(ISC)²

How You Can Become a Cybersecurity Hero

This is the right time to join the cybersecurity industry

The immediate future of emerging technologies looks exciting and promising. Rapid advances over the next five years may help humanity solve some of the biggest challenges like the climate crisis, our ability to cure illnesses, understanding the universe and our microcosmos, and business automation using robots. And you can be part of this endeavor by joining the cybersecurity industry.

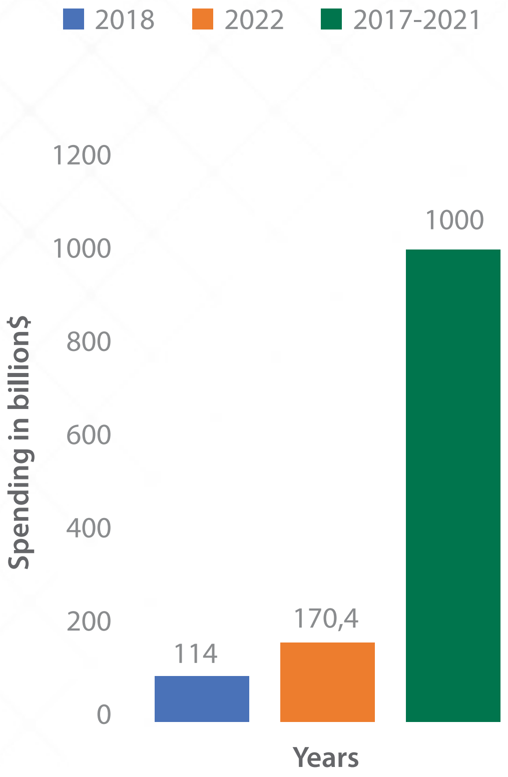
Despite the obvious benefits technology brings, it has also created many cybersecurity and privacy challenges. The overall business risk has increased because of the changing and expanding threat landscape. Cyber criminals are also leveraging these technologies to launch their malicious actions, which are more sophisticated than ever and harder to detect. The World Economic Forum, in their annual Global Risks report[1], have ranked cyber related risks as one of the top ten business risks, second only to environmental ones.

When corporations fail to mitigate and manage these risks, they evolve into security incidents which impact and disrupt businesses severely. The number of high-profile security incidents and breaches that make it to the news headlines highlight the importance of a robust security posture. Considering the degree of digitalization of almost every sector and industry, it is understandable why proficient, highly skilled security staff are required in every organization.

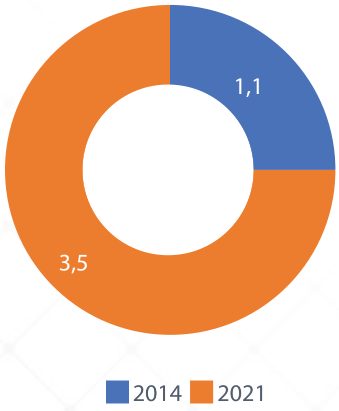
The job opportunities in the cybersecurity sector seem unlimited. Organizations from technology and manufacturing to retailers, airlines and shipping, to financial services and healthcare, government and federal sectors are all seeking skilled security staff. In fact, the US Bureau of Labor Statistics states that the growth in security related jobs will increase at a rate "much faster than normal" compared to all other occupations in the next few years[2]. "Demand for security professionals is expected to be very high, as these professionals will be needed to create innovative solutions to prevent hackers from stealing critical information or causing problems for computer networks," says the same report. Combined with the vast diversity of industry choices, joining the cybersecurity field promises a fast track career with incomes higher than the average salaries.

Cybersecurity is a booming industry. Worldwide spending on information security is on the rise each year, products and services exceeded $114 billion in 2018[3], while it is forecasted the market to grow to $170.4 billion in 2022[4].

