(ISC)²

9 Traits You Need to Succeed as a Cybersecurity Leader

Cybersecurity is an important factor for business prosperity

More than 50% of the world's population is now online[1]. Approximately one million people join the internet[2] each day, while two-thirds of humanity own a mobile device[3]. What is known as the Fourth Industrial Revolution (4IR), is already bringing tremendous economic and societal benefits to the world.

Smart technologies have enormous potential to improve both human life and the health of the planet. However, many new challenges and risks have also surfaced. Cyberattacks have become a common hazard for individuals and businesses. Fifth generation (5G) networks, quantum computing and AI are creating not only opportunities but also new threats.

The need for strong cybersecurity is apparent: an organization falls victim to a ransomware attack every 14 seconds[4], while one successful attack could force businesses to a complete standstill for weeks, or even to shut entirely.

Organizations should not view cybersecurity as just another IT expense for protecting against imminent cybersecurity threats. The fact is that cybersecurity can also play a vital role in driving business growth[5].

Figure 1: Long-Term Risk Outlook. Top 10 risks by likelihood and impact over the next 10 years.[6]

Organizations with a robust cybersecurity strategy have a strong competitive advantage over those that do not. With cyberattacks and security breaches making the news headlines daily, consumers are becoming savvier about the security and privacy of digital services and products, whether they are offered by a large enterprise or a small business. According to recent research by Vodafone[7], 89% of executives are confident that improving their corporate cybersecurity would enhance customer loyalty and trust.

However, companies are still struggling to make cybersecurity an integrated and proactive part of their strategy, operations and culture. Even though cybersecurity professionals are responsible for securing businesses, when companies make big, strategic decisions cybersecurity is often an afterthought, resulting in increased security and business risk. That means companies are losing out on the added value the cybersecurity function can provide.

What businesses need right now are talented, experienced, and knowledgeable employees that understand both the potential and the risks associated with emerging technology. As technology becomes more fabricated into business processes, these experts can lead the challenge of making cybersecurity awareness and safety an enabler of business success.

The skills you need to be a great cybersecurity expert

The business need for talented people represents a great opportunity for cybersecurity professionals like you. But future security leaders need a broad set of skills that job experience alone does not arm you with. You will need to invest in training to acquire these skills to build a solid foundation, feel self-confident and make an impact in your organization. Learning can get you the technical and soft skills required to be a veritable leader.

Technical skill sets

Deep knowledge of emerging technologies

Emerging technologies change the ways businesses work and will also create new roles in the future. IoT, AI, Machine Learning (ML), cloud computing and automation are all seen as important investments to support digital transformation initiatives. New security positions will demand professionals who are knowledgeable about these emerging technologies as well as their inherent security challenges.

Savvy security professionals should acquire this knowledge today as 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.

Strong knowledge of security best practices

Cybersecurity has become a top priority in business today. Security professionals are in demand and the skills gap has made it difficult to find the help required to mitigate risk. A cybersecurity professional must be able to demonstrate sound knowledge of security best practices to include:

- Incident detection and response, to handle any imminent threat of an organization's violation of security policies or standard security practices.
- SIEM management, to take the real-time analysis produced from alerts and translate that into incident response plans.
- Analytics and threat intelligence, to aggregate network and application data to prevent attacks from occurring in the future.
- Identity and access management, to ensure that the security policy demonstrates an acceptable use for various roles and responsibilities within the organization.
- Data management, to handle, analyze, and securely store all types of data, whether on-premise or in the cloud.

Thorough understanding the regulatory environment
Regulations such as the GDPR, CCPA, HIPAA, SOX, PIPEDA dictate the requirements for preserving the security and privacy of sensitive and personal data. Lack of compliance to these regulations will entail huge penalties by the respective national supervisory authorities. Not only will these penalties damage the corporate budget, they will also harm the level of trust people place on the affected organization.

