

Jason Andress, Ph.D., CISM, CISSP, GPEN, ISSAP, is a seasoned security professional with experience in the academic and business worlds. In his present and previous roles, he has provided information security expertise to a variety of companies operating globally. He has taught undergraduate and graduate security courses since 2005 and conducts research in the area of data protection. He has written several books and publications covering topics including data security, network security, penetration testing and digital forensics.

Building Information Security Professionals

A commonly posed question among people looking to enter the information security field is, “How do I get into information security?” This is an excellent question and one that can be answered in a variety of ways, although, perhaps, it is not really the right question to ask. A better question might be, “What do I need to do to build myself into an information security professional?” The distinction between the two questions is narrow, but important.

One might think of this as the difference between looking for a job and looking for a career. Career information security professionals are some of the most passionate, dedicated and engaged people in all of the technology industry. Such focused people can often be found burning the midnight oil on security research, projects and conference presentations, not necessarily because they are being paid to do so, but because they have a strong personal interest in doing so.

THE THREEFOLD PATH TO BECOMING A SECURITY PROFESSIONAL

Moving into the world of the security professional can take one of three main routes: emphasizing experience, emphasizing education or doing a bit of both (**figure 1**).

The Journey, Not the Destination

In the past, when information security was not a field in and of itself, very few people started out as “security professionals.” While many people were doing the job of security, most of them started out on a help desk or in systems administration or in an entirely unrelated field. Often these security professionals did not have a title related to the security field at all.

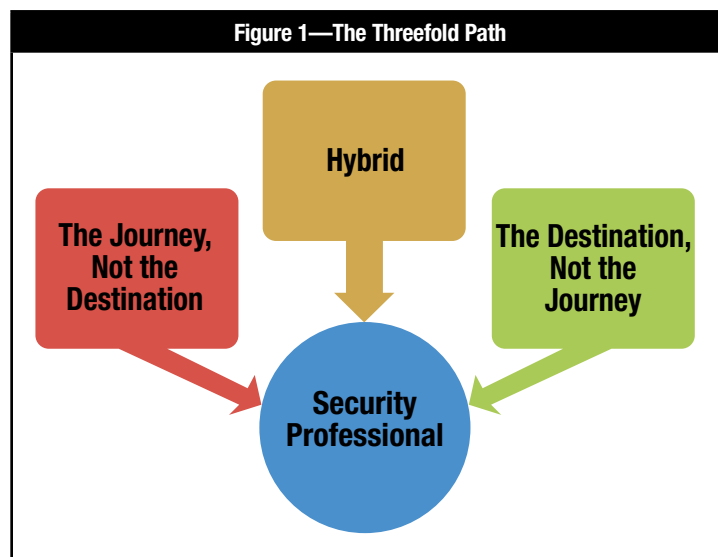
Frequently, those in the security field wound up there after they had worked their way

through the general IT field or had been thrust into the role by pure happenstance or dumb luck. The point being, security professionals did not have a clear career path for quite a long time. Many would argue that this is true today and even proper. The benefit being that those who work through a number of IT-like positions often have a certain breadth of experience, or well-roundedness, that is beneficial to those in security roles. For example, security professionals who have spent a bit of time doing development work might have a much better eye for assessing the risk of a new application than someone in the same position who recently learned the basic concepts in school, but has less hands-on experience.

Security professionals who enter the profession in this manner are often highly skilled and knowledgeable in a wide variety of subjects related to the security field. Unfortunately, this model of security professional development does not necessarily scale well. Waiting many years for security professionals to be ready is not conducive to producing them in any great quantities.

The Destination, Not the Journey

The massive demand in recent years for those who can fill security roles in both the government and the civilian worlds precludes, in some cases,



Enjoying this article?

- Learn more about, discuss and collaborate on information security management and information security policies and procedures in the Knowledge Center.

www.isaca.org/knowledgecenter

Experience tempered with education can result in taking some of the better features of the two approaches while avoiding many of the negatives.

EDUCATION, CREDENTIALS AND EXPERIENCE IN THE SECURITY FIELD

While information security does not yet have the formal licensing of, for example, the medical or engineering fields, a combination of formal education, security training, credentials and experience provide an adequate substitute (**figure 2**) and result in strong, knowledgeable security professionals.