In addition, it is predicted that global spending on cybersecurity products and services will exceed $1 trillion cumulatively over the five-year period from 2017 to 2021[5]. While all other technology sectors are driven by reducing inefficiencies and increasing productivity, cybersecurity spending is driven by cybercrime. The unprecedented cybercriminal activity is generating more and more spending on security.



Unfilled Cybersecurity Jobs Globally



Scale = Millions

Despite the promising statistics, the cybersecurity industry suffers from a lack of skilled personnel. In fact, it is predicted that there will be 3.5 million unfilled cybersecurity jobs globally by 2021, up from one million positions in 2014[6]. The workforce skills gap is nowhere more pronounced than in cybersecurity[7] and experts believe that the problem will worsen[8]. And of the candidates who are applying for these positions, fewer than one in four are qualified enough to fulfill the vacant positions[9].

Do you have what it takes to be a cybersecurity hero?

The executive board and the security managers rely on security practitioners to fortify their business against cyber-attacks. Security practitioners are the "soldiers" of every organization. Simply employing security practitioners is not enough. They also need to be armed with the right skillset and knowledge.

Going back to our army analogy, an army without soldiers is not an army. On the other hand, an army with unskilled soldiers will lose any battle they fight. Cybersecurity is a business battlespace. It is no wonder that the U.S. DoD and NATO have declared cyberspace as the fifth domain of warfare[10]. Every day businesses need to win battles – mitigate threats, prevent vulnerabilities from being exploited, identify malicious actors. And to win these battles they need skilled security practitioners.

You can become an everyday hero and have an impact on your organization if you have the required knowledge and skills, both hard and soft.

Hard skills

Knowledge of emerging technologies

Emerging technologies change the ways businesses work and will also create new roles in the future. The Internet of Things (IoT), Artificial Intelligence (AI), Machine Learning (ML), cloud computing and automation are all seen as important investments for many businesses as they take on digital transformation initiatives. New IT positions will demand professionals who understand these emerging technologies as well as their inherent security challenges.

Savvy IT professionals should acquire this knowledge today as many of these emerging technologies will force change in the workplace tomorrow. Without an understanding of how this technology is impacting IT infrastructure and business, some may find they are left behind as roles evolve to include skills related to emerging technology.

Thorough understanding of security

Cybersecurity has become a top priority in business today. Security professionals are in demand and a significant skills gap has made it difficult to find the help needed to mitigate risk.

In the absence of a dedicated security department, IT team members can make an impact by having a thorough understanding of cybersecurity skills, including security analysis, identity and access management, network security, penetration testing, and incident response.

Risk management is critical

With the IoT becoming ubiquitous, and consumers demanding products with an emphasis on cybersecurity and privacy, organizations are revamping their security policies. The Global State of Information Security survey findings indicate that 67% of organizations have security strategy focusing on risk management[11]. That means there is an abundance of opportunities for an IT professional with an interest in risk mitigation to take the security reins and demonstrate cyber security skills and leadership in this area.

To be able to advocate for risk-based policies and processes, the security professional is required to possess a thorough understanding of NIST's Risk Management Framework (RMF)[12]. Becoming knowledgeable on RMF the practitioner can help their organization to assess risk and establish the appropriate security documentation.

Soft skills

Leadership and communication

It is no longer acceptable for IT team members to work quietly and separated from the rest of the organization. Community, creativity and a clear investment in business priorities are skills critical to the success of IT workers. A certain level of business acumen and engagement is expected. Brushing up on "soft skills" gives individuals an edge as both a teammate and a leader in your IT department.

Knowledge of the value of flexibility

Businesses are placing value on IT professionals who can be flexible and are willing to take on hybrid roles, which ask for a mix of skills. In an effort to be leaner and more agile, organizations expect IT pros to be able to use technical tools, analyze data, collaborate across teams and manage projects from start to finish.

According to a recent analysis, hybrid roles pay 20-40 percent more and represent about 12 percent of all job openings today[13]. Silo-skilled roles are being phased out with a demand for IT workers who can embrace a number of different challenges.