Being compliant is a continuous process and not a one-off exercise. Cybersecurity professionals need to be knowledgeable of the security requirements described in these regulations and exercise the proper security controls with due diligence. Compliance to these regulations provides a competitive advantage and is an added value for every organization.

Soft skills

Leadership and communication
Security experts demonstrate leadership through their credibility, responsiveness, and ethics. Further, communication skills can help a security expert earn trust from senior management, peers and subordinates. Security professionals should be able to provide to their leadership actionable insights, linked to business needs and the risk environment and help the executives make informed decisions.

Passion for learning
Security experts should continuously learn the latest trends, technologies and security challenges within the business environment. They have to be passionate about learning and professional growth to be successful. Security is one of the most fast-paced segments in IT and requires someone with an appetite for knowledge and expertise.

Determination
Cybersecurity professionals must be persistent with an ever-changing threat landscape. Persistence is key. A cybersecurity expert sees a solution through to completion and does not stop until the challenge is solved.

Collaboration
Cybersecurity is a shared responsibility across the organization. Therefore, security professionals must be collaborative and work at all levels to instill a culture that ensures that security policies are not only in place but adhered to. It is also critical to gain buy-in throughout the organization for your security initiatives.

Analytical and critical thinking
A skilled cybersecurity professional is analytical regarding how incidents occur, the attack surfaces prone to exploitation, and how to minimize cyber-attacks. An analytical and insightful security professional anticipates how threat actors will exploit the network and its applications. In a way, the cybersecurity expert should think like an attacker and identify the vulnerabilities ahead of time.

Project management
Finally, as a cybersecurity expert you need to put together comprehensive security solutions to prevent, detect, and respond to cyber-attacks. Rather than thinking of installing a solution as "one-and-done," you need to think more holistically, building a security strategy that aligns to all the resources of the organization.

The cyber challenges putting business success at risk

The threat landscape is changing and expanding

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.

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, which have far reaching implications, such as the GDPR and the CCPA. However, high profile data breaches making the news headlines and abuse of personal data by governmental actors have increased the sentiment of mistrust against the in-place policies and strategies for the processing and storage of sensitive data.

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 portion of organizations affected by a successful cyberattack in 2019 reached 80.7%, up from 78.0% in 2018[8], while the percentage chance of experiencing a data breach within two years has increased from 22.6% in 2014 to 29.6% in 2019[9].

Although these emerging technologies have created 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.

Personal data, credentials are the main target of attacks

Identity is now the new perimeter security. Organizations need to authenticate efficiently and effectively the users or the devices accessing corporate data, whether this data reside on-premise or in the cloud. Digital identities are valuable assets to all organizations, but they are also lucrative targets for cyber criminals. Criminals love to get the job done the easy way, which explains why they use and abuse stolen credentials. Attack types such as hacking and social breaches benefit from the theft of credentials, which makes it no longer necessary to use malware to maintain persistence. Hence, account takeover and credential abuse attacks make it to the top five concerns for cyberthreats for organizations[10].

At the same time, personal data is getting swiped more often than in previous years. Personal data was involved in 58% of breaches in 2019, nearly twice the 30% in 2018[11]. This includes email addresses, names, phone numbers, physical addresses, and other types of data that one might find hiding in an email or stored in a misconfigured database. Once they get hold of this precious data, criminals either sell it on the dark web, where their stock market value is very high, or use it to launch other attacks, such as phishing.

Phishing attacks are the first step for attackers to gain presence in corporate networks

Most security reports agree that phishing is the first initial infection vector seen in security breaches[12]. Phishing is the favorite course of action for social engineering attacks, arriving via email in 96% of the occasions. While credentials are by far the most common attribute compromised in phishing breaches, personal data are also sought after[13].

