Becoming a Cybersecurity Expert

A career guide for professionals and students

Introduction

Cybersecurity is a new name for the computer and network security profession in a world where everything is increasingly connected to everything to communicate and exchange data. As we further discuss below, the cybersecurity risk landscape is changing as more consumers and businesses are shopping and communicating online, storing and processing data in the cloud, and, embracing portable, smart, and Internet connected devices to automate tasks and improve lives.

Cybersecurity has become a hot topic for two main reasons. First, increased hacking cases often result in compromised business information including personal information of customers which must be protected under various privacy and security laws. And second, there is a serious shortage of cybersecurity talent according to many research studies and various countries are scrambling to find the best way to develop cybersecurity experts. In fact, because of the global shortage of cybersecurity experts, some countries such as Australia have expressed a desire to become the leader in cybersecurity talent export to other countries as a way to generate revenue. The cybersecurity talent shortages are expected to affect many countries and last for many years which is why this guide is written to discuss the risk, encourage professionals in related fields and students to pursue a career in cybersecurity, and, seek the support of businesses and governments to promote the profession.

About this Guide

This guide was produced by Identity Management Institute to provide career information and answer common questions for becoming a cybersecurity expert.

This eBook intends to provide a short yet comprehensive guide to encourage and educate others for becoming a cybersecurity expert. With the knowledge in this guide, interested candidates will learn to pursue a career in cybersecurity and reap the benefits of a dynamic, rewarding, challenging, highly in demand, and respected career.

Cybersecurity Risk Landscape

One of the main objectives of cybersecurity is to protect data but high impact and frequent data breach incidents have increasingly challenged the cybersecurity community due to some key factors that we need to consider.

First, businesses collect and retain huge amount of consumer and other valuable data in raw and structured format which are purchased or collected from many sources including user-provided data in social media. This is attractive to hackers as honey is attractive to bees. Second, hackers seem to always be ahead of IT security professionals and take advantage of poorly designed or configured systems to access and steal data before security experts have a chance to identify and fix the security loopholes.

This could be due to the lack of motivation, ownership, and up-to-date cybersecurity skillset. Third, users who are entrusted with privileged access to critical systems and data are easily fooled with phishing and other scams due to lack of adequate education. In fact, over 90% of all data breach incidents in cyber attacks are due to stolen access information from employees in phishing scams. If employees can be educated enough to recognize identity theft schemes, organizations can prevent the majority of cyber incidents if they continue to maintain a strong network security posture.

And finally, the widespread use of various mobile and Internet connected devices which store and share data with other devices and their owners will present even more opportunity for hackers to challenge the IT security community. It is estimated that drones will be a $90 billion industry within a decade and Gartner estimates there are 6.4 Billion "Connected Things" today which are expected to grow to 21 billion by 2020 out of which over 13 billion will be household devices used by consumers.

Human error has been identified as the biggest culprit for data breaches according to many studies. One way to address this issue is to eliminate or reduce user responsibility for managing device security by automating security enforcement. As an industry, we must foresee the risks before they are materialized and be at least one step ahead of the hackers by strengthening the system security controls to the point that there are no known vulnerabilities to the hackers, at least not before we have a chance to fix the issues. With regards to human error and its relation to data breaches, the biggest cybersecurity issue is the powerful access that we give to our privileged users without proper education about the risks, their responsibilities, and consequences of policy violations. Often, users with privileged access are targeted with spear phishing techniques to steal their account information which is the most targeted, easiest, and least costly approach to gain unauthorized access to systems and data. In fact, this type of unauthorized access can hardly be called hacking since the intruders do not independently figure out a way to access the system. But rather, they rely on the naïve employee through phishing, pretexting, and spoofing scams to gain access codes and other information.

Why Identity and Access Management Matters in Cybersecurity

There are five main reasons why identity and access management matters most in cyber security and data protection.

1. First, identity and access management ensures that legitimate parties have the right access to the right resources at the right time while keeping illegitimate parties out of systems. This is probably the most important role of identity and access management in information security. Various parties which may include employees, contractors, vendors, customers, and even devices need access to systems and as such require the establishment of their identities and access provisioning during the on-boarding process. Subsequent processes are needed to remove access as soon as the relationship is terminated and monitor activities to detect hacking attempts or unauthorized activities.

2. Second, parties who have been granted system access pose the greatest risk because they are often the identity theft targets of hackers who need their access privileges to gain access to systems. Regardless of access management mechanism deployed, the easiest way for hackers to gain access to a

system is to steal an existing access. One of the methods for stealing an existing access and gaining unauthorized access to systems is phishing emails which is the root cause of the majority of hacking and data breach incidents. This means that regardless of our information security investments and high tech security systems, access can be compromised if existing access is not protected and often parties with existing access pose the greatest risk and this is why identity and access management matters in cyber security.