Advocate for cyber security culture and best practices

Another important attribute of a cybersecurity hero is taking the lead in advocating for a security culture that is pervasive throughout the organization. In some organizations, employees believe security is someone else's job. Instead, we should be forging ahead with a message that security culture requires everyone to be

invested in the company's defense and protection. This starts with creating a strong awareness program for all users.

The practitioner should also be aware of the latest vulnerabilities and attacks plaguing business, and championing secure application development and the software development lifecycle (SDL). Security must be baked in from the outset of app creation, and development should be thinking about security at the start, not as an afterthought. The security professional who understands the secure SDL might be the person that prevents a headline-making incident from impacting their organization.

Whether an organization is just starting out with a security program or seeking to enhance their operations, a security practitioner brings many applicable skills to the business. Organizational security requires experience in many facets of the technology landscape including:

- Setting access controls
- Understanding and working with trust architectures
- Understanding the ethical boundaries
- Data leakage protection
- Risk identification
- Incident identification and response
- Network security practices

A systems security practitioner brings these practical skills to the organization along with higher level theoretical concepts, such as encryption architecture, cloud security, and application security. This combination of "hard" and "soft" skills is vital for the day-to-day functioning of a security department.

Why is it important to see the big picture?

The breadth of security knowledge and soft skills is a valuable asset for any professional wishing to join the cybersecurity sector. The necessity for expanded skillset is underpinned by the digital transformation initiatives which have changed how businesses work and interact with their employees, customers and partners.

Businesses are being digitalized seeking increased productivity with minimized total cost of ownership and enhanced collaboration between employees and with partners or suppliers. The idea behind digitalization is to use technology not just to replicate an existing service in a digital form but also to use technology to transform that service into something significantly better.

A security practitioner with a solid foundation will have the confidence required to see the big picture and understand the complex cybersecurity ecosystem of emerging technologies, such as the IoT, AI, ML, cloud computing, and containers.

5 technology growth areas affecting security

Internet of Things (IoT)

The proliferation of IoT is astonishing. Industrial IoT sensors have facilitated the real time monitoring of critical facilities such as the energy and water supply grids or weather forecasting systems. In the healthcare sector, medical IoT devices have enhanced the level of healthcare services delivered to patients while minimizing related costs.

Artificial Intelligence and Machine Learning

AI-driven autonomous, self-learning solutions are already used by organizations in the insurance industry, in breast cancer research, in finance and in law enforcement. In the cybersecurity sector, AI's speed, accuracy and computational power offer a unique chance to protect a perimeter-less organization and to continuously process the overwhelming volume of threat data every organization now faces.

Cloud computing and Containers

Cloud-based services offer a scalable and reliable IT infrastructure that is specifically designed to streamline business performance and support development and growth. As opposed to the limitations of traditional on-premises IT infrastructure, cloud environments offer advantages such as flexibility, business continuity, cost efficiency, and scalability. At the same time, containerization and container orchestration becomes more and more popular, since it packages up code and all its dependencies, so the application runs quickly and reliably from one computing environment to another.

Privacy concerns are increasing

Data is at the core of all digitalization efforts. The way this data, often personal and sensitive, is processed and stored is dictated by numerous privacy regulations, many of which, such as the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), have far reaching implications.

It is therefore important for any business to abide by these privacy regulations, since lack of compliance can result in massive penalties, let alone reputational damage. A security professional should have a thorough understanding of the technical and administrative measures specified in these regulations to be able to implement them in the most efficient manner, helping their company respect to their employees' and customers' digital rights.

The threat landscape is expanding

In tandem with the increased privacy concerns, digital transformation initiatives have expanded the business threat landscape because oftentimes security is an afterthought. In a hyper connected world, the question is not if a business gets breached but when they will face a security incident. In fact, the percentage chance of experiencing a data breach within two years has increased from 22.6% in 2014 to 29.6% in 2019[14].