Phishing has always been and still is a fruitful method for attackers. That is why it is the highest cyberthreat concern for businesses[14]. This concern is fueled by the worrying fact that more and more attackers are employing a phishing tactic, known as CEO fraud, through business email compromise (BEC). These kinds of attacks are financially motivated and have proven to be very effective: affected companies could lose as much as $44,000 per compromise[15].

Cloud security is a major concern

Moving corporate data to the cloud is part of the digital transformation businesses undergo. As companies move to the cloud, so do the criminals. Cloud assets were involved in about 24% of breaches in 2019 and involved an email or web application server 73% of the time. Additionally, 77% of those cloud breaches also involved breached credentials[16]. This is not so much an indictment of cloud security as it is an illustration of the trend of cybercriminals finding the quickest and easiest route to their victims.

These statistics contribute to a sentiment of declined confidence about the security posture of cloud-based assets[17]. In fact, 86% of the 8.5 million compromised data records were the result of a misconfigured server, either a publicly facing cloud asset or unencrypted data in the cloud[18]. Organizations fail to understand the shared responsibility model of the cloud providers, where security of the data in the cloud is the absolute responsibility of the owner.

Industrial attacks are increasing

Attackers are not focusing only on businesses for financial purposes. They are also eager to wreak havoc by disrupting the availability and reliability of national critical infrastructure. Events in which threat actors targeted Industrial Control Systems (ICS) and similar Operational Technology (OT) assets increased over 2000% in 2019 compared to 2018[19]. Most of the observed attacks were centered around using a combination of known vulnerabilities within SCADA and ICS hardware components.

There were also many cases where the attackers took advantage of the convergence of IT and OT infrastructure. This overlap allows IT breaches to target OT devices controlling physical assets, which can greatly increase the cost to recover. The explosive use of IoT devices by industries has expanded the attack surface, with threat actors taking advantage of it. Compromised devices with network access can be used by attackers as a pivoting point in potential attempts to establish a foothold in the organization.

Mitigating today's cyberthreat risks takes more than investing in the right technologies. You must ensure those technologies are deployed optimally, configured correctly, and monitored adequately to give your organization a fighting chance to avoid being a front-page news story. An experienced and well-educated cybersecurity professional can put together all the pieces of the puzzle to help any organization build a robust security posture.

The 9 characteristics of a successful cybersecurity expert

The role of cybersecurity experts is to support the mission of their organization by ensuring that cyber risks are managed at an acceptable level. Since no enterprise is immune to cyber threats, organizations need to be prepared for when a breach happens. The end goal of every organization should be resilience, the ability to identify and minimize the impact of an incident to allow business continuity as effectively as possible.

According to the World Economic Forum report "Cybersecurity Guide for Leaders in a Digital World[20]", cybersecurity professionals should adhere to "fundamental" tenets "that an organization must implement in order to embed cybersecurity in the corporate DNA and as part of a comprehensive cybersecurity program in the exercise of due diligence for cyber resilience."

1. **Think like a business leader** to transform cybersecurity from a support function into a business-enabler to foster business reputation, revenue, brand equity, and customer relations. Part of the leadership is the promotion of partnerships, both internal and external, which ensure that business needs are always met while managing associated cyber risks in a most effective manner.
2. **Build and practice strong cyber hygiene**, because the effective and consistent implementation of strong cyber hygiene could have potentially mitigated the majority of the cyberattacks of the last decade.
3. **Protect access to mission critical assets** based on the principle of "least privilege" while building a strong identity and access management system.
4. **Protect email against phishing** Email is one of the most valuable and broadly used means of corporate communication while, according to Verizon's DBIR 2020 report[21], it is the most common cyber-attack vector.
5. **Apply a zero-trust approach to securing the supply chain** that does not assume that a company can be made safe and sound within the perimeter of its "secure" corporate network. A perimeter-less zero-trust approach places control around the data assets and increases the visibility into how they are used across a digital business ecosystem.
6. **Prevent, monitor, and respond to emerging cyber threats** by developing a robust risk-based approach that is tailored to the organization's business context. The security services implemented must be fit for purpose and tailored to the needs of the organization across the dimensions of people, processes, and technology.
7. **Develop and practice a comprehensive crisis management plan.** Crisis management is a critical component of any security program in today's world. Communicating a security incident in a timely manner is as important as transparency and simplicity to form a solid trusted relationship with customers.
8. **Build a robust and tailored disaster-recovery plan** to protect the organization from potential cyber-attacks and to instruct how to react in case of a data breach, while reducing the amount of time it takes to identify breaches and restore critical services.
9. **Advocate a culture of cybersecurity** which puts users in the first line of defense and recognizes the critical role all employees play in the organization's security. Keeping an organization secure is every employee's job.