Figure 2—Components of a Strong Security Professional



Formal Education

To produce security professionals at the pace now required (and to enhance remunerative rewards), a number of formal educational programs have arisen in the last five to 10 years. An enormous upsurge in formal university programs catering directly to the information security field has occurred. These programs range from associate degrees to doctoral degrees and can be found everywhere from large universities to diploma mills. Why the enormous growth? Such institutions follow the demand from the industries forming their advisory boards (where such exist) and/or follow the flow of funds.

the individual molding and long-term development that would produce skilled and experienced security workers. In the last year, a 100 percent jump in security recruitment was seen, with another 30 percent increase predicted for 2014.¹ Just as with other products and services, the information security field and how it develops its professionals must change to meet a huge jump in demand.

There is presently a paradigm shift in the way security professionals are developed. While previously junior security workers would be developed in other related fields, perhaps doing protocol development work, administering Linux operating systems, engineering networks or any number of other similar tasks, now they may start off directly on the security path in order to meet the increased level of demand for such skills.

While it might be assumed that hurrying an individual through the process of becoming a security professional would result in a drop in quality, this really depends on the position in question. In many cases, the junior positions in the field do not depend on a great body of experience and can be performed by most technically inclined people with a certain amount of classroom or on-the-job training.

In a certain sense, the previous paradigm can be looked at as having outsourced the training of security professionals to other fields, and the new paradigm as doing the training of junior security personnel in-house. While this method exhibits certain trade-offs, namely a general loss of well-roundedness as compared to the previous method, one of the big benefits is that people can be put through the process much more quickly in order to meet demand.

Hybrid

A middle ground between the two routes described previously exists as well. While plenty of university programs happily place students directly into a security program from the get-go, there is nothing wrong with doing a bit of each. A number of security professionals in the field (the author included) split the middle of the two approaches by spending time in the various IT and computing fields and then continuing on a path of formal security education and credentialing.

Such an approach can have the benefit of producing a security professional who has a good amount of technology experience and knowledge on which to base decisions, as well as formal training and/or education in the security field.

A sufficient number of such programs exist to fit with the different methods of building security professionals discussed earlier. For those emphasizing general experience in the field, computer science and IT programs are a good fit. Those who choose this approach might benefit from classes on networking, software development, computer engineering and as wide a variety of other related topics as can be worked into a degree program. Although such an educational plan might not be specific to security, such a broad background is certainly helpful in the field.

For those looking to jump directly into a security education, a number of universities now offer specific information security programs at the associate, bachelor and master levels, and some schools even offer terminal degrees (various doctorates, etc.) in security. Such programs, as might be expected, tend to be very focused on security and might indeed be very beneficial in terms of formal security education, but such focus may be a double-edged sword. Where someone with a computer science degree may be able to work successfully in a wide variety of fields, the same might not always be true for the individual with an information security degree.

For those taking the hybrid approach, blending a general education and a security education is likely the desired approach. Many schools now have a fairly good selection of security courses or offer a general degree, such as computer science, with a concentration or a minor in information security. By going this route, a person can develop a good information security foundation and, at the same time, build somewhat of a background in development or systems administration. Even in the case where a particular school does not offer such an option formally, discussing the situation with the department chair or dean may result in developing something similar with creative selection of electives or class substitutions.

Security Training

Security training in a non-university setting has been around a good deal longer than the formal education programs seen in the information security field. Offerings in this area come from a wide variety of organizations, including ISACA®,² (ISC)²,³ SANS,⁴ EC-Council,⁵ CompTIA⁶ and Offensive Security,⁷ among others. The organizations offering such training also frequently offer accompanying certification (discussed at greater length later in this article). As of late, organizations offering training and certifications may be seen

to split into two bodies in order to meet American National Standards Institute (ANSI) requirements to enable greater entry into the government market. SANS (the training side) and the Global Information Assurance Certification (GIAC) are excellent examples of this.

Nearly any type of training in the security area is on offer somewhere from someone in a wide variety of formats, including classroom, online, self-study and everywhere in between. Everything can be found from general information security training, such as might be used as a foundation for a career in information security, to very specific training aimed at a particular tool from a specific vendor. The latter might be applicable to someone further along in their career or working in a particular area of specialization.

