PEERLYST PRESENTS

Beginner's Guide to Information Security

Kickstart your security career with insight from InfoSec experts

PEERLYST PRESENTS

Beginner’s Guide to Information Security

Kickstart your security career with insight from InfoSec experts

Special thanks to our authors, whose insight and generosity embody the spirit of Peerlyst.
Thanks also to Maria Behan, our editor; and Colin Toomey, our cover designer.

Disclaimer of Liability. This crowdsourced publication represents the collective efforts of the authors behind each chapter. Those authors and the publisher have made reasonable efforts to ensure the accuracy of the content of the book, but bear in mind that much of the material here is based on personal experience, anecdotal evidence, and information gathered from a variety of sources. The content contained in this book is no substitute for seeking advice from an information security professional familiar with the facts relevant to your career or organization. The publisher and authors hope this book proves helpful to those considering or embarking on careers in information security, and they disclaim any express or implied warranties.

Peerlyst, Inc.
715 Bryant St.
San Francisco, CA, 94107

Table of Contents

Introduction

By Limor Elbaz

Information security is one of the most vitally important career sectors of the 21st century. The success and even the survival of governments, businesses, and individuals depend on it. It’s also a fascinating—and sometimes lucrative—way to make a living. But even as the world comes to recognize how essential InfoSec is, it’s still a relatively new field, and the paths leading into it are many—though not always well defined.

Peerlyst’s first e-book, the *Beginner’s Guide to Information Security*, aims to cut through some of the confusion about how and where to start, moving you along the road to a successful career in the field. The content you’ll find here has been crowdsourced from members of the Peerlyst online community of InfoSec professionals. Many are longtime experts in some of the sectors that make up this varied field, others are relative newcomers who are eager to share the advice and resources they’ve found most valuable during their own career journeys.

We begin with some chapters that cover ways you can learn about information security, maybe pick up a certification or two, find out about job opportunities, and then, hopefully, snag a job. Then we delve deeper into the InfoSec field, offering perspective and resources that will help you master key skills, like knowing how to protect a network, respond to a security incident, and educate users so they’re part of the security solution—not the problem. Our last chapters focus on “big picture” issues such as women in security (a topic close to my heart), and where InfoSec may be heading in the future.

The Journey into InfoSec

If you’re seriously looking to enter the security field, I won’t sugarcoat it: You’ll encounter some obstacles. It’s easy to learn coding these days, but it can be hard to get your first hands-on opportunities. In security, it’s even more complicated for beginners to get real-life experience. You can do some hacking, sure, but the chances to get involved in legitimate penetration testing are far less frequent. Finding a mentor is tough, given the manpower deficiency in the security space: Everyone is super busy. Accessing commercial products can be expensive, and training is too expensive as well—including most security conferences. In my view, you shouldn’t need pricey certification courses or conferences to become knowledgeable about security.

But where can you learn? Even if you've already gotten a great education—say, a bachelor's degree, or even a master's—chances are that education taught you very little about pen testing, security hardening, monitoring, controls, compliance, etc. This guide can be a start to gaining that knowledge. There's a lot of information here, as well as many guideposts pointing to other information security resources, including books, online courses, and websites.

One of those is the Peerlyst site, which connects the InfoSec community so people can share their experiences and expertise—for free. So if you're interested in security, come check us out. Our online community is all about removing knowledge barriers and sharing real-world information. You might learn some things, even find your tribe.

If you're already in the security trenches, Peerlyst wants to help you help others—and build your reputation for subject-matter expertise while you're at it. When security pros work together and educate each other, people's jobs get easier. And if advice from experts helps more newbies get involved in InfoSec, that will ease the pressure on those who are currently in the field—without compromising on the quality of education.

I hope you find this *Beginner's Guide* both useful and inspiring. And as you continue your journey, I hope to see you online at peerlyst.com!

***Limor Elbaz** is the founder and CEO of Peerlyst, Inc. To hear more from Limor, follow her on Twitter @LimorElbaz, or check out her page on Peerlyst*.

Chapter One

Thirteen Steps for Starting Your InfoSec Journey

By Tracy Z. Maleeff

People have varied motivations for getting into information security. Some see it as a gold rush, and want to head to where the money is right now. Others consider it a calling, a perfect blend of their interests and skills. Then there are those who just fell into it accidentally, maybe by drawing the short straw and getting told that they're now in charge of security. Regardless of how you get your foot in the door, a journey into information security begins with the first step. For those of you contemplating those early steps, let this chapter serve as your guidepost. I'm not an InfoSec expert—in fact, I'm still technically a newbie—but my background in library and information science makes me good at unearthing information and savoring teachable moments. So in that spirit, I'd like to pass along some of what I've learned.

"Get a CISSP!" If I had a dollar for every time that piece of InfoSec advice was dispensed to me, well, I'd have a CISO's salary. A CISSP, pronounced like "sis-pea," is a certification administered by (ISC)² and stands for "certified information systems security professional." When starting out in InfoSec, you quickly learn that certificates—certs, as they are lovingly called—are viewed by many as a necessary evil to getting a job in the industry. The problem with being told thousands of times to "just get a CISSP" is that getting that particular cert requires "a minimum of 5 years cumulative paid full-time work experience in two or more of the 8 domains of the (ISC)² CISSP CBK®." Then you'll actually need to take the exam, which has about a 70 percent passing rate, and maintain certification. There are costs associated with all this. (For instance, the 2016 examination pricing can be found here.)

Are you getting a little stressed out? That's normal.

There's nothing wrong with getting a CISSP; in fact, many jobs require it. It's just not helpful to be given that particular piece of advice when you don't have years of experience or a solid knowledge base yet. It's kind of like telling a 10-year old to just go get a driver's license if they want to get to school. So, keep that CISSP knowledge in the back of your mind, to revisit when the time is appropriate for you.

In your InfoSec journey, you will come across many people who will give you tips, pointers, and opinions. Even the best advice isn't one-size-fits-all.

Don’t fret if one person’s guidance doesn’t fully resonate with you. Talk to lots of people. Letting the advice-giver know your particular situation and background increases the likelihood that you’ll get solid feedback.

The most measured and comprehensive guidance I’ve heard in my InfoSec journey thus far came from Micah Hoffman. You may have heard of his employer, SANS Institute, or you may have seen him Tweet as @WebBreacher. I was fortunate enough to see him speak in person at BSidesCharm in Baltimore this past April. He gave an energizing talk about how to become involved with the InfoSec community. Although Micah made the distinction between the InfoSec *community* versus the InfoSec *industry*, it’s been my experience already that his recommendations have been spot-on for *community* engagement that might lead people into *industry* engagement: i.e., jobs! With Micah’s permission, I present my paraphrase of his 13-point plan, supplemented with additional information from my own experiences and findings.

#1 – Get experience

Many articles you read about the cybersecurity workforce shortage, like this one from *Fast Company*, point to the fact that many InfoSec jobs require skills and experience that don’t come from simply having an IT job or a college degree. Kris Rides, an InfoSec recruiter with the firm Tiro Security, recommends a few ways to get experience to beef up your résumé. The first tip is, to quote Wayne Gretzky, skate to where the puck is going to be. Meaning, if you are already employed, align yourself with the department or group that is handling security for your organization. Either transfer into that department, or offer to help with a project and let the key people know that you are interested in gaining InfoSec experience.

That advice doesn’t just apply to people already employed within the IT department. When I was a librarian at a law firm, I reached out to the CIO and asked if I could help with Cyber Security Awareness Month, and even offered up suggestions. The CIO liked my ideas so much, he implemented all of them and put me in charge of the process of liaising with other departments. I was working in the library and had nothing to do with IT, but by making it known that information security was an interest of mine, I got a chance to get some experience.

For people not currently employed, or working in an organization without a security program, Kris recommends volunteering. Many small businesses or non-profits cannot afford security tools and internal awareness programs, or may not have the know-how to do it. Obviously, companies may be reluctant to turn their internal systems over to a stranger, but you might start by offering them cyber safety tips and suggestions. Work your professional network to see if there are any opportunities for you to volunteer your security knowledge to gain experience that you can proudly put on a résumé. [For more tips from Kris, check out his chapter, "Working with Recruiters."]

#2 - Take control of your self-learning

Micah Hoffman says that there are two types of people: those who take learning into their own hands, and those who wait for someone to tell them what to learn. Be the change you want to see in your InfoSec career, and be motivated to learn. That learning can be in the form of degrees, certifications, or even massive open online courses (MOOCs) or other online training. Do what is best for your budget and time schedule, but as Micah likes to emphasize, just keep learning.

- The National Initiative for Cybersecurity Careers and Studies (NICCS) has lots of information about education, training, and careers in security. *U.S. News and World Report* also offers information about degree programs in the field. Many colleges and universities now offer programs ranging from certificates to doctoral programs in information security.
- The CompTIA Network+ and CompTIA Security+ certifications have been recommended to me as good starting points for newbies in InfoSec. Those are just two of the many certifications you might opt to tackle. *Information Security*'s Dark Reading blog offers a list of "10 Security Certifications to Boost Your Career." Of course, Micah's employer, SANS also offers a wide variety of training programs. Remember that CISSP that I mentioned earlier? You can learn more from the (ISC)² site.
- If free MOOCs are more your speed and price range, there are a few to choose from. Cybrary, EdX, and Udemy are just some options for very low cost or free learning opportunities. Although it doesn't provide guided instruction, the Massachusetts Institute of Technology has made lecture notes, assignments with solutions, and more available for free to the public. Some of their computer

science courses have security classes.

Whichever path you choose, Always Be Learning! InfoSec jobs are for closers.

#3 - Join a group

From my personal experience, joining the Women's Society of Cyberjutsu was one of the best professional development decisions I've ever made. There are a lot of groups to join that could provide you with educational opportunities, training, or maybe even scholarships to help advance your career. For those times when it's about *who* you know and not *what* you know, getting involved with a professional organization could tip the scales in your favor.

There are many different types of InfoSec groups. You may choose to get involved with one that is small and informal, like the kind of thing you would find on Meetup.com. You may choose to engage with a large dues-paying organization like the Information Systems Security Association (ISSA). Successful completion of some certifications automatically qualifies you for membership within the certificate-granting institution. For those of you less inclined to engage with people face-to-face, you can even find groups online through LinkedIn, for example.

No matter how you choose to engage with a group, the important thing is that you connect with like-minded individuals who will help your InfoSec education and career. Find your tribe.

#4 - Set goals

Goal-setting is your action plan for your InfoSec career. Whether you write them down, saved them as notes on your computer, or simply hold them in your head, know your professional goals and work towards them.

Don't take it from me, take it from Nastia Liukin, the U.S. gymnast who was the 2008 Olympics' individual all-around champion: "Set daily, monthly, and long-term goals and dreams. Don't ever be afraid to dream too big. Nothing is impossible. If you believe in yourself, you can achieve it."