How a CISSP can help you prepare for real time incidents

When applying for a cybersecurity professional position you need to be able to demonstrate that you are the leader they are looking for. Security certifications are a token of proof of your expertise and knowledge.

Among all certifications available in the market, the (ISC)² Certified Information Systems Security Professional (CISSP) certification is the one that can provide you with the knowledge required to perform these tasks effectively and link your knowledge back to the business needs. The CISSP can help you become the next cybersecurity leader.

The CISSP Common Body of Knowledge (CBK) provides a cross-disciplinary awareness across the broad spectrum of information security that covers the following eight domains.

Security and risk management
A sound knowledge of the foundational security concepts and principles of information security is required to perform the functions of security and risk management, including developing and enforcing policy, championing governance, and ensuring business continuity in the event of a cybersecurity incident.

Asset security
Having visibility and a solid understanding of what must be protected, what access should be restricted, the available control mechanisms and how these may be abused is the foundation of all security controls. The professional should be able to apply the principles of confidentiality, integrity, availability, and privacy against these information assets.

Security architecture and engineering
Security must be considered in the design, implementation, and continuous delivery of a system lifecycle. Designing and building a secure and resilient information systems architecture can minimize the threats that can be caused by malicious actors, human error, or system failures. It is paramount to understand secure design principles and be able to apply security models to a variety of distributed and disparate systems and to protect the facilities hosting those systems.

Communication and network security
As a security leader you should be able to understand the components of a secure network, secure design, and the models for secure network operation. In addition, you should be knowledgeable about layered defense, secure network technologies, and management techniques to prevent threats across a number of network topologies and converged networks.

Identity and access management
Identity and Access Management (IAM) is the mechanism to manage digital identities and the professional should understand the policies and processes for managing these identities as well as the technologies and protocols required to support identity management.

Security assessment and testing
The activities involved in security assessment and testing to continuously verify that security controls are performing optimally and efficiently to protect information assets. Vulnerability assessments and penetration tests are part of the activities a cybersecurity professional is involved in performing.

Security operations
Security operations should be run in any environment, centralized or distributed, to protect and control information processing assets and to execute the daily tasks required to keep security services operating reliably and efficiently. Security operations include the activities of monitoring security, performing incident response, implementing disaster recover strategies, and managing physical security and personnel safety.

Software development security
Applications and data are the foundation of an information system. Understanding the controls around software, its development lifecycle, and the vulnerabilities inherent in systems and applications is essential to the development and maintenance required to ensure dependable and secure software.

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 to minimize the security risks, benefiting the organization in many ways and helping establish trust with customers and partners.

What are the benefits of being CISSP certified?