While some may take such training classes solely for the sake of increasing their personal knowledge of the topic at hand, many such classes are unabashedly directed at ramping up for specific certifications.

Credentials

An enormous number of security certifications are available, with more being created on a regular basis. Such certifications are often included as a requirement when security positions are opened, with the specific certification requirements depending on the job in question.

As the demand for security professionals increases, so does the demand for security certifications. Certification provides employers with assurance regarding someone's knowledge and skills, as an employer cannot test each applicant's skills. In a sense, hiring managers outsource this to certification organizations. Fortunately, at least for those on the receiving end, this increase in demand often relates to an increase in pay for holders of these certifications, generally an increase of somewhere between 8 and 10 percent for security certifications specifically.⁸

For those new to the information security field, with previous applicable IT experience or otherwise, a number of more general information security certifications exist, such as Security+⁹ and the Advanced Security Practitioner (CASP)¹⁰ from CompTIA, Systems Security Certified Practitioner (SSCP)¹¹ and Certified Information Systems Security Professional (CISSP)¹² from (ISC)², GIAC Security Essentials (GSEC)¹³ and the GIAC Information Security Professional (GISP)¹⁴ from SANS/Global Information Assurance Certification (GIAC). For those not in a specialized area of

the security field, such as forensics or penetration testing, the more general certifications often prove to be a better choice as they are more broadly applicable. Looking at the job postings for security jobs on some of the larger job boards, there are many more positions requesting these general certifications than anything else.

For those who have been in the field longer and find themselves in a more specialized position, or are looking for one, the more specific certifications become considerably more relevant. For penetration testers, for example, certifications such as the GIAC Penetration Tester (GPEN)¹⁵ and the GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)¹⁶ from SANS or the Offensive Security Certified Professional (OSCP)¹⁷ and Offensive Security Certified Expert (OSCE)¹⁸ from Offensive Security may be likely qualifications for such positions. Although these specialized certifications may be much more interesting for the beginning or aspiring security professional to pursue, prioritizing these over more general certifications may limit career opportunities. For those looking toward the aspects of security that are closely business-aligned, the Certified Information Systems Auditor® (CISA®),¹⁹ Certified Information Security Manager® (CISM®),²⁰ or Certified in Risk and Information Systems Control™ (CRISC™)²¹ from ISACA may prove useful.

Additionally, a number of vendors including Microsoft, RSA, Cisco, Symantec, HP and countless others provide certifications specific to their security hardware, software and tools in general. Such certifications may vary considerably in usefulness from one employer and/or environment to the next. While a given environment may be a heavy user of technologies from one particular vendor, another might not see these technologies implemented at all. Security professionals choosing to pursue vendor-specific certifications should certainly keep this in mind when planning for the long-term utility of their certification efforts.

Experience

One of the great conundrums of gaining entry into the information security profession is how to develop sufficient experience to qualify for the desired position. Even those who took the journey-not-the-destination path and have a great deal of relevant, but not strictly security-related experience may have issues in this area as employers often ask for several years of direct experience in a full-time security position. Fortunately, there are several ways to address this.

While direct experience in a security position is not always easy to come by, a number of other methods can enable one to gain functional experience in the security industry. A countless variety of security-related projects exist with which individuals might associate themselves including, for example, blogs, podcasts, security research, conferences, advisory boards for security certification bodies and security tool development. While these might not match directly to a full-time security position, they will likely bring the aspiring information security professional name recognition and connections in the security industry, as well as the potential for valuable experience and learning opportunities. These are certainly beneficial in the areas of career and skill development.

MAINTAINING A BALANCE

As a part of the discussion on education, training, credentials and experience, it is important to find a proper balance among these individual factors. Speaking generally of the security industry, and certainly not every single position, emphasizing one single factor to the exclusion or suppression of another may create a difficult situation.

Those who overemphasize education, training, certifications or certificates (especially certificates), but who lack direct security experience to back up these credentials, may be considered to be merely “chasing qualifications.” Potential employers might look at such individuals as a risk for concentrating more on gaining future credentials than actually doing the job for which they were hired.

