

# Building Information Security Professionals

By Jason Andress

A commonly posed question, particularly among people looking to get into the information security field, is "how do I get into information security?" This is an excellent question, and one we can find 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 definitely present.

We 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. We will often find such focused people 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 burning interest in doing so.

So, that being said, let's talk about how we build information security professionals.

Discuss in Forums {mos\_smf\_discuss:Andress}

## 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, and doing a bit of both.

### The Journey, Not the Destination

In the beginning, when dinosaurs roamed the earth and information security was not a field in and of itself, very few people started out as "security professionals." While many people were doing this job, almost all of them started out on a helpdesk or in system administration or even in entirely unrelated fields like English literature. Often they didn't have a title calling them out specifically as being in the security field at all.

Those who were in the security field wound up there after they had worked their way through the IT field in general for some time, or they may have been thrust into the role by pure happenstance, dumb luck, or bad behavior in a previous life. The point being that security careers really didn't have a clear career path for quite a long time. Many would argue that this is the true and proper path to this day.

One benefit to this approach is that those who worked through a number of IT-like positions often have a certain breadth of experience, well-roundedness some might call it, that is beneficial to those in security roles. If our security professional spent a bit of time doing development work, they 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 experience to which such concepts might be tied.

The benefit to this method of developing security professionals over time is that those who entered the profession in such a manner were often very 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 our security professionals to be ready is not conducive to producing them in any great quantities.

### The Destination, Not the Journey

In recent years the massive demand for those who can fill security roles in both the government and the civilian worlds precludes, in some cases, the individual molding and long-term development that would produce the skilled and experienced security workers we just discussed. In 2011, an estimated 40-50% jump in security recruitment was predicted with the US government budgeting \$55 billion in cyber security spending over the next five years<sup>1</sup>. Just as with any process that lovingly hand-crafts items must change to meet a huge jump in demand, so do we see the information security field changing.

We are seeing a paradigm shift in the way security professionals are developed. While we would have previously developed our junior security workers in other related fields, perhaps doing protocol development work, administering Linux operating systems, engineering networks, or any number of other similar tasks, we now might choose to start them off directly on the security path in order to meet the increased level of demand for such skills.

While we might assume 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, we can look at the previous paradigm as having outsourced the training of security professionals to other fields, and the new paradigm as having done the training of junior security folks in-house. While this method exhibits certain tradeoffs, one of the big benefits is that we can put people through the process much more quickly in order to meet demand.

## Hybrid

We can also choose somewhat of a middle ground between the two routes previously discussed. While plenty of university programs will be more than happy to put us directly into a security program from the get-go, there is nothing wrong with doing a bit of each. A number of security folks in the field (yours truly included) split the middle of the two approaches by spending a bit of time in the various IT and computing fields and then went down the path of formal security education and credentials.

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. Experience tempered with education tends to make a good combination in a security professional, and we are able to take some of the better features of the two approaches we previously discussed without incurring many negatives.

## Education, Credentials, and Experience in the Security Field

Although information security does not have the formal credentials (yet) we might find in other fields such as medicine or engineering, a few main areas are used as somewhat of a substitute. Primarily, we tend to look at formal education, security training, certifications, and experience.

## Formal Education

In order to produce security professionals at the pace we now need to keep up with (and to enhance remunerative rewards), a number of formal educational programs have arisen in the last five to ten years. We have seen a massive

upsurge in formal university programs catering directly to the information security field. These programs range from associate degrees to doctoral degrees and can be found everywhere from large universities to diploma mills. Why? Such institutions follow the demand from the industries forming their advisory boards (where such exist) and/or follow the flow of money.

A sufficient number of such programs exist to fit with the different methods of building security professionals we discussed earlier. For those emphasizing general experience in the field, computer science and information technology programs would be 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, the broad background will certainly be 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 even some schools offering terminal degrees (various doctorates, etc&hellip;) in security. Such programs, as we might expect, tend to be very focused on this specific industry, and might indeed be very beneficial in terms of formal security education, but we should also be aware that such focus may be a two-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 will likely be the desired approach. Many schools now have a fairly good selection of security courses or may 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 while at the same time building somewhat of a background in development, system administration, etc. 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 be able to get us there 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 we finally see in the information security field. Offerings in this area come from a wide variety of companies including SANS, CompTIA, Security Horizons, Offensive Security, and a number of others. We can often find companies offering such training also offer the accompanying certification for the training in question (which we will discuss at greater length below). As of late, we can begin to see organizations offering both training and certifications split into two bodies, this being done to meet the ANSI standards required to enable greater entry into the government market. SANS (the training side) and GIAC (the certification side) are an excellent example of this.