Earning the CISSP proves you have what it takes to effectively design, implement, and manage a best-in-class cybersecurity program. If you ask CISSP certified cybersecurity professionals how they benefited from earning this certification, they will attest to the following:

- **Career opportunities and advancement.** Raising the credibility of your knowledge and expertise in improving corporate security can boost your career and create new opportunities.
- **Broad and fundamental knowledge of cybersecurity.** Acquire versatile, vendor-agnostic skills that can be applied to different technologies and methodologies to understand how security works together to create an in depth defense for your organization.
- **Credibility.** 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.
- **Recognition.** Differentiate yourself to your peers, gaining respect and recognition from a community of security professionals.
- **Broader understanding of the connection between business and cybersecurity.** Develop interconnection and thorough understanding of all the existing and emerging security technologies with business goals leading to better productivity and outcomes.
- **Build trust and confidence with your business partners.** 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.
- **Higher salaries.** Security professionals with a certification qualification earn up to 35% higher salaries than non-certified practitioners.
- **Becoming a member of a strong peer network.** Becoming an (ISC)² member, unlocks a broad array of exclusive resources, educational tools, and peer-to-peer networking opportunities.

How (ISC)² can help

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

The CISSP is recognized as a gold standard for cybersecurity professionals. The CISSP is ideal for experienced security practitioners, managers and executives interested in proving their knowledge across a wide array of security practices and principles, including those in the positions of Chief Information Security Officer (CISO), Chief Information Officer (CIO), Director of Security, Security Systems Engineer, Security Analyst, Security Manager, and Security Consultant.

The CISSP Common Body of Knowledge (CBK) provides an in-depth awareness and expertise across all eight 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, go to https://www.isc2.org/Certifications/CISSP

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™. For more information about (ISC)² visit our website, follow us on Twitter or connect with us on Facebook.

© 2020, (ISC)² Inc., (ISC)², CAP, CCFP, CCSP, CISSP, CSSLP, HCISPP, SSCP and CBK are registered marks of (ISC)², Inc.

References

[1] International Telecommunication Union (ITU), "Measuring Digital Development, Facts and figures 2019", available at https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf

[2] Datareportal, "Digital 2019: Global Digital Overview", available at https://datareportal.com/reports/digital-2019-global-digital-overview

[3] Bank My Cell, "How Many Smartphones Are In The World?", available at https://www.bankmycell.com/blog/how-many-phones-are-in-the-world

[4] PR Newswire, "Ransomware Attack Every 14 Seconds", available at https://www.prnewswire.com/news-releases/ransomware-attack-every-14-seconds---prilock-announces-3-99-for-1-click-protection-300986165.html

[5] Netwrix, "How Can Cybersecurity Help in Business Growth?", available at https://blog.netwrix.com/2019/10/22/how-can-cybersecurity-help-in-business-growth/

[6] World Economic Forum Global Risks 2020 Report, page 17. This is republished in accordance with the Creative Commons Attribution-NonCommercial-NonDerivatives 4.0 International Public License, in accordance with these Terms of Use.

[7] Vodafone, "Cyber Security: The Innovation Accelerator", available at https://www.vodafone.com/business/white-paper/cyber-security-research-the-innovation-accelerator

[8] CyberEdge 2020 Cyberthreat Defense Report, available at https://cyber-edge.com/cdr/

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

[10] CyberEdge 2020 Cyberthreat Defense Report, available at https://cyber-edge.com/cdr/

[11] Verizon Data Breach Investigations Report (DBIR) 2020, available at https://enterprise.verizon.com/resources/reports/dbir/

[12] IBM X-Force Threat Intelligence Index 2020, available at https://www.ibm.com/security/data-breach/threat-intelligence

[13] Verizon Data Breach Investigations Report (DBIR) 2020

[14] CyberEdge 2020 Cyberthreat Defense Report

[15] Verizon Data Breach Investigations Report (DBIR) 2020

[16] Verizon Data Breach Investigations Report (DBIR) 2020

[17] CyberEdge 2020 Cyberthreat Defense Report

[18] IBM X-Force Threat Intelligence Index 2020

[19] IBM X-Force Threat Intelligence Index 2020

[20] World Economic Forum "The Cybersecurity Guide for Leaders in Today's Digital World", available at https://www.weforum.org/reports/the-cybersecurity-guide-for-leaders-in-today-s-digital-world

[21] Verizon Data Breach Investigations Report (DBIR) 2020