#5 - Contribute to an open source project

Have you met OWASP, the free and open security community? The Open Web Application Security Project is a worldwide non-profit dedicated to improving the security of software. By helping them with their efforts, you'll be honing your own skills and potentially, gaining useful skills and contacts.

#6 - Participate at conferences

If you already have some InfoSec knowledge to share, get involved with a conference! Answer those calls for proposals/calls for papers and get out there in front of the community to put your skills on display. Not sure if you are qualified to present? Let the conference submission reviewers decide that for you. Put yourself out there. Consider a rejected CFP as an opportunity to improve. If you don't yet have enough expertise to present on a topic, then be an active participant. Live Tweet, ask questions of presenters, or have conversations with vendors. Figure out your comfort level of participation, then engage! (Also, volunteer! See #8.)

#7 – Check out blogging and podcasting

Much like **#6** and **#10**, there are ways for you contribute to the information security community while learning more for your own personal edification in the process.

- Be a *supplier* of information by writing blog posts on InfoSec forums like Peerlyst about events or conferences you've attended. Start a podcast where you interview industry experts to record and distribute their wisdom.
- Be a *consumer* of information the community puts out. Many of the experienced security professionals in the community craft well-regarded blogs and podcasts that can help you with your journey of learning. Some recommended podcasts are:
    - Banking Information Security
    - Brakeing Down Security
    - Defensive Security
    - PVC Security (full disclosure: I'm a co-host!)
    - Southern Fried Security
    - Find more podcast recommendations here.
- You can't mention security blogs without acknowledging Krebs on Security and Schneier on Security. Find more blogs to follow at the Security Bloggers Network.
- Who says you can't be productive while stuck in traffic? This Peerlyst vlog (video blog) by J. Wolfgang Goerlich will entertain and educate you about security.

#8 – Volunteer

If you haven't yet attended a security or hacker conference, you need to know that many of those are organized by a tireless group of volunteers. Gatherings like BSides, DEF CON, and ShmooCon are the result of the blood, sweat, and tears of your fellow InfoSec professionals who care so much about our community that they give up their free time to make amazing events for us all. Many of the same principles of #3 - Join a group apply here. You will get to meet like-minded individuals, and have fun doing it.

Unsure how you help a con? Answer the call for volunteers that many conferences put out. Tell the organizers your skill set or what you feel comfortable doing. If you are not very socially inclined, but you have audio/visual experience, offer to record conference sessions. There is most likely a conference duty suitable for a wide variety of personality types. From my experience, most con organizers are just happy to have reliable people. When I contacted DEF CON's Crypto Village to volunteer, I let them know that I do not have any lock-picking skills or knowledge related to their part of the conference. But, I wrote them, I have interest, enthusiasm, and willingness to help. They replied, "Those are important qualities to have. Thanks so much for volunteering!" Any time you can turn a volunteering experience into a learning opportunity, it benefits your professional development.

#9 - Ask for feedback

Whether you are fortunate enough to have an InfoSec mentor or are just connected to some experienced industry professionals through social media, asking for feedback is a great way to self-check your goals (see **#4**) or get a different perspective on your journey (see **#11**.) If you are engaged with a group as a volunteer (**#8**) or as certificate holder (**#2**), find a person or a group to be your sounding board. Don't live in a silo, an echo chamber, or any other buzzword for a place where you stay stuck in your bubble. Instead, get someone else's take on your professional development and progress. (See **#11**.)

#10 - Share knowledge

If you are not yet ready to present at conference (see **#6**), Micah Hoffman suggests that you find other ways to share what you do know. Much like the idea in **#1** of volunteering to get experience, volunteer to dispense what you’ve learned. This could take the form of appearing at a career day at a school or holding a brown bag lunch-and-learn about information security for a community group. Sharing knowledge can also come in the form of writing or sharing on social media, see **#7**. One of the best things you can do is to pay it forward by sharing any information that you’ve gained with an InfoSec newbie who is even greener than you.

#11 - Track your progress

This goes hand-in-hand with the goal setting in **#4**. As Micah explained this point during his talk, “Success isn’t how far you got, but the distance you traveled from where you started.” Remember that this is a journey. Think back. Was there a time when you didn’t know what DDoS meant? Are you now able to talk about it without effort—and maybe even explain it to someone? You’re on your way, baby.

No matter how you choose to actually track it, be mindful of how far you are getting as compared to your starting point. As @jessysaurusrex Tweets every Friday, celebrate even your weekly wins. Every win is progress towards your goals. Every failure is just an opportunity for learning.

#12 – Do some professional networking via social media

Learn what to do when you have stacks of business cards, not stacks of protocols. Once you join a group (**#3**) or start attending, presenting, or volunteering at conferences (**#6** & **#8**), you’ll begin growing your professional network of information security contacts.

- First, decide which social media platforms you wish to use, and what professional identity (branding) you want to create. Many InfoSec professionals choose to have a layer of anonymity and are known by a handle. Figure out how you want to be known, and on what channels you’d like to be contacted. Stay consistent so you don’t confuse people, or let communications fall through the cracks.
- Peerlyst is a great place to start, since it’s a forum specifically targeted to the InfoSec community. You can go there to introduce yourself, ask and answer questions, join discussions, research security products and topics, post blogs, and start building a reputation for expertise (or at least enthusiasm) in your particular areas of interest.

- LinkedIn is the most common way to have a professional social media relationship with someone. That's the purpose of that outlet, which allows you to follow or join groups, in addition to following or connecting with an individual.
- Twitter is a real-time and active way to see what discussions are going on in the information security world. Twitter Lists are a great way to keep track of people in the industry. A good way to follow new people, and to get new followers as well, is to live Tweet from conferences. Follow a conference hashtag to see who is expressing interesting—or funny—thoughts.
- There are other ways to engage with an online community of information security professionals. Some are more formal than others. Determine the level of engagement you'd like to have, and then maintain it. In my June 2016 presentation, "Cultivate Your Network Like a Garden," I talked about how you need to keep professional network connections healthy and thriving by keeping in touch with people. Tend to your network like you would a plant: too much or too little attention will make for an unhealthy plant.

#13 - Surround yourself with smart, motivated people

Following steps **#1** through **#12** will help you achieve this. As you advance on your journey, you will find friends, classmates, colleagues, or co-workers in information security that will challenge, inspire, and motivate you. People are a very big part of your InfoSec professional development. Embrace soft skills like people networking in order to learn more and help your career. For every personality type, there is a way that you can feel comfortable engaging with the information security community—and reaping the rewards of doing so.

Each of the above points cribbed from Micah Hoffman illustrates how you can build upon your experiences to begin your journey into an information security career. Help out your fellow travelers along the way, dispensing wisdom as you learn and move ahead. I myself can see the progress that I've made in the past year by applying Micah's advice. I encourage you to follow it as well. Your InfoSec journey begins with a single step. Start now.

***Tracy Z. Maleeff** spent 15 years as a librarian and information professional.*

Since catching the information security bug, she has applied her research, analytical, and instructional skills to the field. She owns Sherpa Intelligence and provides research and social media consulting services with a focus on the tech industry. She likes to share the information she finds as she learns it herself and Tweets as @InfoSecSherpa. You'll find links to Tracy's Peerlyst posts by going to her page.

Chapter Two

Starting a Career in Network Security

By Dean Webb

How I Came to Be in IT—Even Though I Dislike Programming

So many people mistakenly believe that all jobs in IT are programming jobs. I tried programming when I was a kid, got tired of all the typing and eyestrain from bug hunts, and decided I didn’t need to get into IT. I was one of those people with a mistaken belief.

Fast forward to 1995. I was leaving my teaching career and needed to find another line of work that would allow me to keep supporting my family at the same pay or, failing that, a job that would start close to what I was making and then ramp up quickly. I was a humble man, so I would accept any career except sales. I’m terrible at sales.

Lucky me, I got a job doing desktop support. Now, a very important thing to consider in a career path is to look around wherever one works to discover the jobs that nobody else wants to do because they are difficult. Relative to regular desktop support, networking desktop support was difficult. There were openings in that support line, and I took advantage of that opportunity and brought my passion with me.

After seven years of doing IT that plenty of other people said was too difficult for their taste—and also involved very little programming—I took a pay cut and went back into teaching. I did that for another 11 years, when I once again sought one of those IT jobs without programming. This time, it was in networking.

Why networking? I’d had a little experience with it in my past stint in IT, and wanted more. It was very difficult, and lots of people avoided it because of that. To me, that meant that things would ramp up quickly in that line of work. I figured I’d take the job that barely matched my salary as a teacher with 16 years’ experience—a near-entry level job in the field—and then work my way up into a mid-level job.

To my surprise, choosing to focus on network security moved me into the mid-level role much faster than I anticipated. Network security is more difficult than pure networking, because it has to embrace many more disciplines. However, it fit my personality rather well. I like letting my mind take a paranoid twist on what I see, asking what could go wrong, then figuring out how to protect against that potential problem.

And there’s still no programming—so of course I really enjoy that aspect. I don’t mind hacking config files and writing a few scripts, but the majority of my work is analyzing problems and thinking through solutions, so I’m all good.

Preparation for a Career in Network Security

Step one, recognize the fact that the dominant vendor in the networking space is Cisco. As such, being familiar with Cisco gear can go a long way in getting that first networking job. The differences between commands used on Cisco products and other vendors are not insurmountable, so don’t feel as if studying for Cisco certifications will limit you to just that one vendor.

Many of us experienced people strongly recommend getting the Cisco Certified Network Associate (CCNA) Routing and Switching certification first, so that anything learned about security will be built upon a firm, general foundation. It also means being able to get a general entry-level job in networking. Often, one has to be a networking guy before one can become a network security guy.

My advice would be to get that CCNA R&S test done and start looking for your first networking job. Study for and take the CCNA Security test in the meantime. Résumés take about two months from first posting to getting into HR systems, so don’t worry if it takes a while for recruiters to respond.

Getting up to speed in network security will cost you a little bit of money and a fair amount of time, but you’ll probably be pleased with the return on investment. In terms of certification costs, prepare to spend $300 on the CCNA Routing and Switching test, and $250 on the CCNA Security test. Official cert guides, which I strongly recommend, will be another $100 to $200, depending upon which ones you purchase and what condition they are in. The payoff for taking these steps could be an entry-level job that will pay a good deal more than the national average for entry-level jobs requiring a college degree, which stands at around $30,000. To me, that’s a great return on investment.

Read the books, take the practice tests, and use GNS3 to practice with the commands covered in the material. GNS3 is a free tool with many tutorials. Seek out networking forums (oddly enough, I run a set of networking forums and participate actively on Peerlyst), and ask questions to gain more understanding. Answer questions on the forums as well, to gain even more understanding. Those forums will also be places where newcomers to the field can start building relationships with experienced people, and those guys often know where potential job openings are.