Nearly any flavor of training in the security area we might desire is on offer somewhere from someone, in a wide variety of formats including classroom, online, self-study, and everywhere in between. We can find everything from general information security training, such as we might use as a foundation for a career in information security, to very specific training aimed at a particular tool from a specific vendor which might be applicable to someone further along in their career.

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.

## Certifications

Although discussions on the various security certifications have been done to death, we would be lax not to at least mention them here. An enormous number of such certifications are available in the industry today 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.

For those new to the field with previous applicable IT experience or otherwise, a number of general information security certifications exist such as the Security+ and the CASP from CompTIA, the SSCP and CISSP from ISC2, the GSEC and the GISP from SANS/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, we will find many more positions requesting these general certifications than anything else.

For those who have been in the field for longer and find themselves in a more specialized position (or are looking for one), the more specific certs become considerably more relevant. For penetration testers for example, certifications such as the GPEN and the GXPN from SANS or the OSCP and OSCE from Offensive Security may be likely qualifications for such positions. Although these may be much sexier and more interesting certs for the beginning or aspiring security professional to pursue, prioritizing these over the more general certifications may, in fact, be career opportunity limiting.

## Experience

One of the great conundrums of gaining entry to the information security industry is how to develop sufficient experience to qualify for the desired position. Even for 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 will often ask for several years of direct experience in a full-time security position. Fortunately, there is more than one way to skin this particular cat.

While direct experience in a security position is not always easy to come by, a number of other methods can enable us to gain functional experience in the security industry. A countless variety of security-related projects exist with which an individual might associate themselves including blogs, podcasts, security research, conferences, advisory boards for security certification bodies, security tool development, and many more. While these might not measure directly up to a full-time security position, they will likely bring with them 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 area of career and skill development, and the people we work with may very well be the same to point us to our next job.

## Maintaining a Balance

As a part of the discussion on education, training, certification, and experience, a consideration is how we balance these individual factors out. Speaking generally of the security industry, and certainly not every single possible position, emphasizing one single factor to the exclusion or suppression of any of the others creates a considerably more difficult situation to cope with as a security profession.

Those who would overly-emphasize education, training, or certifications (especially certifications), but who lack in the direct security experience with which to back up these credentials, might very well be considered to be merely chasing these "paper" qualifications. Potential employers might look at such individuals as a potential risk for concentrating more on gaining future such credentials than actually doing the job for which they were hired.

In the reverse situation, with a highly experienced individual lacking in formal education, training, or certifications to point at, potential concerns exist as well. Such individuals might be considered 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 (especially the CISSP), might very well mean that the individual is filtered out at the HR level when applying for jobs and never even has the chance to explain why their great body of experience compensates for their shortfalls in other areas.

### Where to Start?

A frequently asked question from those looking to get into the security field is "where do I start?" While starting from a dead stop and jumping directly into the field can be a daunting and difficult task, starting to move in the right direction can only be of benefit.

Check into professional security organizations such as local ISSA or ISC2 chapters or more hacker oriented groups such as local Defcon or 2600 meetings. Keep an eye out for security conferences nearby, or even make a trip out 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. Yes, such classes can be expensive when self-funded, but we may also find discounts through local organizations or even a freebie for participating in security communities such as The Ethical Hacker Network (thanks Don!).

Last, but certainly not least, get out there and participate in the field. Talk 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. Even when walking into a job interview with no direct security experience, these things will stand us in much greater stead than having nothing to show at all for being interested and active in the field.

---

Footnote 1: <http://completeittraining.com/what%E2%80%99s-behind-the-huge-demand-for-it-professionals-in-security>

Dr. Jason Andress (ISSAP, CISSP, GPEN, CEH) is a seasoned security professional with a depth of experience in both 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.