In the reverse situation, with a highly experienced individual lacking formal education, training or certifications, potential concerns exist as well. Such individuals may be thought to be lacking in ambition or drive, as such credentials are often milestones to indicate certain points in the security professional’s career progression. Additionally, lacking certain credentials expected of mature security professionals (e.g., the CISM or CISSP) might mean that the individual is filtered out at the HR level when applying for jobs, before they even have the chance to show off their skills to the hiring manager.

WHERE TO START?

Where does one start? While starting from a dead stop and jumping directly into the field can be a daunting and difficult task, beginning to move in the right direction can only be of benefit. Here are a few tips:

- Look into professional security organizations, such as the local Information Systems Security Association (ISSA), ISACA or (ISC)² chapters, or more hacker-oriented groups, such as local Defcon or 2600 meetings.

- Keep an eye out for security conferences nearby, or make a trip to one of the larger conferences such as Defcon, RSA or DerbyCon.
- On the education and training side, try to take a few classes at a university or even from a training vendor to get a start in the field. Such classes can be expensive when self-funded, but discounts may often be found through professional organizations.
- Last, but certainly not least, get out there and participate in the field. Speak at a conference, lend a hand with a project, write a paper or an article, post on a blog, participate in forums and generally start to build a brand.

As noted by computer security and privacy specialist Bruce Schneier, “It doesn’t matter what you know or what you can do if you can’t demonstrate it to someone who might want to hire you. This doesn’t just mean sounding good in an interview. It means sounding good on mailing lists and in blog comments. You can show your expertise by making podcasts and writing your own blog. You can teach seminars at your local user group meetings. You can write papers for conferences, or books.”²²

Even when walking into a job interview with no direct security experience, these things will stand in much greater stead than having nothing to show at all for being interested and active.

ENDNOTES

- ¹ CyberCoders, “Dramatic Increase in Cybersecurity Jobs to Continue Into 2014,” CyberCoders.com, 11 July 2013, <http://blog.cybercoders.com/post/55203970304/dramatic-increase-in-cybersecurity-jobs-to-continue>
- ² ISACA, www.isaca.org/education/training/pages/default.aspx
- ³ (ISC)², <https://www.isc2.org/reviewseminars/default.aspx>
- ⁴ SANS, www.sans.org/find-training/

- ⁵ EC-Council, www.eccouncil.org/Training
- ⁶ CompTIA, www.comptia.org/training.aspx
- ⁷ Offensive Security, www.offensive-security.com/information-security-training/
- ⁸ Foote Research Group, *2Q 2013 IT Skills Trends*, 2013
- ⁹ CompTIA, <http://certification.comptia.org/getCertified/certifications/security.aspx>
- ¹⁰ CompTIA, <http://certification.comptia.org/getCertified/certifications/comptia-advanced-security-practitioner-%28casp%29>
- ¹¹ (ISC)², <https://www.isc2.org/sscp/Default.aspx>
- ¹² (ISC)², <https://www.isc2.org/cissp/default.aspx>
- ¹³ Global Information Assurance Certification (GIAC), www.giac.org/certification/security-essentials-gsec
- ¹⁴ Global Information Assurance Certification (GIAC), www.giac.org/certification/information-security-professional-gisp
- ¹⁵ Global Information Assurance Certification (GIAC), www.giac.org/certification/penetration-tester-gpen
- ¹⁶ Global Information Assurance Certification (GIAC), www.giac.org/certification/exploit-researcher-advanced-penetration-tester-gxpn
- ¹⁷ Offensive Security, www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/
- ¹⁸ Offensive Security, www.offensive-security.com/information-security-certifications/osce-offensive-security-certified-expert/
- ¹⁹ ISACA, www.isaca.org/cisa
- ²⁰ ISACA, www.isaca.org/cism
- ²¹ ISACA, www.isaca.org/crisc
- ²² Schneier, Bruce; “So You Want to Be a Security Expert,” Schneier.com, 2012, https://www.schneier.com/blog/archives/2012/07/how_to_become_a_1.html

The *ISACA Journal* is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *ISACA Journal*.

Opinions expressed in the *ISACA Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors’ employers, or the editors of this *Journal*. *ISACA Journal* does not attest to the originality of authors’ content.

© 2014 ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, MA 01970, to photocopy articles owned by ISACA, for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

www.isaca.org