Although these emerging technologies have opened up amazing new organizational capabilities, they have also created new complexities, interconnections and vulnerability points which cyber criminals have quickly learned to exploit. Traditional perimeter and rules-based approaches to cyber security no longer apply to the new digital organization, since users are now accessing the organization's most sensitive resources remotely and beyond the traditional perimeter security.

In a perimeter-less business environment, the breadth of knowledge and the skills of a security professional can help minimize the friction and the uncertainty around security and its impact on the overall business risk.

Weak or lack of proper security controls leave organizations vulnerable to the exploitation of known vulnerabilities. For example, expired digital certificates, use of outdated security and encryption protocols, lack of asset visibility, improper patch management, and use of weak passwords to protected cloud-based apps to name but a few of known causes of security incidents, lead to data breaches and huge penalties and financial loses which can jeopardize the very existence of a business.

However, the vast majority of security incidents, no matter their scale, could have been avoided if applicable security controls and security professionals were in place. Knowledgeable and skilled security professionals with the use of proper technology and processes can minimize the security risks of any organization and can ensure a robust security posture.

The importance of broad security knowledge

A skilled professional with broad security knowledge can become an organization's most valuable asset. Having a broader understanding of security incidents, the security practitioner can make accurate and timely impact assessments based on the changing threat and technology environment, assisting the executive board in allocating the resources required to implement proportionate mitigation measures, ensuring a cyber resilient organization. Implementing security controls aligned with the overall business goals, the security professional can help minimizing the security risks, benefiting the organization in many ways and helping establish trust with customers and partners.

On the tactical level, the security professional can ensure a robust, yet useable security program. Having in place security controls that do not consider the human element can lead to friction, frustration and minimized productivity, while the users will try to circumvent those measures in favor of their convenience, leaving the organization open to malicious actors, either external or internal. Ensuring that the security program has the right ingredients of controls and usability can help create a cybersecurity culture and a cyber resilient organization.

Considering all the technological advances, their application in all aspects of life and their inherent security and privacy challenges, the professional wishing to enter the cybersecurity sector is presented with endless options; they may choose to become generalists or specialists, work in a specific industry or be employed as consultants. The choice is yours.

How a security certification qualification can help practitioners

Many cybersecurity personnel transition from IT seeking to advance their career in a different, yet similar sector. Whether you are a university graduate developing your career and want to specialize in cybersecurity or kickstarting a second career (such as a retired veteran), being able to demonstrate your knowledge and skills can make you stand out from the competition.

Hiring managers want to see a token of proof of your practical experience. Therefore, having a security certification can be one of the most essential qualifications when applying for a vacant cybersecurity position. Earning such a certification comes with many benefits, such as:

- » **Career advancement**. Raising the credibility of your knowledge and expertise in improving corporate security can boost your career and create new opportunities.
- » **Versatile skills**. Acquire versatile, vendor-agnostic skills that can be applied to different technologies and methodologies to understand how security works together to create the defense in depth for your organization.
- » **Personal branding**. Differentiate yourself to your employers, and peers, gaining respect and recognition from a community of security professionals.
- » **Solid foundation**. Acquiring a breadth of knowledge can help you build a solid foundation to be better prepared to mitigate and respond to cyber-attacks.
- » **Self Confidence**. Develop skills to reach a deeper, better and broader understanding of cybersecurity challenges and solutions.
- » **Stronger skillset**. Expanded knowledge can arm you with a stronger skillset to fulfill your roles and responsibilities.

- **Make an impact**. Be able to speak competently about current security trends and risks in the market and how those security issues directly impact the business, partners or the customers.
- **Vision**. Develop interconnection and thorough understanding of all the existing and emerging security technologies with business goals leading in better productivity and outcomes.
- **Higher salaries**. Security practitioners with a certification qualification earn up to 35% higher salaries than non-certified practitioners.

Which areas of knowledge should a security practitioner's certification cover?