3. Third, parties with access to systems and resources make judgment errors when confronted with phishing attacks and other hacking methods by giving away their sensitive access information to hackers. This is often due to the lack of education and training for teaching the parties about the importance of keeping access information confidential and the techniques for detecting and mitigating hacker attempts to steal their information.

4. Fourth, parties with access to systems and authorization to perform tasks are often the ones that are well positioned to commit fraud and cover their tracks to avoid or delay detection. Corrupt insider risks are real and this is another area where identity and access management solutions can be leveraged to monitor user activities and detect unusual transactions based on predetermined criteria.

5. And lastly, identity and management matters because as regulatory requirements expand for customer identification, suspicious activity detection and reporting, and identity theft prevention, identity and access management solutions are needed to validate, track, and report on identities for compliance purposes. From a regulatory compliance standpoint, IAM services help companies manage various requirements such as Know Your Customer (KYC) and related Customer Identification Program (CIP), transaction monitoring for Suspicious Activity Reporting (SAR), and Red Flags Rule for identity fraud prevention.

As you can see, identity and Access Management (IAM) is extremely complex and critical in managing information security risks. Although technology is an important part of identity and access management, effective IAM also requires processes and people for on-boarding users, granting and removing access, and keeping unauthorized users out of systems. Once an IAM strategy is established, technology can be deployed to automate the identity management lifecycle and reduce errors which often exist in manual processes.

Identity and access management risks continue to evolve worldwide as new threats and solutions are introduced, and laws are implemented. Specifically, cyber crime, identity theft, and related fraud are on the rise and various governments are scrambling to address privacy of consumers and manage risks through regulations.

As companies become more aware of the urgent need for managing identity and access management risks, deploying systems, designing processes, and employing skilled staff also become apparent and are brought to the forefront for managing risks. IAM is a risk-based function that can help an organization

achieve competitive advantage through state of the art technology such as biometric authentication to lower operating costs, increase efficiency, and reduce the risk of security breaches.

Industry Statistics and Salaries

The cybersecurity market is expected to grow from $75 billion in 2015 to $170 billion by 2020. According to industry analysis, more than 200,000 cybersecurity jobs in the U.S. alone were unfilled in 2015 which is up 74% over the past five years and it is estimated that the global cybersecurity job postings to be around one million.

The demand for cybersecurity jobs is expected to outgrow the supply of cybersecurity experts. Consider that 6 million cybersecurity related jobs will be globally available by 2019, with a projected shortfall of 1.5 million cybersecurity experts.

The U.S. News and World Report ranked the information security analyst career eighth on its list of the 100 best jobs for 2015. It stated that the profession is growing at a rate of 36.5% through 2022.

Cybersecurity experts typically earn an average salary of about $6,500 more than other IT staff according to published reports. The most recent median pay for an information security analyst is $88,890 per year, according to the Bureau of Labor Statistics, which also states that the typical education required for entry level jobs is a Bachelor's degree. The lowest 10% earn less than $50,300, and the highest 10% earn more than $140,460.

Benefits of a Cybersecurity Career

Companies are increasingly acknowledging the need to hire and retain cybersecurity experts as evidenced by the global shortages in talent pool. As mentioned, some recent studies suggest that there will be a shortage of 1 to 2 million cybersecurity jobs by 2019 in all levels and disciplines which we will cover later. The shortage is almost 10 times the shortage that exists in 2016. As a result of this shortage, salaries are also expected to increase for cybersecurity experts as many companies whether large or small and public or private increasingly worry about security breaches and their negative consequences.

Career Change

The first question that some candidates may ask themselves while reading this guide is does a cybersecurity career make sense for me given my education and past experiences, and can I successfully transition? Anyone can become an expert in any field if they determine exactly what they want, decide to commit, and dedicate themselves to the career transition by designing and executing a career transition plan. You can become a cybersecurity expert no matter what your current level of knowledge and experience is but it might just take you longer than someone who has worked in the information technology field and who has some knowledge of the IT world. After reading this guide, you might even decide that cybersecurity is not for you. This guide is not about teaching you about cybersecurity skills because there are so many credible resources out there that already do that. This guide is about giving you some information about the cybersecurity industry and showing you a strategy that will help you create a roadmap for becoming a cybersecurity expert.

Cybersecurity Career Options

As mentioned earlier, many of us have education and professional experiences which can be enhanced to advance our careers in cybersecurity without starting all over again. For example, you may have a degree in a Computer Science or you may have had exposure to IT management, computer programming, system administration, and network engineering. These skills can be quickly expanded and applied to cyber security in a variety of functions.