Eventually, you will put your résumé together and apply for that first job in the field. Keep in mind that if one is applying for a job that asks for a Cisco certification, there will be difficulty getting into the interview pile without it. I've heard of cases in which employees were vouching for a candidate, but even then, HR objected that the candidate was missing a "required" part of the job specifications.

Fortunately, there tend to be many openings in network security because of the high demand for network-security skills. Unfortunately, a poorly written résumé with no cover letter won't get very far. Customize a cover letter for each position you shoot for, and customize a résumé for each type of position. There are other resources on résumé writing, so I will pass over that topic for now. [If you're looking for some tips on résumé-writing, check out the guide's chapters on "How to Prepare for an InfoSec Interview" and "Working with Recruiters."]

Where should you focus your job search? As of 2016, the best markets for network security tend to be anywhere where one can find an IT department for a bank, pharma company, or oil company. Government departments also have a huge demand for security, as do major defense contractors. That means the most jobs on offer are in the major urban centers in Texas, the Northeast Corridor from Boston to D.C., and California.

Your first job in network security will likely be a contract role. There's nothing wrong with that—by the time that job is complete, it's likely that other ones offering more pay and more challenges will crop up. Your second and third jobs might also be contract roles, and there's nothing wrong with that, either. Full-time security roles typically require three to five years of experience, so get all the experience you can in those three to five years!

Advancing Your Career

Getting a CCNP Security certification is almost required for a full-time, salaried security role. If you can get a similar vendor certification, that is just as good. Just know that many job requisitions will ask for a CCNP or similar certification—and if you have a CCNP Security cert, you won’t have to explain how the one you have is similar to a CCNP.

If you’re working in network security, one way you can help your career advancement is by keeping track of each product and vendor you’ve worked with. And sometimes experience with one vendor gives you cred with an employer who’s looking for different, but similar, skills. Worked on a Palo Alto firewall? Congratulations, it’s very similar to a Juniper one.

Even products with a completely different Web interface or command-line environment will share a common underlying theory and set of best practices if they’re in the same technology family. Worked with an intrusion-prevention system? Congratulations, they all do the same things, more or less.

The best thing any aspiring network security person can do is to volunteer to work on a new product or a difficult product. Study that product, learn it, and become a master with that product. The work put into such an effort tends to pay off in a big way down the road.

It’s also important to keep current on security news and emerging security products. While my forums, www.networking-forums.com will cover networking in general, including security, there is a specialist website, www.peerlyst.com, that I can highly recommend to anyone wanting to immerse himself or herself in the jargon, concerns, and discussions of security. Remember that just knowing about products and trends doesn’t qualify you to add them to your résumé, but it does help to be aware of what’s out there and how it stacks up relative to the products one is currently using.

Speaking of résumés, it’s a good habit to update yours every three months or so. Add highlights and big accomplishments while removing less-relevant details. Maybe there’s nothing to change, but by reviewing it, you can get a sense of what direction your career is headed in and how satisfied you are with your current position.

Prepare to do documentation, particularly in mid-level roles and higher. Places that put a premium on security—banks, government entities, healthcare facilities—also have a host of regulations that require documentation. The documentation isn’t specific to network security, but it is part of the role if you’re working for those kinds of employers. Having good writing skills is a definite plus—even if they depend upon running a spell- and grammar-check in a word processor.

Finally, develop patience. It will be needed when programs are slow to load, when everyone blames the firewall for every problem, when waiting for budgets to be approved, when discovering that the budget was approved—but for a different vendor than the one recommended, and on and on. Patience is also needed when studying network traffic patterns, waiting for an anomaly to recur, and building out rulesets for security devices.

Network security is a rewarding career, and I love my experiences in the profession. And did I mention there's no programming? I totally love that part.

***Dean Webb** is a Dallas-based computer and network security specialist. He has started a career in IT twice, and watched it develop rapidly into a very satisfying line of work each time. As a former teacher, he enjoys passing on useful information to anyone willing to hear it. To hear more from Dean, check out Networking-Forums.com or his Peerlyst page.*

Chapter Three

How to Prepare for an InfoSec Interview

By Fabio Baroni

Let’s imagine for a moment that you’re sitting on the sofa watching TV, or out with friends at the seaside—in short, relaxing—and suddenly an alert comes in on your phone. You just received an email from a big company asking you whether you’d be interested in coming in to interview for a position as an information security specialist or a penetration tester. You’ve been studying really hard during your free time and information security is your biggest passion—although you haven’t actually worked professionally in the field before and you certainly didn’t expect such an email. What do you do?

First of all don’t panic: Today is your lucky day. InfoSec is a technical, competitive, and highly specialized field, and recruiters are having a hard time filling the gap between the demand and the availability of talented security professionals. They use a variety of systems in order to discover the best candidates, often even using open source intelligence-gathering techniques (OSINT), such as those used for the first phases of a real pen test. If a recruiter contacted you, he or she probably saw something good or interesting in you, something that distinguishes you from the crowd.

Take Time to Get to Know Yourself

Now it’s time to leverage the good reputation you’ve got and demonstrate how you earned it during your interview. Take a notebook and a pen and write down who you are, what your education has been, your professional experience, your fields of expertise, your strongest social skills, your certifications, your interests, a few things you are really good at, and your hobbies.

When you’ve done that, write what your personal goals are, what your dream job would be, what you really would like to do with the rest of your career. Then take a red pen and circle those areas and keywords that are most relevant for you. Write those words on a new piece of paper, and see if you can draw a line to logically connect them together. Plotting things out this way will also help you see if there are some weaknesses or obstacles that you need to solve before reaching your goals. And remember: Set realistic goals, but don’t underestimate yourself.

Now that you’ve refreshed your sense of “you,” take another look at that email and focus on the job description. Is it something that might be of interest? Does it excite you? Is it an office job, or will you be working remotely? If it would require relocating, is that an option for you? Do you want a change in your life, or do you want to keep your living situation pretty much as it is? Are you alone, or have you got a family? Answering these questions early on should give you a general sense of whether or not an opportunity is worth pursuing.

If so, use the information you gathered to write a good résumé (if you don’t have one already) and a cover letter tailored to the specifics of the job and company. Proofread it (carefully—and no, just using a spellchecker isn’t enough). Then send it off to the recruiter.

Study and Practice

Do your homework before the interview. If you don’t have much time for studying new things, at least review some important topics and think of the questions your interviewer might ask you. If you’ve got a friend or acquaintance with experience in the role you’re aiming for, ask him or her to give you some advice, or maybe even simulate an interview. If you say something wrong or incomplete in response to a question, your friend may be able to point out your mistakes and help you prepare stronger answers, so you’ll feel more confident on the day of the interview.

Try to get a good rest the night before the interview, then wake up early, have a solid breakfast, take a shower, and dress smart. If it isn’t an online interview, you’ll need to arrive at the office ahead of time. Give yourself a cushion to ensure you won’t have to rush. Something unexpected might come up, and you don’t want to be late or nervous or tired because you missed a bus and ran a mile.

Present Your Best Self

When you meet your interviewer, shake his or her hand firmly, and when you sit down to talk, keep calm, sit up straight, and maintain eye contact while speaking. Speak clearly and try to avoid interrupting the person you’re talking to, as well as long silences.

Why am I going over the basic social skills that your mother probably nagged you about when you were a kid? For good reason: 93 percent of our communication is delivered by non-verbal means such as body movements, gestures, intonation of the voice, and proxemics (distance between you and your interlocutor). It takes just one-tenth of a second for someone to judge you based on a first impression, and that judgment can be lasting. It’s harder to turn a negative first impression into a positive one than vice versa. It may strike you as superficial or even prejudiced, but appearance-based bias is a natural psychological mechanism, one that exists for all of us to some extent. So you may as well try to make it work for you, not against you.

If You’re Not Offered the Job

Hey, it happens to us all. And sometimes it’s for reasons we’ll never know, or never be able to control, so those situations aren’t worth dwelling on. But if you know you didn’t put your best foot forward in the interview, analyze what happened, and think about what you might do differently next time. We all fail at times, but that’s human—and helps you do even better next time. Don’t feel discouraged.

If You’re Offered the Job

Congratulations: You should feel proud of yourself. And remember that until you sign a contract, you’re not committed to the job. You may want to reconsider the offer or go for other interviews so you have a better basis for comparison. You are free to do what you want in your life, including accepting or refusing a job offer—or even trying to strike a compromise so a position will suit you better.

If you’re offered the opportunity to work remotely, your first instinct may be to go for it. Working remotely has some great perks, including staying home with your family, not having to relocate or commute, and choosing where you live without your job narrowing your options. You can even work in bed in your pajamas if you want; some people do. How awesome is that?

Well, let me tell you something: If you’re going to hold onto your job, working from home requires discipline. First of all, wake up early, prepare a schedule to follow even if you work at home, and adjust it as needed to create a good work-life balance. It may sound strange if you haven’t tried it yet, but people who work remotely may end up working even more than if they worked in a office.

So who should work remotely—and who might want to think twice about doing so? Well, if you are an experienced consultant with many years of work experience under your belt, a remote work situation could be perfect for you. But if you are young and newly qualified, I’d advise you to work in an office, if that’s an option. You’ll likely be surrounded by colleagues who share the same passion for computers and security, and you'll be able to cooperate with them on projects. Even if they have different roles and expertise, you may still benefit from talking to and learning from your co-workers.

If you want to improve your chances of getting hired as a security professional, work hard and prepare yourself in advance, so that you are ready when a job offer comes up. The recommendations I've given you may help you up your performance during an interview by, say 20 percent, but long-term preparation is what makes really a difference. There is an Abraham Lincoln quote that I really like: "Give me six hours to chop down a tree, and I will spend the first four sharpening the axe."

If the job you're aiming for is challenging, be ambitious. Don't worry if you don't know everything, as long as you have a strong foundation to build on. Challenges will make you grow professionally and boost your self-esteem, so don't avoid them. Especially if you are new or junior in the InfoSec field, my advice is to seize the chance and attempt the interview even if you aren't totally confident in your success.

If you'd like to read more in-depth advice on getting job-ready, check an article I shared on Peerlyst called "Cracking the InfoSec Interview for Fun and Profit."

Fabio Baroni *is an information security consultant and researcher specializing in vulnerability assessment, network and Web application penetration testing, malware analysis, and exploit development. A Linux/FOSS evangelist, Fabio's motto is "Trying to make the Internet a safer place."*

For more from Fabio, check out his website, or his Peerlyst page.