Searching for the correct security certification, the security professional will end up with a handful of choices. Therefore, they face a dilemma which to select. Besides selecting the one that addresses specific interests and practical experience, it is important to investigate the body of knowledge each certification offers. A security practitioner's certification should cover the following security domains.

Access Controls

By learning and exercising access controls the security professional can specify what users can do, which resources they can access and what operations they can perform on a system. Adaptive access controls are about authenticating, and authorizing business employees based on contextual information and predefined conditions.

Security Operations and Administration

One important security control is to have visibility into the business assets to be aware of what there is to protect. Acquiring knowledge about security operations such as asset management, change management, assessments, and awareness training, the security professional can identify information assets and document the processes required for the implementation of policies, standards and frameworks that ensure the confidentiality, integrity and availability of these assets.

Risk Identification, Monitoring and Analysis

Organizations face a wide range of security challenges today, including expanding risks to organizational assets and customer data. Therefore, understanding and managing these risks are integral components of a successful corporate security program. Identifying risks to information systems and developing and implementing controls to mitigate the identified risks are the cornerstones of an enterprise-wide risk management process.

Incident Response and Recovery

Planning for unexpected events is an act of prudence. Organizations must plan and be prepared to act during an incident or a breach. Learning how to develop incident response and business continuity plans the security practitioner can assist their organization to navigate safely through the troubled waters of a security incident back to normal operations. Proper contingency planning and incident response are vital for an organization's survival.

Cryptography

Cryptography is plugged into the overall framework of confidentiality, integrity and availability. Encryption is the foundation of keeping data secure and is the single measure mentioned in all regulations and jurisdictions. Being aware of encryption protocols, techniques and certificates, the security professional can make an impact and help their business be compliant with all regulations and standards while preserving the confidentiality, integrity and availability of corporate data.

Networks and Communications Security

All businesses rely heavily on both public and private networks to develop their business and communicate with their employees, partners or third-party suppliers. The security practitioner should be aware of the required measures to prevent unauthorized disclosure of information in transit or tampering and eavesdropping of the communication channels while considering the network structure, the data transmission methods and the transport protocols.

Systems and Application Security

In an ever-changing threat landscape, where cyber attackers are becoming more intelligent, leveraging encryption to hide their tracks and movements, artificial intelligence and adversarial machine learning, code-signed malware, and social engineering tactics, businesses need to adopt security best practices. The security practitioner needs to be able to identify and analyze malicious code, implement device security, configure cloud security and virtual environments.

Security Controls Implement the Security Policy

The above domains of knowledge cover the whole breadth of security operations. These security controls involve aspects of policy, oversight, supervision, manual processes, actions by individuals, or automated mechanisms implemented by information systems. Therefore, the security practitioner is presented with massive career opportunities in any of the areas covered by the security controls domains depending on their skills and interests.

Being knowledgeable about these security controls is important for one more reason. By implementing these controls, the security practitioner can help with the enforcement of the corporate security policy. They can have a significant impact and be a cybersecurity hero not only in the security silo, but enterprise-wide up to the executive board.

A corporate security policy is the cornerstone document of a company's risk management program. The security policy defines the who, what, and how regarding the security of the company's data, assets, and IT systems, and plays an important role in an organization's overall security posture. Security policies reflect the acceptable risk of the executive management and therefore serve to establish a security mindset within the organization.

Having a security policy is not enough. The policy must be enforceable and applicable to everyone, from the CEO down to the newest employee. The executive management must lead by example and comply with the security policies and the consequences of non-compliance with the policy. Otherwise, mistrust and apathy toward compliance can plague the organization. If the policy is not enforced, then employee behavior is not directed into productive and secure computing practices which results in greater risk to the organization.

While a security policy is at the strategic level and serves as the "letter of intent" of the executive management, the security controls are at the tactical level. The primary objective of security controls is to reduce security risks by enforcing the corporate security policy and data security best practices. The selection and specification of security controls is accomplished as part of an organization-wide security program for the management of risk to organizational operations and assets. The risk-based approaches to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, policies, regulations, standards, and guidelines.

