The Human Side of Cybersecurity: Careers

Cyber cops? In the 1990s, who would have thought that technology would offer an endless number of job opportunities fighting the bad guys? The technical nature of cybercrime offers information systems specialists unique career options in a world where cybercrime can be complex and frustrating to end users. It is useful to look at cybersecurity careers, with special emphasis on how one might make choices in a field that is always changing from a technology perspective but remains constant from the behavior elements that drive its proliferation.

Cindy Baxter, CISA, ITIL Foundation
Is director at What's the Risk, LLC. Her practice focuses on integrated risk control and process assessments for cybersecurity, privacy and business continuity/disaster recovery. She views risk management and control assessment as a chance to learn the nuts and bolts of a client's business and help them worry less because gaps have been uncovered and a stronger operating model can be built. Baxter draws upon her experience in banking, insurance, healthcare and technology after holding compliance and management roles at State Street Corporation, American International Group (AIG), Johnson & Johnson and AT&T. When she is not doing risk and audit work, she enjoys volunteering on climate and environmental issues that impact her community.

The History of Cybersecurity as a Profession

The outlook for working as a cybersecurity expert has never been better and has been in high demand all along. At the turn of the century when distributed denial-of-service (DDoS) attacks first occurred, network carriers scrambled to train existing staff and recruit as many professionals as possible. The small number of network security professionals struggled to keep up with what was then an unexpected surge in illicit activity, at the worst of all times, just as reliance on network technology was growing exponentially with the promise of the Internet. Network providers had dreamed of the business value of the Internet for marketing and sales, research, and government work, and they were not alone. Criminals with a technical bent seized their own opportunities, and cybercrime started a never-ending upward climb.

Activity that one would consider technology crime surfaced in the 1990s, focusing on phone scams and initially prompting organizations to hire those versed in law enforcement. Consider this common 1990s-era story of phone scamming that was used as a teaching example for network business sales teams (names and details are altered):

Jeff Dareme checked his presentation material as he gathered his belongings from his hotel room. It would be another interesting day on the traveling education road show to make sure ABC Network Provider's sales teams were keeping their business customers informed about the surging number of phone scams that were impacting customers and the company alike. After 20 years with the New York Police Department (NYPD), this job was a great shift away from the day-to-day stress on the beat. Sales teams always sat wide-eyed as Jeff retold stories of scammers at New York City's Penn Station, preying on unsuspecting victims. They always marveled at his tape recording of someone's feisty grandmother pushing back on the criminal caller, and they always looked heartbroken

when the grandmother succumbed to the criminal ploy. He enjoyed setting the stage for those in the class who thought these crimes only happened to the old and unaware. Jeff would switch to his business stories of successful Private Branch eXchange (PBX) scams at major corporations where unsuspecting receptionists would connect phone hackers to international lines and open voice mailboxes. The scenarios laid out, Jeff would end the class with the critical message to educate customers about these schemes. Even though he used the same story at each road show stop, it was always an interesting day at work. Who knew he would leave the police force, join the phone company and still fight crime?

The reality of cybersecurity is that it is a multitude of disciplines with many potential career directions. The story of Jeff Dareme discusses the onset of technical crimes back when pay phones, phone banks and PBXs were the enablers. New York City was a hotbed for tech scammers, as were other cities around the world.

The core competencies of investigative skills, technical know-how and a healthy skepticism about human behavior are still at the heart of security career success today, a key reason why ISACA®-trained professionals do so well in the field. Despite the myriad technical methods for committing cybercrimes, all activity is based on behavioral drivers, whether they are the desire and need for money, or the desire to promote a political, religious or other ideology by shutting down the ideologies of others.

It is an interesting parallel to the risk assurance discipline, where the abilities to recognize and assess inherent risk allows establishment of preventive controls, while IS auditing expertise leverages the ability to uncover issues and determine solutions that lead to sounder, more stable operating environments. Understanding criminal intent and reacting in the most effective manner have led to a boom in detective careers such as forensics analysis, while education and the need for awareness have caused a career surge regarding preventive disciplines such as cyber consultants and ethical hackers.

Every industry, every nonprofit, every mom-and-pop business needs attention.

Cybersecurityventures.com called for the cybersecurity talent crunch to reach 3.5 million

"THE REALITY OF CYBERSECURITY IS THAT IT IS A MULTITUDE OF DISCIPLINES WITH MANY POTENTIAL CAREER DIRECTIONS."

unfilled jobs globally in 2021.[1] Research on this number was corroborated by multiple sources and went so far as to assert that "every IT position is a cybersecurity position now."[2] The timing for the ISACA professional has never been better.