Chapter Four

Working with Recruiters

By Kris Rides

In this chapter, my goal is to help you become an attractive candidate to external (agency) recruiters, as well as increase your chances of being noticed by internal (corporate) recruiters. As a candidate who attracts recruiters, you will get several benefits, such as access to positions before they are advertised, or in some cases, before they are even signed off. Recruiters will also use their relationships with the decision makers to jump steps in the recruitment process, or potentially move you along the process, taking priority over other candidates' applications. When a recruiter gets some face time or dedicated phone time with a decision maker, the recruiter will have multiple candidates to discuss, but perhaps only the time to highlight one or two résumés. You want to be one of those. Below are the steps that you can take to become one of those highlighted candidates—a process that starts way before you even connect with a recruiter.

First Things First

First, let me start with few questions every candidate should have thought about, and have answers to, before he or she looks to move jobs or start a new career:

- Why do you want to make the move?
- What does your perfect job look like?
- What locations are you willing to consider?
- If relocating, is everyone involved in that decision on the same page?
- What salary and benefits do you currently get, or what did you get in your last role?
- What salary and benefits are you looking for, ideally?
- For the perfect job (location and role), what's the minimum salary and benefits you would accept?

Résumé

Next, you should think about your experience and how you are going to represent that on your résumé. I am going to be a little controversial here and say I don’t believe in paying someone to write your résumé. Résumés are personal, and although it’s good to take advice, and perhaps have someone review it, you want a résumé that reflects your personality, not someone else’s.

The basis of every résumé you send out should be a good standard format that you follow as you add relevant experience to flesh out the roles you’ve played during your career so far. Most jobs in InfoSec require good verbal and written communication skills. Your résumé is an example of your ability to communicate. Keep it factual, concise, and easy to read.

Here is a little feedback that we’ve heard repeatedly from InfoSec clients we have recruited for, which may help you prepare your standard résumé:

- Don’t include pictures or dates of birth.
- Don’t overdo it with logos, whether for companies or certifications.
- Keep your professional summary to one or two lines that give facts about your experience.
- Submit the copy as a Microsoft Word document. Many clients request that recruiters add a cover page that has the qualification notes they have taken, and PDFs do not allow that.
- Don’t go crazy with your use of columns or fonts. Keep it simple.
- Keep the résumé’s length to two or three pages, no more—no matter how many years’ experience you have.
- Experience from more than 10 years ago does not need to be described in detail. Company name, job title, and start- and end-date should be sufficient.

You now have a general résumé ready to send out, one that takes into account your previous experience and what you would like to move on to.

Next, think about how you are going to approach your job search. First, look at your network and ensure that you are maximizing it. Then, make sure you keep a good log of your direct applications, as well as where your agency recruiters are sending you.

Honesty Is the Best Policy

There are so many bad bits of advice out there that will only damage your chances of getting a job, so it’s extremely important to be honest with your recruiter. Here are some examples of the typical areas where candidates are tempted to stretch the truth—and the likely outcomes:

Area: Multiple job applications, or having a recruiter submit yours when you

have already applied.
Perceived outcome: Multiple applications increase your chances of getting noticed.
Actual outcome: If the company comes back saying your résumé is a duplicate, it looks like either you have poor control over your job search, or your recruiter hasn't done his or her job properly. Neither outcome is good for your reputation or your job search. In all my time recruiting, I have never seen a positive outcome from multiple applications. If you are truly unsure, give the recruiter a heads-up; it's very easy for him or her to find out if a client has seen your résumé already.

Area: Salary.
Perceived outcome: Inflating your current salary will increase the offer.
Actual outcome: Clients will generally require a W2 and previous paychecks to back up your earnings claims. If you lie on your application, you will immediately have the job offer pulled. Also, most external recruiters' fees are based on a % of the salary that they negotiate for you. This means it is in their interest to try to get you the best offer they can. The better the offer, the bigger chance you will accept—and they will earn their commission. Work with your recruiter to justify an increase in salary; if he or she is a specialist, they can advise you on what's happening in your market.

Area: Skills and experience.
Perceived outcome: Adding skills, experience, or qualifications will get you past the initial résumé qualification.
Actual outcome: Hopefully none of you are tempted to do this. There is nothing worse for a candidate than a hiring manager finding out that a candidate fabricated or exaggerated qualifications during a technical interview or background check. Clients often know that the job description is a wish list where they will need to be flexible. An honest candidate who says "I don't know X, but I have worked with their competitors" or "I haven't got experience in Y, but here is an example of me learning a new product at my last role," will get much further along in the process.

Area: Changing start or end dates.
Perceived outcome: It will help you avoid those awkward questions about gaps in your résumé.
Actual outcome: If you are successful in getting the job offer, a background

or reference check will very quickly show these gaps. No client will accept a dishonest candidate.

Finding a Good External Recruiter

If you are an experienced candidate looking to break into information security, I recommend creating a strong relationship with external recruiters that specialize in this niche. They will be able to give you advice on your best route into the industry, and how you as an individual can improve your chances of getting into the position you want. Look at who is advertising the types of positions you are interested in, in the locations you want to work. Don't be afraid to give those recruiters a call, and if you don't get through the first time, try again. Or connect with recruiters on LinkedIn, Peerlyst, or other professional social media sites and drop them a message.

Completely New to InfoSec?

Although there will be opportunities through recruiters, they are few and far between. Oddly enough, this actually doesn't have anything to do with your experience, and is down to business reasons. Companies pay external recruiters fees to find them the ideal candidates, and generally they do not pay fees to hire someone who needs to be trained to do the job. These positions are likely filled by direct applicants, so here are some recommendations as to how you can build your experience and maximize your chances:

- Look at the experience and qualities you have and how and where those attributes might apply in the information security field.
- Can you get involved with information security in your current company? An internal transfer is easier than a move to another company—especially if you're switching gears in your career.
- Use your company network. For instance, is there an information security person internally who would be willing to mentor you as you learn out of hours?
- If you work for a small company with no InfoSec budget, can you apply what you learn in your own time and help your company improve its security?
- If you have heavy experience in a specific industry, remember, a move within the same industry will be an easier change and will maximize the experience and credibility you've built up.

- Look for people via social media that have made the same career change as you are looking to make, and see if they will pass on some advice.
- If you’re currently not working, can you volunteer your experience to small companies that may have little or no budget and be willing to let you improve their security posture while you gain experience and references?
- Are you willing to do paid/unpaid internships at companies to build your experience?

My final note to all looking to either move to, or within, InfoSec, is that there is nothing that compares to building your network. Try to get to as many conferences as possible. Some are expensive, but others aren’t: For instance, BSides holds some of the best free conferences all over the country. If you want to attend and give something back to the community, that’s even better. You would be surprised how many conferences rely on volunteers in order to run smoothly. As a volunteer, you will have the time to interact with people who could be your future colleagues, bosses, or employees. Also, don’t forget to attend meet-ups of local chapters of organizations such as the Cloud Security Alliance, ISSA, ISC2, OWASP, etc.

Kris Rides *is the CEO of Tiro Security, a specialist information security recruitment and professional services company. He is a trained social engineering penetration tester and a founding board member of the Los Angeles chapter of the Cloud Security Alliance. Kris serves as an advisory board member for the Center for Cyber Security at California State University, Fullerton, as well as for CyberWatch West (CWW). He has been working in recruitment for over 15 years, with more than 95 percent of that time spent recruiting in the tech industry. To hear more from Kris, check out his website www.tirosec.com or his Peerlyst page.*

Chapter Five
How to Get Started in Cryptography
By Shamil Alifov

Regardless of your choice of career paths in the information security field, you will come across such terms as cryptography, encryption, cryptographic protocols, hashing algorithms, and so on. In this chapter, I will provide some basic notions of cryptography, provide a list of resources, and suggest some paths to becoming savvy in the field.

A Short Introduction

Cryptography or *cryptology* is a study of various techniques for achieving such aspects of information security as *confidentiality*, *authentication*, *data integrity,* and *non-repudiation*. These four key aspects are the primary goals of cryptography:

- **Confidentiality is the property that keeps information secret/non-available to unauthorized parties. For example, you want to send a message to your friend, but do not want anybody else to be able to read it. Thus, you need to apply some magic techniques to make your message unreadable by anyone besides your friend.**
- **Authentication relates to the identification of a user and data; in other words, it is a process of confirming that the data and user are genuine. As an example, say you get a message from a friend and you want to be sure that the message is really from your friend, not an unknown person who is impersonating your friend.**
- **Data integrity is related to ensuring that information is not changed or manipulated by unauthorized parties. The focus in on verifying that that the data or message that you've received is genuine and hasn't been altered by an unauthorized third party.**
- **Non-repudiation prevents a user from denying authorship of actions and information they've made. For instance, a friend of yours may promise to join your team in Pokémon Go, then refuse to admit they'd made that promise. To resolve that type**

of situation, there should be a trusted third party (say, some mutual friend) who will keep track of everybody's commitments.

Essential Terms

One of the central notions of cryptography is encryption/decryption. *Encryption* is a process of transforming simple text/data, called *plaintext*, into unintelligible form, named as *ciphertext*. *Decryption* is the inverse process of encryption.

Cipher is an algorithm that performs encryption/decryption. A *key* is a secret string of characters or symbols that is used for the encryption/decryption of plaintext/ciphertext. Sometimes, the term *cryptosystem* is used instead of cipher. There are two types of ciphers depending on the use of keys: *symmetric* and *asymmetric*.

Symmetric ciphers, also referred as *secret-key* ciphers, use the same key for encryption and decryption. Symmetric cryptosystems are divided into two groups: *block* and *stream* ciphers. In block ciphers, operations of encryption/decryption are performed on blocks of bits or bytes, whereas stream ciphers operate on individual bits/bytes.

Asymmetric ciphers, alternatively named *public-key* ciphers, use two keys, one for encryption and other for decryption.

Cryptanalysis is a study of techniques for "cracking" encryption ciphers, i.e., attacks on cryptosystems. And chances are you've heard about *hashing algorithms*, which involves taking an input of any length and outputting a fixed-length string, called a *hash*. Which can be used, for example, as signatures or for data-integrity purposes.

List of Resources

If you're just getting interested in the field, a good starting point for reading about cryptography-related topics is Wikipedia's Cryptography Portal.

Online courses

Cryptography I – Course by Professor Dan Boneh from Stanford University.
Cryptography – Course by Jonathan Katz from the University of Maryland.
Practical Cryptographic Systems – Course taught by Matthew Green at the John Hopkins University.
Practical Aspects of Modern Cryptography – University of Washington

course by Josh Benaloh and Brian LaMacchia.
Journey into Cryptography – Course in cryptography from the Khan Academy.
Applied Cryptography – Course in cryptography from Udacity.
Cryptography – Course from Cybrary.