On the other hand, your background may be outside of IT security such as auditing and enterprise risk management which gives you the ability to quickly assess risks and see the big picture. All you need is to learn the IT security risks and controls to become a cyber security expert in your chosen niche filed.

Cyber security experts have a wide range of career options across a variety of industries. More importantly, industries such as banking, finance, healthcare, government, and retail which collect, retain and process consumer information have a pressing need for such experts.

The cybersecurity field includes generalists and technical experts at many levels and is comprised of thought leaders and governance experts, executives and managers, consultants, technical product managers, network and cloud security experts, technical writers, vulnerability testers, white hat hackers, security architects, system security engineers, and cryptographers to name a few. As in any other career, cybersecurity experts also need to have interpersonal skills to communicate with peers, clients, and employers.

That said, cybersecurity candidates must be open minded as there are so many different paths that candidates can take. Some want to be cybersecurity program managers or auditors while others may prefer a more hands-on technical approach to cybersecurity. As data is generally processed and stored in digital form for the most part, all candidates must have sufficient technical knowledge about IT and computer networks, IT security threats, and the best possible solutions. Depending on the chosen cybersecurity field, some may need more in depth technical knowledge than others but almost all cybersecurity experts must have computer and system network security knowledge and interest to succeed.

Preparing for Transition

A decision to whether or not pursue a career in cybersecurity depends on many factors including your interest in information security, commitment, and current skill level.

Some cybersecurity candidates may already be in a position to leverage their existing skills or opportunities in their current environment to make a relatively quick career switch. For example, IT professionals with very good technical expertise can cultivate and turn their current skills into a viable cybersecurity career. Or, professionals in system security audit and IT risk management can find a niche within the cybersecurity field where they can apply their analytical skills to cybersecurity and vulnerability assessments.

In addition, those in environments which offer opportunities for further education and training must seriously consider the available support to enhance their careers. For example, government agencies and the military not only need the best cybersecurity experts and offer great career opportunities in cybersecurity, but they also offer some of the best education and hand-on training to their staff. If you are already employed by these entities or plan to join them, consider leveraging their resources to improve your career.

Educate Yourself

Many information security professionals hold a bachelor's degree in computer science, information security, or related technical field.

Although it's not always necessary to have a college degree for a cyber security job, it's increasingly becoming a requirement in cybersecurity job descriptions due to the complexity of our connected digital world. A college degree doesn't just enhance someone's IT skills but also other skills which are needed for a successful career such as writing, analysis, critical thinking, communication, project management, and presentation.

But what if you don't have a college degree? In some cases, experience and professional certification which we will cover later can replace a college degree. There comes a point in our careers when experience has more weight than education but if you are just starting your career, a college degree and professional certification will certainly enhance your chances of getting the job of your dreams. That said, you don't have to attend a super expensive college and there are many options that can even help you such as getting a degree online while you work and if your employer covers portions of the tuition, you should definitely look into it. There are also grants and scholarships available to qualified candidates. For example, Cisco introduced the Global Cybersecurity Scholarship program which consists of $10 million in program budget to increase the pool of talent with critical cybersecurity proficiency. There are probably other sources of financial support and many more will be forthcoming.

There are many other ways that candidates can gain education. For example, you can find and read many articles written by experts in a variety of cybersecurity areas. Reading articles and news is a common practice for all cybersecurity experts even those with many years of experience because new threats and solutions are constantly introduced as we embrace new technologies and trends as a society.

There are also many specialized boot camps with hands-on training which are a week long and somewhat expensive. But they present a great opportunity to learn from experienced instructors.

Below are some general tips for enhancing your knowledge:

- Take college courses whether you pursue a degree or not,
- Attend conferences and seminars,
- Join professional associations,

- Explore Wikipedia topics,
- Research various cybersecurity topics on the Internet,
- Read IT and security books, magazines, and blogs,
- Subscribe to cybersecurity newsletters and news channels,
- Participate in online discussions,
- Write articles based on research and recent news, and
- Teach yourself using any other methods such as building and securing computer networks at home.

Gain Experience

Gaining as much practical experience as possible is necessary to make yourself more valuable and promotable. Don't overlook all the skills that you can learn from practical experiences. If just starting your career, get into a related field and start improving your resume and professional experience. In fact, working while you consider going to school can save you time and possibly money if the employer offers financial support for employee education.

Build a Network

Once you become a cybersecurity expert, you need a professional network to support you for finding and keeping a job. Consider the following tips:

a. Join LinkedIn groups as well as professional networks and security organizations,
b. Attend local security group meetings and events,
c. Collaborate with cybersecurity teams and projects,
d. Volunteer at cyber security and IT conferences,
e. Participate in information security projects, and
f. Offer your expertise in discussion groups.

