

How to Grow the Right Cybersecurity Practitioner

Introduction

Cybersecurity is an ever-changing, ever-evolving practice. Because of this, the right cybersecurity practitioner will require hands-on experience and continuing education throughout their career to stay current in the field. A solid dose of interpersonal and organizational skills, which complement the technical, are also essential.

So, whether the search begins inside your bank or externally, filling this position is critically important due to the level of trust and responsibility that is provided the person who holds this role.

Finding the Right Professional

When choosing a cybersecurity practitioner, look for honesty, applicable degrees, and certifications along with previous job experience. If you don't have strong experience within your institution to help with the evaluation, consider bringing in a trusted third-party partner, such as one you use for your IT audits.

Focus on candidates for the position who have solid written and oral communication skills (consider requiring a written component to the interview process), a willingness to collaborate with others, and a friendly demeanor.

You should also take into consideration if the individual has a solid track record of being a [lifelong learner](#), which will help to keep them self-motivated so they continue to learn. Make any expectations that you have for the position known during the interview and hiring process. Document the educational plan and success factors.

Educational Plan

Whether you hire someone with 20 years of experience or new to cybersecurity, your path will be similar. You will want to groom that employee so that they develop the skills and habits that will make them successful in your organization.

Provide the training that you feel will be most valuable to them, while also monitoring and documenting their progress. If you need to remind the new employee repeatedly to complete something, as an example, that might be a red flag.

Putting together an educational plan takes time. The [National Institute of Standards and Technology](#) and the [National Initiative for Cybersecurity Careers and Studies](#) offer guides on cyber workforce development, while ICBA's Community Banker University offers [Bank Security Certification](#) and other training.

Training should introduce them to banking as well as their new IT department. Training should cover any gaps they might have in their education. Introduce them to project management training and communications.

Once complete, move onto the technical training to bring your cybersecurity practitioner up to speed on the specifics to your IT environment, emerging technology, and IT bank regulations. Bank-specific [cybersecurity training](#) from ICBA is a valuable option.

Suggested Training

- Internal bank or teller training to learn more about banking
- Video training from a reputable company:
 - Business Analyst Training
 - Project Management Training
- Technical Training as it applies to your specific IT infrastructure
- [FFIEC regulations and guidance](#)
- Your regulator's specific guidance
- [ICBA's Cybersecurity Certification or IT Institute](#)
- Technical and management degrees

Consistency is Key

Meet regularly with your new cybersecurity practitioner to review their progress. Verify that they are getting something out of the training and learning it to the degree that you feel is important.

Because sitting through eight hours of training can be difficult, consider having the individual complete four hours of training and another four hours of reading. You can also encourage them to spend part of each day attending project meetings or shadowing IT staff, or other departments, to learn more about the bank. To measure their level of engagement in the learning process, solicit suggestions on how to improve the IT department, security department, or bank.

First Projects

The U.S. Cybersecurity and Infrastructure Security Agency offers free guides, tools and services on [cybersecurity assessments](#), [detection and prevention](#), and [cybersecurity training and exercises](#) that might make a good first project for your new cybersecurity practitioner to implement, while benefiting your financial institution by possibly reducing your yearly IT assessment costs. These and other resources are listed on the ICBA [website](#) for future reference.

Additional Resources for Community Banks

New cybersecurity practitioners should be engaged with the follow organizations to keep up on new information and to look for future training opportunities:

- [ICBA](#)
- [FS-ISAC](#)
- [InfraGard](#)
- [CISA](#)

Final Thoughts

Identifying the right cybersecurity professional is key, and continuous learning is part of the practitioner's job and your job as a leader. By utilizing available resources, community banks can groom excellent IT staff. Should you have further questions, please do not hesitate to reach out to ICBA to discuss your bank's needs.