Cryptography books

The Handbook of Applied Cryptography – A fundamental textbook in the area of cryptography written by Menezes, van Oorschot, and Vanstone. It covers all the needed topics and theory, making it an excellent reference.
Cryptography Engineering. Design Principles and Practical Applications – A great book by Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno. It will teach you how to think like a cryptographer and build cryptographic protocols.
Security Engineering – A textbook written by Ross Anderson, professor of computer security at University of Cambridge.
Introduction to Modern Cryptography – A textbook by the famous cryptographer Mihir Bellare.
Crypto 101 – An introductory book for programmers.
A Graduate Course in Applied Cryptography – A textbook by cryptographers Dan Boneh and Victor Shoup from Stanford University.
Applied Cryptography – This one is pretty old, but it is still one of the most used books in the field. Bruce Schneier’s book covers a lot of cryptographic algorithms with source codes in C.
A Tutorial on Linear and Differential Cryptanalysis – A detailed tutorial by Howard Heys.

Top blogs

A Few Thoughts on Cryptographic Engineering – From Mathew Green, a cryptographer and professor at Johns Hopkins University.
Schneier on Security – Bruce Schneier's blog.
Bristol Cryptography Blog – Official blog of Bristol University’s cryptography research group.
Outsourced Bits – Blog of Seny Kamara, associate professor of computer science at Brown University.
Light Blue Touchpaper – a blog of a security group at the University of Cambridge.
Ellipticnews – All about advances in elliptic curve cryptography.

Useful websites and links

Peerlyst – Social network for security professionals.

Cryptography Stackexchange – An excellent place to find answers to your questions.

Subreddit Cryptography – Subreddit where you can find news, discussions, and links related to cryptography.

IACR – Official website of International Association for Cryptologic Research. The website hosts an e-print archive of the latest results in the field. In the "Jobs" section, you can find open vacancies for positions related to cryptography and security.

Awesome Cryptography – A great list of cryptography resources and links.

An Overview of Cryptography – An overview of cryptography-related topics by Gary Kessler.

CrypTool – An educational tool about cryptography and cryptanalysis.

MysteryTwister C3 – International cipher contest initiated by CrypTool; a great place to learn and solve riddles.

The Cryptopals Crypto Challenges – A collection of 48 practical programming exercises that demonstrate attacks on real-world cryptosystems.

Learning Crypto

There are basically two ways of getting started in cryptography, either earning a master's/PhD degree in the field, or through self-study. Obviously, the latter path is way more challenging, so I'll offer some tips for self-learners.

Associate professor of computer science Seny Kamara of Brown University has a great blog post called "How Not to Learn Cryptography," in which he discusses potential strategies for learning cryptography and offers valuable advices. The blog post considers the theoretical aspects of cryptography and, at this point, I'll quote Bender from *Futurama*: "I am afraid, we need to use… math."

The books I've listed above provide introductory mathematical background in such areas as probability theory, information theory, complexity theory, number theory, and abstract algebra. After "fixing" the gaps in your mathematical background, start reading articles and try to comprehend them, even if they seem over your head at first. Try to develop your interests in one or two particular areas of cryptography, so you can "dig" deeper and deeper.

When it comes to learning applied (practical) cryptography, I'll pass on some advice that I was either given by others or figured out for myself:

- **The strongest advice is to read a lot about cryptographic algorithms/suits and their implementation. Focus on real-world algorithms, rather than on "textbook" ones. Familiarize yourself with cryptanalysis techniques and the common pitfalls in implementations. Research the failures of past, for example, the BEAST attack against TLS. And do not forget that security and cryptography go hand-in-hand**
- **Learn how to use cryptographic tools, libraries, and frameworks.**
- **Solve crypto challenges and publish your solutions. Working on The Cryptopals Crypto Challenges will provide you with a good learning curve, because you will improve your coding skills (if you need to) and demonstrate attacks on real-world algorithms.**
- **Implement cryptographic algorithms in the language of your choice. For example, consider the SHA family of hash functions, which is described in FIPS 180-4.**
- **Create and build your own algorithms just for fun, but do not assume that your algorithms are unbreakable. Try to break your own algorithms and find weaknesses. However, bear in mind this famous saying by Bruce Schneier: "Anyone, from the most clueless amateur to the best cryptographer, can create an algorithm that he himself can't break."**
- **Cryptography Stackexchange is a great place to learn. An excellent way to begin is by asking questions, then move on to providing answers to the questions of others.**
- **Participate in discussions, including on Peerlyst. Organize educational sessions about topics in cryptography for your peers or co-workers. Participate and contribute to open-source projects.**

Shamil Alifov *is from Turku, Finland. He has a bachelor's degree in applied mathematics and a master's in data security and cryptography, and is excited about pursuing a career in security and cryptography. To hear more from Shamil, check out his Peerlyst page.*

Chapter Six

How to Secure Your Data

By Yuri Livshitz

Data security can be based on the classic CIA triad: confidentiality, integrity, and availability. Here's a summary of the steps needed to achieve those three critical objectives:

Confidentiality

Confidentiality is the hardest data-protection goal to reach, because people (employees, vendors) need to have access to your organization's data—otherwise that data is useless. Even read-only permission that's limited to employees is sufficient to breach data confidentiality—and most organizations' confidentiality policies are much more relaxed than that.

In order to properly secure data, an organization should develop clear and precise standards of data classification. Usually data access is governed via a data-access control scheme.

A simple and sound way to develop one is using role-based access control (RBAC). Basically, RBAC organizes data access by group membership, limiting access to data based on employees' roles in the organization. For example, only workers who belong to the "finance" group will have access to finance department documents.

In order to achieve proper implementation of RBAC, access to data should be governed by data owners (usually department managers) and assigned to employees only after the data owner's signed approval. Organizations should limit access only to those employees who are approved by management on a need-to-know basis. In addition, procedures should be set up to ensure immediate permission removal in the case of termination or role change for an employee.

Senior management support is necessary in the data-governance definition stage. Management should also enforce disciplinary measures in the case of data-usage abuse. That will help prompt not only proper data usage, but also security awareness in the organization.

In order to simplify data governance, information should be segregated by levels of importance and risk, since it is very complicated to safeguard all the data in organization using the same standards. Some data has to be available to every employee, while other information is highly restricted, and should be accessed by management only. That sensitive data has to be protected by more security measures in order to safeguard it. In some cases, in order to archive "defense in depth," multiple security devices from different vendors are recommended.

A key technology for data confidentiality is data leakage prevention (DLP), a system that tracks specific sets of sensitive data. For example, DLP can issue alerts when sensitive files are copied to a USB, or credit-card numbers are shared. DLP is a great tool, but it requires precise, organization-specific data classification and alert creation in order to be effective.

Security by Obscurity

During the data-access planning stage, organizations should avoid "security by obscurity," a term for the practice of storing data in complicated formats or hard-to-find places. Obscurity is a poor security practice, because it creates a false sense of security. You believe that people won't find your data—but you may well be wrong. It's not wise to underestimate potential attackers' ability to unearth, and figure out what to do with, your data. As long as access to information is possible, you should create technical controls to guard that data.

Encryption

Sensitive data should be encrypted to prevent data access and misuse if media, servers, or endpoints are stolen or lost. All modern operating systems support full-disk encryption. Data in motion has to be encrypted using SSL/TLS. And you shouldn't allow user authentication via plain HTTP, since then employee credentials are sent in plain text, which can be easily sniffed by an intruder.

All Web applications in the organization should use HTTPS as a standard. Keep in mind, however, that encryption doesn't guarantee full data security, as data is always decrypted at some stage, which means it can be exposed.

Integrity

Data integrity is extremely important for any organization. It's especially critical in ones that deal with sensitive material such as health records or financial data. Damage to data integrity can have severe implications. In certain mission-critical systems, if data is modified by an attacker, it could lead to loss of life.

To protect data integrity, regular audits of information access and change are required. Data access has to be centrally logged, in case a bad actor manages to damage log data at the endpoint. Any employee who modifies sensitive data should do so using his or her personal user name. This allows non-repudiation, which means that an employee who modified data can't deny his or her action. Any "super user" access to sensitive files has to be strictly prohibited to guarantee non-repudiation across the organization.

To truly safeguard information integrity, you'll want to incorporate change management technology. Change management basically tracks changes to data, requires management approval of changes, or prevents changes forbidden by policy. Change management usually stores snapshot of data and tracks changes that are performed on it. Those changes are compared with system policy, and carried out only when they are in compliance with the policy. There are numerous change management products that can apply granular policies to track and prevent unwanted changes on almost any device, from storage filers to firewalls. One of best-known systems for change management is free SVN, which allows the detailed tracking of data inside a file, as well as granular permission control.

Audit and Monitor Data Access

Access to data and modification of data has to be logged and recorded in the central SIEM system. A SIEM system is important for data security, since it consumes multiple logs and allows those handling security to connect the dots and create a big picture that gives insight into multiple events. For example, it can draw attention to a user who sends abnormal amounts of data outbound, or one who connects to an unusual amount of servers. To utilize a SIEM system properly, its dashboards and metrics need to be set up to measure organization-specific data access activity.

A complimentary control that can greatly enhance data security is an insider threat detection system. Those usually use machine-learning algorithms to analyze log data to find users' behavior abnormalities and alert on those. This technology enhances threat mitigation when an attacker is in reconnaissance mode, allowing the detection and prevention of new and unknown threats.

Availability

It is obvious that data availability is critical to any enterprise. Yes, data that isn't accessible to anyone may be perfectly secure, but it's worthless to the enterprise if it can't be seen and used. Even more problematic is data that gets destroyed, which can create severe problems for a company's business and reputation.

Another thing to think about is that in the case of data damage, the organization may want to be able to restore older data. The timeframe within which data has to be fully restorable and usable should be aligned with an organization’s business goals and SLA policies. In some cases, highly critical data should be backed up in numerous places to ensure high data resiliency and the ability to carry out a successful restoration under a range of circumstances.

You should also be aware that your data could be damaged by malware that remains dormant for long period of time. Therefore, organizations should schedule data backups in order to guarantee business continuity in the case of a malware-related disaster. Backups should be created on a yearly, monthly, and weekly basis, and stored in an offsite location. It is critical to encrypt backup data in order to prevent untrusted access to it.

Data backup and restore capabilities, especially now that ransomware is a major threat, shouldn’t be solely IT’s responsibility. The information security team should be involved in backup policy planning and tests, since data restoration ability is critical to business continuity.

Following the CIA methodology outlined above will guarantee a good standard of data security in your organization. Though in order to have great data security, it is important to maintain security awareness among employees. Good security awareness among IT personnel and other employees will allow your enterprise’s technical controls to work effectively. Not only should employees receive continuous security education, the organization’s information security policy has to be clear—and regularly updated. Employee’s knowledge of and adherence to information security policy are critical to robust data security. [Note: Check out this chapter to read more on security awareness programs.]

***Yuri Livshitz** is an information security engineer at the International Air Transport Association (IATA), where he specializes in aviation security incident response processes. He has experience in incident response and security defense automation. Yuri holds both the CISSP and GCIH information security certifications. For more from Yuri, check out his Peerlyst page*.