High-Demand Careers

Today's high-demand cyber job market hosts endless possibilities in every geography. One cyber position can easily lead to another position, giving the career seeker endless opportunities to grow in expertise. Career paths in play include some of the following, with openings noted as of 24 June 2021:

- Information security auditors. Listings on Indeed.com show 12,900.
- Ethical hackers. Indeed.com showed more than 650 openings.
- Cybersecurity forensics/information security analysts showed 131,000 unfilled jobs based on US Bureau of Labor Statistics data for 2019, and an increase of 31 percent is anticipated by 2029.[3]
- Global network engineering, still a focal point for cybercrime, showed job openings in excess of 16,500, on *Indeed.com*.

There are even more possibilities from which to choose, according to CyberDegrees, including these top-10 jobs by salary:[4]

1. Chief information officer (CISO)
2. IT security architect
3. IT security manager
4. Security assessor
5. Security engineer
6. Information security consultant
7. Security director
8. Penetration tester
9. Incident manager
10. Information security specialist

Enjoying this article?

- Read *State of Cybersecurity 2021, Part 1. www.isaca.org/state-of-cybersecurity-2021*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

With so many possibilities, how is one to choose the best cyber career path?

Know Thyself

The best starting place to determine where career success lies is with you. Do you prefer remote work? Do you like the thought of pulling up stakes and living somewhere else? Do you like the excitement of day-to-day crisis management? Do you feel that sense of accomplishment when you crack and block an attack, or do you feel you have made a difference when you have spent time with others, teaching them how to avoid cybercrime pitfalls? Knowing oneself can be a challenge. Personality adds a further dimension to career assessment. Job seekers often turn to personality tests with a mix of curiosity, cynicism and acceptance, while assessing fit.

From an enterprise perspective, personalities are typically divided between individual contributors and managers. There are four broad personality categories broken into two larger categories often used for consideration:

- Individual contributors prefer independent work and thrive on owning the outcome based on their knowledge and research:
  1. **Individual contributors-analysts**—Enjoy detail work and consider data from a logical and objective perspective to confirm their work conclusions.
  2. **Individual contributors-creatives**—Imagine solutions that may be unconventional. Creatives thrive in a changing environment and are not afraid to create change themselves. They are more apt to take risks than individual contributors-analysts.
- Managers prefer to lead others for a collective outcome. In addition to working with people to provide coaching, they are comfortable with program administration in support of their group, such as payroll, employee education and team meetings:
  3. **Manager collaborators**—Look to facilitate the work of others and feel a sense of accomplishment when those working for them achieve success. Their patience enables consensus and encourages group conversations to arrive at solutions:
  4. **Manager commanders**—Are not afraid to take the lead when deadlines loom or emergencies occur. Successful manager commanders have mastered the art of leading a group with enough transparency and encouragement to avoid the pitfalls of group dissent that can undermine completion of an on-time solution that meets the required results.

Personality assessments offer one of many considerations for career selection. Another consideration is adeptness with technology. In the ever-changing world of cybercrime, being a technology generalist is more important than understanding a specific technology given the rapid change of technical innovation, especially by hackers. Instead of a specific expertise, the ability to detect unusual activity, behavior or trends and a willingness to ask even what seems to be basic questions is most important. I have been amazed time and again when I have uncovered gaps, unusual activity and even illicit behavior when I was certain I knew a lot less than those I was questioning. One can learn to abandon concern over asking "dumb" questions or requesting even more data, and once that happens, cyber stories start to unfold.

> "DESPITE THE MYRIAD TECHNICAL METHODS FOR COMMITTING CYBERCRIMES, ALL ACTIVITY IS BASED ON BEHAVIORAL DRIVERS."

Brooklyn's Story

Beyond personality and work/life consideration, how else can one select the best fit job? It is helpful to list the positives and negatives of the career choice, which requires research to determine those pros and cons. Brooklyn's story shows how she sorted through her options while staying true to herself and her lifestyle needs.

