifications and education can be a benefit when it comes to getting a promotion or heading up a new team or department.

Having a resident cyber security specialist is becoming a priority for many businesses. Knowing that the qualifications of someone with that job responsibility, as well as what they should be responsible for in that role, is key for finding the right fit for your company.