Chapter Seven

Basic Network Security

By David Longenecker

A computer with no network connection is relatively easy to secure: if the only threats are those with physical access to a system, physical controls such as locked doors and armed guards (obviously depending on the value of the thing being protected) have worked reasonably well for generations. However, a computer without a network connection is of limited use in today's world. Communication, education, social media, streaming entertainment, business transactions, or remote control and equipment monitoring—all depend on information passing from one computer to another. And just like the front door of a bank can be used both by legitimate patrons and by robbers, a network connection can potentially be used both by authorized users as well as by those with malicious intentions.

At its most basic, defending a network—whether a simple home network, or a global enterprise network—starts with a few fundamental practices: deliberate use of passwords; keeping devices and software up to date; and managing what communication is allowed in and out of the network.

Manage Passwords

- **Change the default password on all devices and accounts.** Out of the box, most devices and network appliances come with an easily found password (often username "admin"/password "admin"). If you don't change the default password, it's a veritable invitation for someone else to take control of the device.
- **Use unique passwords for every device and account.** Reused passwords are a hacker's dream: all too often, a password will be stolen from say, an unimportant news site, only to be used to break in to one's bank accounts or take control of network security devices. Unique passwords per device and account ensure that if one password is stolen, *only* one password is stolen.
- **Use a password generator.** The human brain has unconscious biases and patterns, which often lead to predictable passwords. In a somewhat dated presentation, professional password cracker Rick Redman showed that a random 9-character password might take a

couple of months to crack. However, he is frequently able to crack half of the passwords in a given sample in less than 20 minutes, simply because of the predictable patterns we fall into. While the presentation is dated and the time periods are doubtless shorter with current computing power, the point remains: random is better.

Manage Devices

- **Keep device software and firmware up to date.** Android OS, Apple iOS, Windows, Mac OS X, and many software products have automated update features. To a lesser degree (though thanks to FTC action this year, this may be improving), network equipment also has such features. Turn them on. Software developers make mistakes—that's what the updates fix. If your car had a factory defect that might leave you stranded on the side of the road, and the manufacturer offered a free fix, you'd take them up on it, right? This is the same thing.
- **Turn off unnecessary features.** If you have ever participated in paintball or a snowball fight, you know it is impractical (if not impossible) to defend yourself in the middle of a field, exposed on all sides. Similarly, every program and service on a computer is a potential area of exposure to manage. By removing features and services that you do not use, you remove potential avenues for a malicious hacker to compromise the network.
- **Choose wireless network names selectively.** Most wireless routers have a default SSID, or wireless network name. This is convenient, but can have unintended consequences. Out of the box my router labels its wireless networks as ASUS and ASUS_5G. As does every other ASUS wireless router. In the world. Maybe you don't want to label your wireless network "123 hometown street" but it is a good idea to name it something a little less common than the default. Otherwise, any device you connect to your home wireless network will look for that network name everywhere it goes, and may well try to connect with a hacker's cleverly-named "ASUS_5G" network outside Starbucks.
- **Log in to network devices securely.** Many network switches and routers, both commercial and home-oriented, can be managed

through HTTPS and SSH, as well as HTTP and Telnet. The former are secured protocols that encrypt communication between you and the device, while the latter are non-secure protocols that communicate in the clear. An unscrupulous user on your network could listen in to the connection and sniff out your username and password, thus enabling them to log in to the device later. If possible, disable the HTTP and Telnet protocols entirely. If a device does not allow disabling these protocols, make a practice of logging in only over HTTPS or SSH.

Manage Network Traffic

- **Enable a firewall.** The primary purpose of a firewall is to stop undesired traffic from entering or exiting the network. If you have a wireless network, it almost certainly has a built-in firewall. If not, Windows has a built-in firewall that you can turn on by going to the control panel and opening the "Windows Security Center" panel. More and more entertainment devices are becoming Internet-aware, though (game consoles such as the Wii or PlayStation; set-top boxes such as Roku or TiVo; Blu-Ray players; and even televisions themselves). If these devices are connected straight to the Internet, they can become targets for hackers and used as an entry point to access your more valuable systems. If at all possible, they should be connected through either a wireless router or through a hard-wired router that has a built-in firewall.
- **Keep logs.** And look at them.
- **Manage name resolution.** A Web filter is commonly found on library and school computers, and frequently on corporate networks as well. It is intended to prevent access to inappropriate content, but in many cases will also prevent access to sites known to host malware. The simplest work by controlling the domain name system (DNS), the "phone book" for the Internet. There are a variety of free* DNS services that simply don't resolve website addresses that go to known undesirable** or malicious content. More accurately, they resolve such websites to a benign address that warns you about the nature of the site. In terms of "bang for the buck," this is one of the strongest additions you can make to

the security of your home or small business network. The linked blog post explains how this protection works, and shows some popular options.

* There's always fine print. Most of the “free” options specify “free for personal use only.” If you run a small business from your home, I'm not going to tell you when you cross the line from personal to commercial use (there are lawyers for that). I will tell you that several of these DNS providers offer commercial solutions for fees ranging from reasonable to eye-popping.

** Undesirable is in the eye of the beholder. Several available services provide the ability to allow or block websites based on categories, allowing the network administrator to tune the blocking to suit your personal or organizational acceptable use policy.

***David Longenecker** is a hacker and cybersecurity specialist based in Austin, Texas. To hear more from David, visit his website and check out his Peerlyst page*.

Chapter Eight

Security Awareness: The “People Part” of Information Systems

By Darrell Drystek

Security awareness is all about human behavior—not only training, but influencing and inspiring people to “do the right thing.” That is a skill unto itself, and those who master it will find that it opens many new doors for career advancement in the field of information security.

People are the reason we build information systems and strive to improve usability by introducing new technologies to deliver information more efficiently. People are the fundamental, but least predictable, part in every business process and information system. They always were, they always will be. And as you may already know—or will soon find out—people are the sole reason we must invest in and develop “information systems security controls.”

What Is Security Awareness?

The Information Security Forum (ISF) Standard of Good Practice (section SM2.4.1) provides a superbly concise definition: “Security awareness is the extent to which staff understand the importance of information security, the level of security required by the organization and their individual security responsibilities.”

Why Is Security Awareness Important?

Organizations spend millions on technical security controls, but it only takes one careless, frustrated, or uninformed employee to create a very large mess. The root cause of far too many security incidents is sloth or apathy—employees not following security policies and procedures, employees poorly trained in safe data-handling practices, employees falling prey to social-engineering scams.

Security incidents, even small incidents, cost money. Each and every avoidable cost is a drain on funds that an organization could put to better use on things like product development, marketing, improving employee compensation and working conditions, and so on. **The collective and individual state of employee security awareness directly affects the probability of the organization incurring avoidable costs.**

The Weakest Link Cliché

Have you ever noticed how random human behavior is? You can tell people what to do, what not to do, ask them if they understand, and watch them nod in agreement. Despite all that, they'll then go ahead and do precisely what you warned them against!

"People are the weakest link!" That cheeky little sound bite, crafted by some tall forehead and seemingly endlessly repeated by security professionals shifting blame for security failures, is a knife that cuts both ways:

- True. Yes, no matter how diligent, how well trained and motivated they are, users sometimes fail. Sometimes, they fail repeatedly. Perhaps they fail only once, but at the worst possible moment.
- And, guess what? The "People are the weakest link" observation also applies to all of you security guys or gals, whether you're established in the field or a newbie. If the state of security awareness is low at your organization, don't just complain about it. Instead, learn more about the situation, and take the appropriate steps to mentor the individuals who make up the "people part" of information systems. Teach, advocate, and inspire them to learn how to identify and manage information security risk, using the security controls program you've worked so hard to implement. And never forget that "the people part" you need support from includes everyone in the organization, from the boardroom to the mailroom.

The Enigma of Security Awareness

Every creature on this planet is born with a certain amount of "instinctive security awareness," a natural ability to perceive danger using various sensory detection methods (i.e., sight, smell, sound) and react in one of three possible ways: freeze, flight, or fight. With experience, we begin to further parse threats and adjust our reactions based on "learned security awareness." In a perfect world, we would all learn quickly how to assess the credibility of a threat and always react appropriately. Alas, people are all somewhat unique in terms of motivation, speed, and retention. And with information systems, achieving, maintaining, and improving the collective and individual states of security awareness is further complicated by frequent technology change, ever-morphing threats, and poorly designed and/or poorly executed security awareness programs.

An Effective Security Awareness Program

The uncomfortable truth about information security (or any form of security, for that matter) is that it adds a certain amount of overhead to every action considered or taken. While folks want and expect to be secure, they will only truly embrace security processes when they perceive demonstrable value.

An effective security awareness program is as much about marketing as it is about dispensing training. Fostering a security culture requires winning and maintaining support for the organization’s data assurance and controls program from employees at all levels of the organization. While security policies and procedures state *what* the employee must do, security awareness fosters understanding of *why* it is important for the employee to adhere to those rules and activities.

Here are the three “R”s for a truly effective security awareness program:

- **Relevant.** It must be appropriate for the organization in terms of operations, demographics, culture, the specific target audience(s), and applicable legal and regulatory requirements.
- **Recurring.** It must be managed as an ongoing concern, fostering employee awareness and support through continuing engagement, positive reinforcement, and remedial action when warranted.
- **Reportable.** It must provide measurable results on the progress of the program to stakeholders, as well as indemnification/evidence of action for legal or compliance requirements.

When properly done, a security awareness program will deliver exceptional value for the time and money invested. To demonstrate return on investment (ROI), show the monthly trend in undesirable/avoidable costs, including: volume of service calls to IT help desk, volume of employee downtime or service outages, and the sum of all traceable security incident response charges. When a security awareness program is effective, those undesirable/avoidable costs decline.

Want to Learn More About Building an Effective Security Awareness Program?

The author of this chapter shares tips and lessons learned in developing and managing a security awareness program in the Peerlyst.com series *Solving the Enigma of Security Awareness*.

Darrell Drystek *has over 30 years hands-on experience in developing and implementing innovative information systems and services solutions. He is a passionate advocate of improving information security risk management through improved security awareness. Darrell is an ISSA senior member (awarded 2012), as well as an ISACA program director and board member (Winnipeg Chapter). You can learn more about Darrell by visiting his profiles on Peerlyst.com https://www.peerlyst.com/users/darrell-drystek and LinkedIn.com.*

Chapter Nine

How to Respond to a Security Incident

By Yuri Livshitz

Security incidents happen suddenly, and an organization's key functions can be significantly damaged. Incidents create a high level of tension—which might escalate to panic. In order to avoid both the damage and the panic, an organization should be well prepared for security incidents.