Brooklyn Puente was intrigued by her career options after attending a local ISACA conference in New Jersey, USA. Initially interested in risk management, Brooklyn studied and passed her Certified in Risk and Information Systems Control® (CRISC®) certification,

planning to use her skills in the insurance industry where she currently worked. She liked the way she could quantify financial, regulatory and client risk to create emerging insurance products. Formulas made sense, application logic complimented the outcomes she expected and her personal spin on the data made new products more than a set of numbers on the page. She also liked the flexibility of risk management, which let her consider any industry should she decide to move to a different organization at some point. The conference opened her eyes to new possibilities. Security topics were clearly the buzz that everyone was talking about during the general session. Encouraged by what she learned, Brooklyn opted for a CSX-P certification. She passed the tests and, liking what she did to get ready, she decided to go deeper and pursue the Certified Information Security Manager® (CISM®) certification. With her CRISC, CSX-P and CISM credentials in hand, Brooklyn felt she had options to do everything she liked, but she faced a new conundrum. Should she stay with her risk management job where she had the latitude to craft new insurance offerings using risk-based modeling, or should she become a cyberprofessional?

To help her decide, Brooklyn reached out to several people she met at the conference, a bit outside of her comfort zone, but she had heard too many stories about the value of networking and was willing to grit her teeth and give it a try. She researched the jobs that were most appealing and took notes on the skills that were required. Based on her research, she developed several interview questions for those she would contact, which she felt would make the results objective and easier to correlate to a final job choice. She decided to interview five people, enough to draw reasonable conclusions. Finally, after collecting the data, she decided to take a personality test based on a suggestion brought up by an interviewee who found it useful in his job search.

The information Brooklyn collected from the interviews confirmed that day-to-day cybersecurity work and the more strategic aspects of a cybercareer would be good to consider. She had sorted through options, first at her own company and location, and then looked at a few other organizations and locations. She noted working hours and options for remote vs. in-person office requirements. She thought about management options but decided against it, at least for now. There was too much fun to be had by doing her own work without worrying about the needs of others. Plus, the sense of accomplishment she got from calling something her own was important at this point, especially since she had amassed some work experience and had studied hard to earn her certifications. It was time for some personal recognition with pay to match. She honed the list of job opportunities down to two fields, ethical hacking and cyberforensics. As she considered the job details and her research, the choice was clear.

> "IN THE EVER-CHANGING WORLD OF CYBERCRIME, BEING A TECHNOLOGY GENERALIST IS MORE IMPORTANT THAN UNDERSTANDING A SPECIFIC TECHNOLOGY."

Brooklyn's story resonates with many IS risk and audit professionals. The ever-growing field of cybersecurity need not be a daunting evaluation, but there is comfort in collecting information and networking with others before jumping into something new. Still, the amount of research needed depends on individual comfort regarding how to assess whether the position is a good lifestyle, financial and personality fit. Growing from a new position to another position is also a strong possibility, and that reduces the risk of getting "stuck" with a decision that does not turn out as expected.

Conclusion

The list of activities to consider before applying for a position is doable for almost anyone:

- Consider a personality test and keep the results in mind while examining the job requirements.
- Think about lifestyle flexibilities that are important. For example, incident and recovery management often requires in-office presence and a great deal of face-to-face time with those impacted. Hours can be as long as the incident and recovery efforts continue. Another example is analyst work, which can often be done remotely and with more flexible hours.
- Consider pay requirements for your lifestyle.
- Research both the enterprises under consideration and the job opening itself.

> THE LIST OF ACTIVITIES TO CONSIDER BEFORE APPLYING FOR A POSITION IS DOABLE FOR ALMOST ANYONE.

- Network with others. Use LinkedIn, attend conferences and get contact information. Do not be afraid to bring up your search even at the next virtual gathering or in-person event you attend.
- When you network, take notes and follow up with thank-you notes. That effort can lead you to even more contacts.
- Write out a positive and negative attribute list for each job considered. As you apply and interview for the positions, refine the positive/negative list based on what you learn.

And, most important, keep learning. ISACA is continually offering the latest in cybersecurity education. ISACA cyber certifications, in my opinion, have more than kept pace with the cybercrime industry. It is a great time for career seekers and learners alike.

Endnotes

1 Morgan, S.; "Cybersecurity Talent Crunch to Create 3.5 Million Unfilled Jobs Globally by 2021," *Cybercrime Magazine*, 24 October 2019, *https://cybersecurityventures.com/jobs/*
2 *Ibid*.
3 US Bureau of Labor Statistics, "Computer and InformationTechnology Occupations," *Occupational Outlook Handbook*, USA, 19 April, 2021, *https://www.bls.gov/ooh/computer-and-information-technology/home.htm*
4 Staff Writers, "Cybersecurity Jobs: Overview," CyberDegrees, 3 June 2021, *https://www.cyberdegrees.org/jobs/*