Improve Soft Skills

No career can be successful if you don't have sufficient soft skills and political acumen. Cyber security professionals must have great analytical and communication skills to succeed. Even if you end up having your own cybersecurity company, being able to attract and retain customers requires great customer service, understanding customer needs, being punctual, and communicating your company services effectively.

Although soft skills can also be taught, experience and learning from mistakes is critical in mastering soft skills. The key is to be aware of the mistakes to correct them as soon as possible and avoid repeating them.

In the IT world, one of the challenges of highly technical professionals is their inability to communicate with non-IT persons such as business executives and board members. The other challenges that IT professionals struggle with or fail to master is understanding the business in which they operate.

If cybersecurity experts can effectively understand their industry and business as well as IT security risks and solutions, and clearly communicate their thoughts by tailoring their message so the intended recipients of the message understand the message, they will succeed and go very far in their careers.

Pursue Certification

Whether you are currently employed or considering to join the workforce, professional certification is extremely valuable and even a requirement for many job postings. In fact, certified professionals in all fields tend to earn more than their peers who are not certified.

The cybersecurity industry is wide and offers many specialized training and certifications. Individuals who consider a wider expertise in cybersecurity will most likely need numerous professional certifications which cover a variety of niche, technical, or general topics as well as hands-on capabilities depending on their interest. There are many organizations which offer cybersecurity governance, risk management, compliance, and technical certifications including Identity Management Institute (IMI) which offers 8 certifications in the areas of identity theft risk management and compliance, system security and data protection, identity governance, and access management.

As you discovered in the above section describing why identity and access management maters most in cybersecurity, IAM is the most complex and critical function of information security which aims to let the legitimate parties access systems while keeping illegitimate parties out. As cybersecurity professionals protect computer networks from external threats such as malware, they also manage the identities of various entities and their access to systems in the entire Identity Life Cycle. In a connected world of "Internet of Things", device identity management will be critical and the definition of identity theft will expand to include device identity theft by another device.

Identity Management Institute offers eight (8) identity and access management training and certification programs to global novice and experienced cybersecurity professionals. For example, IMI manages the following registered certifications which are highly sought by global professionals. You can click the links to learn more.

Certified Identity and Access Manager (CIAM)

Certified Access Management Specialist (CAMS)

Certified in Data Protection (CDP)

Your can learn more about other IMI certifications and how they can meet your security training needs for advancing your cybersecurity career. Click here to learn about.

Final Thoughts

As more data is proliferated, portable and connected devices enter the consumer and commercial marketplace, and system users continue to fall victims to identity theft schemes causing the majority of cyber intrusions, security threats and vulnerabilities will continue to rise. Consequently, the

cybersecurity profession will be more visible and important in the coming years and the Chief Information Security Officer (CISO) in responsible companies will be an Executive team member with direct access to the Board.

Cybersecurity is a dynamic and valuable profession in which members can be as creative and ambitious as they want to be to maneuver their career paths. There are many growing and evolving opportunities in security threat identification, solution development and marketing, risk analysis, and gap remediation whether at general or technical levels of management and operations. It is up to individuals to discover and pursue their desired cybersecurity paths and create a lasting and satisfying career for themselves. Not everyone wants to be a hands-on technical expert or part of the executive management team.

The business community and governments have a moral and legal duty to protect their customer information as well as their business information which if compromised can potentially place consumers, national security, and other businesses at risk. All parties must within the realm of their operations, duties, and risks, help promote the profession and support interested candidates become experts in their chosen specialty area of cybersecurity.

Contribute

As you pursue your successful career path, don't forget to give back to the community. Share this guide with everyone who wants to become a cybersecurity expert. Even those who are not interested in cybersecurity can benefit from this guide by learning to improve themselves and switch their careers. You may adopt a kid and coach them, speak to high school and college graduates about their career options, and share the knowledge you gain from this guide with others.

Discover Your Career Beacon

You are reading this guide because you either know what you want or are exploring the cybersecurity career option to determine whether it is a viable option that matches your character, interests, and needs. If you are sure that you want to be a cyber security expert, you are off to a great start in your career. And if you are assessing the opportunities in cybersecurity to decide whether this is the right career for you, then even if you decide not to pursue cybersecurity as a career, then at least you get to know yourself a little better which can only help you regardless of which career you pursue. One thing you need to consider in your career management is that you don't need to pursue the same career all your life and many professionals change their careers multiple times as they get to know themselves better. Click here to read an article about career selection.

About Identity Management Institute

Identity Management Institute (IMI) is a leading international organization which provides thought leadership, training, and professional certifications to its global members in various areas of identity and

access management including governance, system security and data protection, technology, identity theft protection, and regulatory compliance. These training and certification programs collectively support members and validate their skills in the growing cybersecurity career field.

More information can be found on the IMI website.