Preparation

A key factor in a solid incident response plan is establishing a process to make incident response a structured, documented, and accountable activity. An organization should have a security incident response team (SIRT), which will investigate and document incidents. In large organizations, SIRT personnel will be based on InfoSec and security operations and control (SOC) groups; in smaller companies, the members of the SIRT team will come from InfoSec, IT, and even development teams. Senior management should set a framework for SIRT operation, and give the SIRT sufficient support to make investigation and response actionable. (Here's a sample framework.)

Application and system owners ought to understand the importance of security incidents and comply with SIRT requests for information during the course of incident investigations.

The SIRT is responsible for playbook creation, based on the organization's risk assessment of possible security incidents, and come up with plans for a structured way to react to them. For instance, it is important to rank incidents by severity level. It is critical to differentiate between security events (less serious) and security incidents (serious and requiring immediate action). A security event, like a virus on endpoint, might escalate to incident level, but typically it can be addressed via standard procedures or even automation. (Here's a manual on creating an incident response playbook.)

The SIRT should create a list with everyone's contact details and a summary of each team member's responsibility. Those contacts should be aware that in the case of an incident, they might be contacted. Perhaps the best way to do that is via an SMS alerting system with an escalation policy (PagerDuty is a good example of such a service). It's also important to create a structure of contacts outside the SIRT; for instance, those who will be responsible for public relations or legal activity should a high-profile incident take place.

Every step you make in reducing your organization’s threat surface by blocking ports or reducing access rights will save you an immense amount of work later on. It is highly advisable to do regular incident drills in order to verify that you have a proper incident response process in your organization. The development and maintenance of an incident response process should be considered an ongoing corporate project, complete with milestones and maturity-level checks. Only long-term investment and senior management commitment can guarantee an operational SIRT—and therefore, successful security incident mitigation.

An enterprise should also perform regular penetration tests using outside vendors to uncover blind spots in organizational defenses, and develop strategies for mitigating those newly discovered risks. Pen tests can also showcase the quality of your organization’s security monitoring.

Identification of Security Incidents

It is critical to identify incidents as early as possible to significantly reduce any damage that might be done by bad actors. For swift identification, security information and event management (SIEM) technology should be used. SIEM can integrate and correlate distributed events and alert on hostile or abnormal behavior. A best practice for incident investigation is to enrich your SIEM solution with external threat data. That external threat data can highlight known threat activity in your organization.

Another key factor in incident identification is a good data-analysis capability. It is vital that an organization’s SIRT measures baselines, and investigates deviation from those baselines. When doing so, it is critical to include logs from all the important systems in the organization.

It is important to remember that any security incident might just be just a deception designed to distract from another, more sophisticated, breach attempt. Therefore, when a security incident is discovered, only part of the security team should investigate it. Other SIRT members should monitor the other, non-affected systems with even greater diligence. If your analysis leads you to believe that vital company assets—or even people’s lives—might be at risk, immediately notify management and if warranted, law enforcement. You should act responsibly, putting people’s safety and security first.

Containment

IT and security should take swift action in order to limit an incident’s impact. When an incident is identified and verified, indicators of compromise should be documented and a high-priority ticket opened. Information should be gathered to determine all the servers, endpoints, and users involved. IT should limit involved users’ permissions, or even disable the users. IT should also limit affected systems’ network connectivity to prevent any communication between infected machines and healthy ones in the corporate LAN. The top goal of the SIRT during the containment phase is to protect critical systems and limit bad actors’ ability to move inside the network. Each step should be properly documented with sufficient details regarding why, how, by whom, and where containment actions were performed.

Eradication

After compromised systems are contained, SIRT should return breached systems to working order. This would be done using restore from backup, maintaining original storage as evidence. Disks of the breached sever can be later used for forensic investigation.

During the incident-eradication stage, it’s important to avoid any software reinstall on breached servers. Only healthy and verified backups should be used. If backup of the infected servers is vulnerable to a known exploit, it has to be patched before you connect it to the corporate network, to reduce the risk of additional breach.

The topic of forensics is beyond the scope of this chapter, but I’ll say this: If your organization requires court-admissible evidence following an incident, it’s advisable to consult with professional forensic experts, as only properly collected computer evidence is admissible in court. Performing forensics on your own can lead to a break in the chain of evidence; therefore, always consult an expert lawyer during evidence collection.

Recovery

Recovery is about restoring the service that got breached. During this stage, it is important to verify that service is fully available again, including data and previous customizations. Infected systems’ owners should verify that restored systems function properly.

Monitoring and verification of restored systems is of extreme importance to prevent any additional breach attempts. Attackers might use new tactics against previously breached systems; therefore comprehensive monitoring techniques should be used.

Lessons Learned

After a company has recovered from an incident and infected systems are patched or replaced, the "lessons learned" phase should begin. Security staff should complete all documentation that wasn't done during the previous incident response steps. Documentation should be detailed and structured to answer specific questions regarding why, where, and how the incident occurred. The final chapter of the incident report should include practical steps to take in order to avoid similar incidents. From this document, SIRT can create a new playbook to streamline the incident-response process.
This is also the time to set up a meeting with the owners of breached servers and applications, brainstorming ideas on improving the incident response process and contributing content that can be used to develop a detailed action plan to avoid similar incidents in the future.

Further Reading

The *Incident Response Handler's Handbook* is must-read material, as it lays out the methodology of the incident response process.

Yuri Livshitz *is an information security engineer at the International Air Transport Association (IATA), where he specializes in aviation security incident response processes. He has experience in incident response and security defense automation. Yuri holds both the CISSP and GCIH information security certifications. For more from Yuri, check out his Peerlyst page*.

Chapter Ten

Women in Security

By Cheryl Biswas

Where are all the women in information security? As breaches and threats increase the need for talented and skilled people in a growing range of InfoSec roles, our representation as women is not rising. We need to change that, because for women in security, our time is now.

The women I’ve met in our field have some of the most interesting stories to tell about their journey here. There really is no one defined path. Nor should there be. Security works best as an amalgamation of our experiences, insights, and skills. Think of how metal is forged, with one material being combined with others to give it strength, flexibility, resilience. That’s exactly what happens when women join the security ranks. Many of us have backgrounds in business, communications, education, and other areas where soft skills flourish. And it has been noted that those are missing from tech and InfoSec. There is a correlation here.

The threat landscape is always changing as new exploits are built, new attack vectors added. Threats evolve, and so must security, because attackers have the advantage both in time and resources. The fact is, you can’t defend against what you don’t see. We have watched recent and destructive transformations in malware—especially ransomware—move from the loss of time and money to the potential loss of life as hospitals became the targets and patients the victims. The attack on the Ukrainian power grid showed that much of our critical infrastructure is exposed to attack—and we can no longer assume the security of systems we once thought of as segregated and secure.

We need to change much of what we’ve been doing in security to step up and meet the new challenges coming our way. That means taking a more proactive approach and looking ahead, anticipating what might potentially become a target. In other words, taking a page from the Red Team Handbook and thinking like an attacker. Otherwise, we’ll keep losing ground and get caught up in clean-up after attacks.

This is where women, and what we have to bring into the field, can become a much-needed strategic advantage. Our differences will make us stronger by broadening our collective perspective—how we take in information, analyze the data, and do threat intel. But the reality is that there just aren’t enough of us here yet.

In her article for *CIO Online*, Maria Korolov summarized the key findings from (ISC)2's report "Women In Security" based on their 2015 Global Information Security Workforce Study. Here are the facts. Only about ten percent of information security professionals are women. And that number has actually gone down since 2013. What's more is that with regard to senior management roles, women comprise less than 9 percent. You can expect them to be highly educated and mature, yet their earnings are often less than those of their male counterparts.

In her piece on the subject, "Women In InfoSec – GRCers more than hackers? If so, so what? Plus bigger cultural questions," Sarah Clarke points out "the superficially happier story: InfoSec governance, risk and compliance (GRC) seemingly boasts 20 percent women (including moi)." She also raises an excellent question, one Peerlyst CEO Limor Elbaz posed on the site to kick off an interesting discussion: "Why GRC and not hacking?"

In my view, it comes down to how we perceive ourselves and our abilities in relation to what others believe we should be doing. Case in point: discovering my instincts are strongly red team, when my previous roles have been support positions. Yet a good attacker will understand defense positions in order to break security and find the weak points. It makes sense to know both. And why wouldn't women be as curious to figure out networking, or reverse engineer a block of code, when we are experts at untangling many other aspects in life? There is no genetic imprint that says we cannot become expert hackers—just a societal bias.

There may indeed be things that many women do differently than many men—and some of them may address areas people cite as lacking in InfoSec: soft skills, nurturing new talent, communicating to build bridges across the gaps. Probably because of societal conditioning, women tend to be stronger in those areas. But we are individuals, not stereotypes. Don't ask us to conform to some safe image of a business suit and requisite credentials. The real women I know in security march to their own beat, and how they present themselves is a confident assertion of who they are. The diversity among us reflects a rainbow of talent and skill. Accept us for who we are, as we are. Then watch us deliver what we were meant to do.

Let me make this assertion: we don't want to get the job because we are women, but because we can prove that we are the most qualified. Merit is the real differentiator, because we need the most capable and dedicated people filling security roles.

For a start, one thing we can do is really become resources for each other. Mentoring is a gift we give ourselves, as it reinforces not only our knowledge and technical understanding, but strengthens the bonds between us. We have tremendous role models who can nurture and mentor women just coming into security, as well as those of us who are already here. Then, we can pay it forward.

Many of us talk about how we found our way here, sometimes as a second or even a third career choice. That is what makes security so special to us. It’s our passion, our calling. Very much our destiny. We found a way to meet the challenges and overcome the obstacles to do what we love. For some of us, that meant making tough choices in terms of family and work priorities. We wouldn’t have to choose between the two in an ideal world, but the reality is that working moms have to juggle more responsibilities, and that means regularly having to choose between career or family in your daily routine. Security isn’t just a 9-to-5 job. The nature of things like breaches mean that situations will follow you home, and then there are the demands of learning to keep pace. You can’t always expect support from your family or your workplace. Talking about these choices can yield insight into not only the decisions we’ve made, but the social and workplace forces that shaped those decisions. And those discussions aren’t just good for women, but for men as well.

Something many women have voiced, and which is a hallmark of those in InfoSec, is our love of learning. Continuous learning fuels the information security field. Technology is ever-changing; constant new developments mean constant new threats and an expanding attack surface. We need to stay current and stay informed. That is how we can ensure that we are developing new skills for both detection and attack.

I think if women see more women visibly talking and writing about key security issues, it will send a message. Women keynoting talks at major conventions, or writing pieces for publications. On that note: we need to stop building panels without women. Include our voices and invite our contributions. This isn’t just a “geek guy” domain. It isn’t just about networks and coding. There are “big picture” issues, with overlaps into other areas. Attackers don’t take downtime, and the threats are constantly growing and changing. Security does not happen in isolation.

