FEATURE

# Future-Proofing a Career in Cybersecurity

## The Skills Gap

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

***https://bit.ly/2Cq2x23***

日本語版も入手可能

***www.isaca.org/currentissue***

Help wanted! Millions of security professionals needed to help fill critical roles required to protect the world's infrastructure, data and people—apply now!

Security professionals are in high demand, but the challenge is that there are not enough qualified employees to fill open enterprise requisitions. For confirmation, it is worth taking a look at ISACA's report *State of Cybersecurity 2018*.[1] Part 1 of the report outlines workforce development and mentions that 59 percent of the respondents to the survey upon which the report is based have open, unfilled security positions. Years of costly incidents and breaches have led to chief executive officers (CEOs) worrying about security threats. PricewaterhouseCoopers 2018 report *Threats: What Keeps CEOs Up at Night Differs by Region*[2] highlights that executives are concerned about cybersecurity threats—a concern that was ranked number 10 in 2017, but has risen to number four in 2018. Cybersecurity is now a top executive topic and one that has the board of directors paying attention, too.

**Mike Saurbaugh,** CRISC, CISM, CISSP, MSIA
Serves as a director of technical alliances with business development solution integration responsibility for enterprise customers. Previously, he spent nearly two decades leading cybersecurity and technology in financial services and was the head of cybersecurity for 12 years. Saurbaugh is faculty with IANS Research and strategically advises Fortune clients on cybersecurity. Involved from the onset with Security Current when it launched, Saurbaugh served as the research director, leading a number of strategic projects for global security vendors and CISOs. Saurbaugh is also a mentor with cybersecurity accelerators MACH37 and Queen City Fintech, and he owns a security consulting LLC where he conducts independent advisory and risk assessment engagements. Saurbaugh has served in various curriculum advisory committee roles for higher education.

Though there is seemingly no end in sight for enterprise anxiety over security issues, there is no guarantee employees will have perpetual job security and be immune to changes in the industry that disrupt human capital. Security professionals need to evolve and enhance their careers to better position themselves for continued employment because technology and automation will be a priority for security leaders playing catch-up to the adversary.

Whether candidates are new to the security field or have some tenure, it is imperative that they not rest on their laurels and keep advancing the career skills that employers are seeking.

### Technical Skills—Taking Initiative and Learning Something New

Security practitioners have plenty of opportunity to learn new skills, in many cases at low to no cost. Employers will likely allocate some budget to obtaining new skills, but, regardless, practitioners need to invest in themselves and assume the employer will not. Technology moves too quickly to sit back and get comfortable.

Employees should be dabbling in new technology to at least understand the basics. Years ago, building a lab would have required expensive hardware and licenses. Today, there is a plethora of opportunity to build a lab in the cloud at minimal cost. This is a fantastic way to build something, break something, build it back again and then share the experience with others. It is a great story to tell. There is significant value in explaining this in a technical interview or, as an experienced hire, being able to convey to a potential team the ability to "walk the talk." In many cases, this may be enough to land the next internal or external position.

The list of new technologies continues to grow, but there are a few that stand out in the short term, despite the list’s ongoing expansion. Following are a few growing areas where practitioners can and should devote some time to help ensure that they are in a better position to land that next role:

- Python
- PowerShell
- Amazon Web Services (AWS)
- Microsoft Azure
- Docker
- Analysis and incident response
- Application security
- Kubernetes
- Threat intelligence
- Threat hunting
- Forensics
- Malware analysis
- Penetration testing
- Data science fundamentals

> “PRACTITIONERS’ CURIOSITY AND INTEREST IN TRYING SOMETHING NEW, ESPECIALLY IN THE SECURITY FIELD, SHOULD BE AN EXPECTATION AND SOMETHING EMPLOYERS SEEK.”

When embarking on a course, it may become apparent quickly that it is not the right path. It is okay to fail fast. Practitioners’ curiosity and interest in trying something new, especially in the security field, should be an expectation and something employers seek. Determining that the technology is not interesting or it is too much of a struggle to grasp the basics is fine, but it is important to move on and try something else as opposed to remaining comfortable.