Security controls help materialize the policy. Here's where the role of a security practitioner becomes vital. It is the security professional who will implement these controls contributing the knowledge and skills to the overall robust security posture of their organization.

Why the Systems Security Certified Practitioner (SSCP) is the right certification for you

SSCP. Systems Security Certified Practitioner

An (ISC)^2 Certification

The security practitioner profession is always changing, and even the brightest minds can benefit from having a guide on the journey to success.

The (ISC)^2 Systems Security Certified Practitioner (SSCP) certification covers everything you need to know about security controls, therefore is ideal for IT administrators, managers, directors and network security professionals responsible for the hands-on operational security of their organization's critical assets. Certification shows you have the advanced technical skills and knowledge to implement, monitor and administer IT infrastructure using security best practices, policies and procedures.

The SSCP Common Body of Knowledge (CBK) provides an in-depth awareness and expertise across all seven security domains discussed here, helping to build and showcase a solid cybersecurity foundation, strong and versatile skillset, which will become a valuable asset to anyone seeking a career advancement in the cybersecurity sector.

(ISC)^2 is the leader in security certifications and is acknowledged by companies worldwide. (ISC)^2 can help you discover the right path, create your plan and thrive throughout your career. To learn more about SSCP, check out certification details here, or download the Ultimate Guide to the SSCP and get started today.

About (ISC)^2

(ISC)^2 is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)^2 offers a portfolio of credentials that are part of a holistic, programmatic approach to security. Our membership, more than 150,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the public through our charitable foundation – The Center for Cyber Safety and Education^{TM}. For more information about (ISC)^2 visit our website, follow us on Twitter or connect with us on Facebook.

Resources

[1] World Economic Forum, The Global Risks Report 2020, available at https://www.weforum.org/reports/the-global-risks-report-2020

[2] U.S Bureau of Labor Statistics, Occupational Outlook Handbook, Information Security Analysts, available at https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-1

[3] Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019, available at https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

[4] Gartner Forecast Analysis: Information Security, Worldwide, 2Q18 Update, available at https://www.gartner.com/en/documents/3889055

[5] Cybersecurity Ventures, Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021, available at https://cybersecurityventures.com/cybersecurity-market-report/

[6] Cybersecurity Ventures, Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021, available at https://cybersecurityventures.com/jobs/

[7] World Economic Forum, This is what the future of cybersecurity will look like, available at https://www.weforum.org/agenda/2017/08/the-us-is-upping-its-game-against-cyber-attacks-but-the-security-industry-faces-a-huge-challenge

[8] Harvard Business Review, The Public-Private Partnership That's Working to Make New York City a Global Hub of Cybersecurity Talent, available at https://hbr.org/sponsored/2019/06/the-public-private-partnership-thats-working-to-make-new-york-city-a-global-hub-of-cybersecurity-talent

[9] MIT Technology Review, A cyber-skills shortage means students are being recruited to fight off hackers, available at https://www.technologyreview.com/s/612309/a-cyber-skills-shortage-means-students-are-being-recruited-to-fight-off-hackers/

[10] Gen. Larry D. Welch USAF (Ret.), Cyberspace – The Fifth Operational Domain, available at https://www.ida.org/research-and-publications/publications/all/2/20/2011-cyberspace-the-fifth-operational-domain

[11] PricewaterhouseCoopers (PwC), Global State of Information Security Survey (GSISS), available at https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html

[12] NIST, Risk Management Framework (RMF) Overview https://csrc.nist.gov/projects/risk-management/rmf-overview

[13] Burning Glass Technologies, The Hybrid Job Economy: How New Skills are Rewriting the DNA of the Job Market, available at https://www.burning-glass.com/research-project/hybrid-jobs/

[14] IBM, Cost of a Data Breach Report 2019, available at https://www.ibm.com/security/data-breach