Here is my advice for other women working in technology. Believe in yourself and your passion. Don’t let people tell you who you are, and perhaps more important, who you are not. Look to others in the field, and let their journeys be a guide. Network where you are comfortable, perhaps in local groups, to build connections. Share your interests and grow your knowledge. There is much to be done, and we need you here.

If I had been scared off by the current biases, I wouldn’t be here. I am older; I am a woman; I have no formal training and am still working on my certifications. The initial lure of Stuxnet had me follow it down the InfoSec rabbit hole of learning. I took that passion and shared what I discovered—and that led to developing programs, weekly security briefings, going to conferences, and giving talks. I have met with resistance and made hard choices, but it has been so worth it. I’ve landed my dream role: threat intel as part of a national cybersecurity team.

Now it’s your turn to join me in saying, “I am a woman in information security, and I am here to stay.”

***Cheryl Biswas** is a cybersecurity consultant focused on threat Intel with KPMG in Toronto, Canada. She is fascinated by APTs, mainframes, and ICS Scada—as well as passionate about creating security awareness. She has a specialized honors degree in political science, has held a variety of roles in IT, and is ITIL designated. As well, she writes a security blog https://whitehatcheryl.wordpress.com and guest blogs, and has spoken at BSidesLV, Circle City, and BSidesTO. The views expressed here are solely her own, not those of her employer. For more from Cheryl, you can follow her on Twitter as @3ncr1pt3d, or on her Peerlyst page.*

Chapter Eleven

The Defender’s Changing Role

By Adrian Sanabria

Technology and IT are changing fast. One of the biggest changes we’re seeing is literally *a change in the pace of change*. Agile, continuous integration and continuous deployment are all about increasing the pace of software development with more frequent code releases. Add to that mobile, SaaS, and cloud, and the way security is traditionally designed just doesn’t work in our ever-evolving environments. Security’s role in the enterprise is changing, too. It *has* to change—and security professionals can’t afford to be left behind.

In fact, it can be argued that traditional security approaches haven’t worked out too well, so what do we have to lose?

A Layered Approach

Security isn’t “core” to IT—that’s one of the biggest reasons it is hard to sell to the business. What happens when you create a website without any security input? Nothing, at least, not initially. It works just fine. Maybe it works for a year or five, without any problems. It might just be luck or circumstance that takes a company’s website that far without vulnerabilities and oversights being exploited, but it’s pretty easy to see why so many don’t take security seriously, or put it on the back-burner.

Security exists to find and fill the gaps left by imperfect systems. Software has bugs. Architecture has flaws. Even hardware can have fatal issues that make it unsuited for public use until fixed. Security as a secondary layer is an important concept, because it enforces the point that security isn’t an entry-level field. To find these bugs and flaws, the underlying systems must be intimately understood. Is it possible to become an expert in database security without first achieving expert-level knowledge of databases? Perhaps, but the individual who did so would have serious knowledge gaps, and couldn’t hope to be an expert on the same scale as someone who spent years working as a database administrator prior to getting into security.

Becoming an effective security professional requires more than just a technical understanding of Oracle or TCP/IP or AWS or WebSphere. Experience interacting with non-security types and dealing with the daily challenges and constraints that exist outside security are equally as important as understanding core security principles. It is this non-security experience that allows the security professional to recognize when a recommendation is reasonable or unreasonable. It is what allows the security professional to see and accept the need for compromise when it arises. In addition, non-security experience gives the security practitioner credibility and the perspective necessary to empathize with others. Understanding individual employees' roles—sitting with them, watching them do their jobs—gives perspective and creates a baseline of understanding. Being able to commiserate and connect with employees on an individual level eases communication. Just a few minutes sharing off-topic IT war stories can build the *rapport* necessary to get things accomplished faster and more efficiently.

Key takeaways:

- Security is always a secondary or enabling layer
- Security must have direct knowledge and experience with the underlying technology layer in order to be effective at protecting it or recommending feasible solutions
- Prior experience with core disciplines goes a long way in earning respect and cooperation; practitioners are seen as having "paid their dues" and can speak the same language

A Changing of the Guard

To reiterate, IT is changing fast, and the speed of IT is changing. Software development trends that once might have been dismissed as fads are quickly becoming the norm. Most businesses with development shops and sizable IT footprints are at least dabbling with cloud, agile, and DevOps-associated processes and technologies. This is a world where major release cycles are measured in weeks or days, not months or years. To achieve these speeds, nearly everything in this world has an API and is partially or fully automated. To survive in this environment, security solutions and professionals alike have to not only understand these environments and tools, but be able to work in these mediums as well.
Issues with traditional security approaches:

- Few security teams can ever be "well-rounded" enough

- Security teams often aren't qualified to advise IT employees who are already subject matter experts (SMEs)
- Adversarial/dysfunctional relationships emerge when security is managed "from a distance" and infrequently communicates with other teams—except to deliver bad news in the form of demands
- Technology changes are fast and frequent; attackers adapt quickly
- Defenders and security tools adapt slowly

In the past, looking for a solution to a problem in security meant talking to some vendors, running a proof-of-concept, and signing an invoice. In this new environment, the question "why not build our own?" is coming up more and more often. With more practitioners who are also programmers, the question makes sense, and thus "build versus buy" is considered more often in decision-making processes. In addition, it is more common for security practitioners to work closely with IT, often literally, by being physically located at a desk adjacent to IT employees with non-security roles, rather than grouped together and isolated away from other parts of the business like the security teams of old.

Amazon's concept of the "two-pizza team" suggests that the ideal size for a group working on an IT or software project is one that can be fed by two large pizzas—say, six or seven individuals, max. Amazon ensures that at least one of these individuals is always well versed in security. This means that at least one member of the team is considering security requirements and the implications of design and architecture choices as the product is being built. Building secure from the start is exponentially cheaper and limits the likelihood of disruptive changes later on.

As IT changes, so must security.

Traditional IT isn't going away overnight. These trends are taking place slowly in some organizations, and rapidly in others. Those that change more slowly and have more complex and differentiated environments will see both paradigms co-exist for an extended period of time. Let's explore how this impacts both environments and teams:

- Traditional IT:
    - Goals: reduce and minimize reliance on non-essential traditional assets
    - As lower-level IT layers are outsourced (racking systems, running cable, managing datacenters, patching and managing operating systems), the need

    for the infrastructure-heavy security skillsets will decline
    - A large portion of existing IT and security knowledge lie in these lower layers of IT
    - The concept of bi-modal IT further confuses things (the idea that the goal shouldn’t be to eliminate traditional IT, but to achieve compromise)
    - Employees that don’t intend to or can’t re-educate themselves are in danger of being laid-off and replaced—this goes for security staff as well as non-security IT roles
- Cloud, or DevOps-first
    - Goal: increase agility through automation, reusable components and consistency
    - Goal: reduce likelihood of large failures by releasing fewer features more often
    - Goal: reduce inefficient spending by replacing long-term CapEx-based technology commitments with short-term subscription-based options
    - Development skills are needed at every layer—code is written to manage everything from core infrastructure components to business continuity, network behavior, and security policy
    - Start-ups looking to staff security teams are finding it more effective to hire developers and teach them security than to hire existing security professionals and retrain them
    - Security problems that are very difficult to solve in traditional environments are often simpler in new environments due to the programmatic nature of cloud-based technologies and the tools built to support them
    - Administrative and management consoles are consolidated; less consoles, more API interactions

Changing the Psychology of Security

What if we took things a step further and integrated security more deeply into IT? What would happen to the number of breaches occurring if every member of IT was a security expert? Consider the idea that, if an individual owns responsibility for an asset, whether that asset be application code, 50 Windows servers, or a datacenter, they *own it*—security and all. This is feasible, too, as each individual doesn’t need to be an expert in everything, only the direct field they are responsible for. In other words, the term “subject matter expert” or “SME,” when applied to a non-security field, should include security as well.

With this “distributed” approach to security, the goals of protecting against attacks and breaches seem much more feasible. Instead of a handful of overwhelmed security experts, most—if not all—of IT would be able to shoulder the brunt of that responsibility without security expertise outside of their key IT area. More than a decade ago, Elisabeth Hendrickson wrote a paper called *Better Testing, Worse Quality*. That outlines this issue, but with regards to the quality-assurance industry, not security. However, the issues and the situation she describes seem eerily similar to what we see in security. Why shift the responsibility for security to asset owners?

- No one knows and understands the technology’s opportunities, constraints, and dependencies better
- Traditional security departments can become a bottleneck for a company’s performance and progress—sometimes hamstringing the security team itself
- Little to no time wasted on remediation conflict: what to fix, how to fix it, when, and at what priority level
- Likely that fewer security issues arise due to security and technical SME knowledge residing in the same individual
- Drives the cost of securing systems down, in terms of labor, efficiency, and efficacy by getting it right early on more often

So, if more security resources get baked into the workforce, what happens to the security department and the traditional security role? These roles could shift towards becoming more of a consulting group within the enterprise. IT might run vulnerability scans, prioritizing and fixing problems, but they still need the perspective of those who can see the “big picture.” The time will come when only two of three critical vulnerabilities can be fixed in time, and the security team can assist in selecting the best two. Be assured that traditional security and IT roles won’t be going away any time soon. However, those staying behind and not adopting new skillsets may end up being seen as the new “mainframers” of the IT world, hanging on to their increasingly obsolete bare metal and waterfalls.

To compare the old and the new security practitioner, here are examples from real job postings:

Traditional security job postings ask for…

- Monitoring security alerts
- Manage network security
- Manage endpoint security
- IR/Forensics
- Penetration testing
- Vulnerability scanning
- Policies/Standards
- Compliance/Regulations
- Log management
- DR/BCP (Disaster Recovery and Business Continuity)
- Security awareness

Agile/DevOps shops are looking for…

- Influence design, architectural standards, processes
- “Ability to automate tasks”
- “Teach secure coding practices to software engineers”
- “Experience testing for vulnerabilities in Ruby on Rails applications”
- Identify gaps and recommend fixes
- Identify gaps and *build* fixes
- JSON, REST, XML, SQL experience
- “Experience with DevOps, CI/CD, Chef, Puppet”
- Routing, load balancing, network protocols
- *6 out of 10 jobs reviewed required skills with emerging technologies*

A final thought: **If you want to understand where security is going, stop looking at security, and start following IT innovation, trends, and changes.**

For more on this theme, take a look at my *Motherboard* piece “We Need to Change the Psychology of Security.”

***Adrian Sanabria** is an industry analyst at 451 Research, where he does his best to make sense of the security industry for clients. After over 15 years as a hacker, security professional, PCI QSA, and incident responder, he still sees the cup as half full. To hear more from Adrian, check out his Peerlyst page and follow him on Twitter.*