While this is not an exhaustive list, Coursera,[3] edX,[4] LinkedIn,[5] Udacity[6] and Udemy[7] offer various technology courses for free or at low cost. Also, Microsoft offers training on Azure,[8] and Amazon offers training on AWS.[9]

Ultimately, technical skills will more than likely win the job for the candidate. This can be hard, especially for experienced candidates who have progressed up the management ranks. It is all the more reason for managers who are not doing the day-to-day hands-on work to do their best to keep their skill set up as much as possible.

## Soft Skills Matter

Conversely, employees who have fewer years of experience, but aspire to a higher-level position should be working on attributes that will set them apart. Soft skills do matter. It is very easy to overlook soft skills in the security and technology field.

Soft skills are personal attributes that support interaction with other people. It is much different from the solitude that often comes with technology work and extended computer time with the screen and keyboard providing bidirectional communication.

It is no secret that businesses rely on technology, making cybersecurity a key area of focus for businesses eager to protect systems and data. Soft skills are required to obtain buy-in from the business. Many technologists excel in technology due to requirements for system security, uptime and functionality, and may not have essential soft skills.

What soft skills and personal attributes are influential in career growth? Many of these are no surprise, but they are sometimes given less focus:

- Communication (written, verbal)
- Team orientation
- Organization
- Project management skills
- Service orientation
- Business finance comprehension
- Business acumen
- Emotional intelligence
- Empathy
- Listening
- Personability
- Negotiation

### Enjoying this article?

- Read *State of Cybersecurity 2018–Part 1: Workforce Development* *www.isaca.org/state-of-cybersecurity-2018*

Soft skills translate into professionalism, too. In other words, career advancement often depends on professional growth and dropping bad habits that hold people back. Being someone who others want to work with can be a significant career advantage. Managers can always train skill, but ridding employees of a bad attitude is a completely different challenge and one that many are not willing to fight long term. It goes without saying in information security, but for the sake of full inclusion, it is important to stress the need to be true and genuine and hold a high degree of integrity.

## The Importance of a Professional Network

Building a strong professional network is essential. Employees who spend too much time isolated from others in their industry are likely to find it difficult to pivot to the next organization when they want to make a change. This is not to say loyalty and dedication to one's organization is a negative, but time does need to be made for connecting with others.

Some may find this rather obvious and are well on their way to establishing a strong professional network. Surprisingly, though, it is easy for some to stay within their comfort zone and not engage with others. The challenge is that when these individuals are seeking their next position, they may have trouble finding a role they desire. Many positions are not posted externally and sometimes, before they are even posted, up-and-coming opportunities may be known to peers. Those who are connected may stand a better chance of getting an earlier opportunity to demonstrate that they are the better candidate.

Obviously, social networking is a great place to get started. Professionals do not have to be the most acclaimed user of Twitter or LinkedIn, but they are advised to have some sort of presence (at least on LinkedIn). In addition, conferences are a great place to meet new people and start to forge new relationships. It may be uncomfortable for those who are not overly social, but there is a need to start making connections one by one. There is no shortage of low- to no-cost conferences to meet new people in the local area. Many global events can be attended online.[10]

Conferences need speakers. Consideration should be given to submitting to the call for papers (CFP). Speaking at conferences is a great way to improve one's personal brand. Done well, it is a way to start being identified as a leader in a particular discipline. However, speakers must beware because the security industry will scrutinize the content, so speakers need to be prepared to deliver highly informative presentations.

## Give Time to Help Others

Those who have learned a lot should share their knowledge. What does this do for a career? For starters, it helps promote a personal brand and recognition in the industry. In addition, it increases education on the topic among technical and nontechnical people. This is a common outcome of conference talks and individual blog posts. The security industry thrives when practitioners and managers share what they have learned, both good and bad, in their day-to-day activities.

It is great when security knowledge reaches a technical audience, but what about nontechnical people? The average person who has a smartphone and/or a computer uses most of the same applications as the rest of the world when it comes to office work and social media. Volunteering some time to help educate nontechnical people on how to better secure their data and the systems they use can go a long way toward expanding one's technical reach in the world. It also helps practitioners work on communication skills. Acronyms do not work well with laymen or the business. This is a chance to hone in on enhancing communication skills to get the point across.

This activity makes for a great conversation with current and potential future employers. It is a blend of so many useful traits that employers seek: technical prowess, soft skills, contributions to the profession and initiative, to name a few. Furthermore, it is not uncommon for employers to have a volunteer program initiative for the workforce in which professionals can contribute and help increase knowledge, skills and abilities among those involved.

For more experienced professionals, mentoring junior employees can be a rewarding experience. Granted, a lot of this will be done within the organization itself, but it is not to say that it cannot be done outside the corporate environment, too. If someone reaches out and shows genuine interest in learning from experience, it is a good time to lend a hand. At the same time, mentoring should not be overly draining, so managing the time allocated is important.

## Additional Options and Resources

Certifications have been sought by practitioners for years and still hold a place for many in the industry.

Their value varies, based generally on the enterprise hiring. If an organization requires certifications, then there is value in holding one or more. Some organizations do not care and are more interested in job skills than in whether candidates have initials after their name. But, in general, certifications carry merit.

For newer employees in the field, they are certainly worth looking into and obtaining. Credentials from CompTIA, ISACA®, (ISC)² and SANS, along with vendor-specific certifications, offer the opportunity to indicate to employers that a certain level of mastery has been achieved. Additionally, and this goes for experienced employees, it also shows some dedication to the field and career. After all, unless an employer is requiring a certification, a lot of this is based on initiative and exemplifies dedication to and passion for one's career path.

A respected personal development resource, regardless of the employee's career focus, is StrengthsFinder,[11] which helps people identify their strengths vs. calling attention to weaknesses. The idea is to continually capitalize on strengths to be more successful. Too often, weaknesses are the focus, which can drag people down. However, by leveraging strengths, people tend to excel and are happier in the process.

Those who wish to remain informed on what is going on in the industry job market should check out CyberSeek,[12] which is a culmination of career path information for employers, employees, educators and students.

The National Initiative for Cybersecurity Education (NICE),[13] offered by the US National Institute of Standards and Technology (NIST), focuses on education, training and workforce development. The framework on which the initiative is based[14] outlines knowledge, skills and abilities that are needed to perform tasks in a role.

## Conclusion

Careers are what people make of them. There are no guarantees. It is in a person's best interest to continue to evolve and not sit back and wait for something to happen. The security field needs all kinds of people with diverse backgrounds and experiences. As mentioned earlier, technical skills tend to capture the most attention, but there is a need for well-rounded individuals. When faced with a choice, it is preferable to err on the side of learning more on security technology, but still putting some effort into soft skills as time allows.

The job market continues to look promising for quite some time, but it is unlikely to last forever. In the meantime, putting in the extra effort to learn a new technology, enhance soft skills and build a professional network while giving back in the process is likely to result in the phrase, "You are hired!"

> “THE SECURITY FIELD NEEDS ALL KINDS OF PEOPLE WITH DIVERSE BACKGROUNDS AND EXPERIENCES.”

## Endnotes

1. ISACA®, *State of Cybersecurity 2018*, *https://cybersecurity.isaca.org/state-of-cybersecurity*
2. PricewaterhouseCoopers, *Threats: What Keeps CEOs Up at Night Differs by Region*, 2018, *www.pwc.com/gx/en/ceo-agenda/ceosurvey/2018/gx/business-threats.html*
3. Coursera, *www.coursera.org/*
4. edX, *www.edx.org/*
5. LinkedIn, *www.linkedin.com/*
6. Udacity, *www.udacity.com/*
7. Udemy, *www.udemy.com/*
8. Microsoft, "Get Hands-on With Cloud Technologies From Microsoft," *https://www.microsoft.com/handsonlabs*
9. AWS, "Welcome to AWS Training and Certification," *https://aws.amazon.com/training/*
10. InfoSec Conferences, "The Community's Official Cybersecurity Conferences Directory for 2018," *https://infosec-conferences.com/*
11. Rath, T.; *Discover Your CliftonStrengths*, Gallup Press, USA, 2007
12. Cyber Seek, *www.cyberseek.org/*
13. National Institute of Standards and Technology, "National Initiative for Cybersecurity Education (NICE)," USA, *https://www.nist.gov/itl/applied-cybersecurity/nice*
14. National Institute of Standards and Technology, "NICE Cybersecurity Workforce Framework," USA, *https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework*