CISSP®

Certified Information Systems Security Professional

An (ISC)² Certification

DO YOU have what it takes to LEAD in Cybersecurity?

INSIDE

Cybersecurity Drives Business Growth	3
What's Keeping Leaders Up at Night?	4
Cybersecurity Needs More Skilled Professionals	6
Technical Skills for Leadership	6
Soft Skills for Leadership	7
What Cybersecurity Leaders Have in Common	8
How CISSP Positions You as a Leader	10
Benefits of CISSP Certification	13
Flexible Training for CISSP	14
Next Step: Get The Ultimate Guide to the CISSP	15
About (ISC)^2	16

Cybersecurity Drives Business Growth

The number of cyberattacks businesses suffer each year is overwhelming. In 2021, 85.3% of organizations experienced a successful cyberattack, while those experiencing six or more attacks rose to a new high of 40.7%.[1] Now more than ever, cyberattacks have become a common hazard for both individuals and organizations.

Cybersecurity is so much more than another IT expense for protection against imminent cybersecurity threats — it plays a vital role in driving business growth.

Organizations with a robust cybersecurity strategy have a strong competitive advantage. With cyberattacks and security breaches making headlines daily, consumers are becoming savvier about the security and privacy of digital services and products, whether they're provided by large enterprises or small businesses.

What organizations of all sizes need right now are talented, experienced and knowledgeable cybersecurity teams who understand both the advantages and the risks associated with emerging technologies.

[1] 2022 Cyberthreat Defense Report

85%

of organizations experienced a successful cyberattack

What's Keeping Leaders Up at Night?

As organizations continue to pursue digital transformation initiatives, the threat landscape is always expanding. In today's hyperconnected world, the question isn't whether a business' data will be breached but when. In fact, more than three-quarters of cybersecurity professionals say a successful attack at their organization is somewhat or very likely in the coming 12 months.[2]

Although emerging technologies have created amazing new organizational capabilities, they've also created new complexities, interconnections and vulnerability points that bad actors have quickly learned to exploit.

[2] 2022 Cyberthreat Defense Report

Identity Theft

Identity is the new perimeter security. Organizations need to authenticate the users or devices accessing their data. Attack types such as hacking and social breaches benefit from credential theft.

Phising Attacks

Most security reports agree that phishing is the initial infection vector seen in security breaches. The 2021 Data Breach Investigations Report from Verizon finds phishing increased by 11% the previous year and was present in 36% of breaches.

Cloud Security

Moving data to the cloud is part of the digital transformation businesses are undergoing. As companies move to the cloud, so do the bad actors.

Cybersecurity Needs More Skilled Professionals

It's important to understand what's happening now in the field of cybersecurity. Research shows **the global cybersecurity workforce needs an influx of approximately 2.7 million cybersecurity professionals to effectively defend organizations' critical assets.**[3] And the need shows no signs of slowing. The Bureau of Labor Statistics projects **the information security industry will grow by 33% through 2030 — that's 25% higher than the 7.7% growth rate across all industries.**[4]

The need for talent represents a great opportunity for cybersecurity professionals. But future leaders need a broad set of skills that job experience alone does not provide.

[3] 2022 Cyberthreat Defense Report
[4] Bureau of Labor Statistics, U.S. Department of Labor, Occupational Outlook Handbook

The following are some of the essential skills required of today's cybersecurity leaders.

Technical Skills for Leadership

Deep knowledge of emerging technologies

Emerging technologies change the ways organizations work and create new roles. IoT, AI, Machine Learning (ML), cloud computing and automation are all important investments to support digital transformation initiatives.

Strong knowledge of security best practices

Cybersecurity is a top priority for organizations. 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 it 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 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-premises or in the cloud

Thorough understanding of the regulatory environment

Regulations such as the GDPR, CCPA, HIPAA, SOX and PIPEDA dictate the requirements for preserving the security and privacy of sensitive and personal data. Lack of compliance results in substantial penalties by the respective national supervisory authorities. Not only do these penalties damage an organization's budget, they harm the level of trust from their clients and customers.

Soft Skills for Leadership

Leadership and communication

Cybersecurity experts demonstrate leadership through their credibility, responsiveness and ethics. Strong communication skills can help them earn trust from senior management, their peers and junior staff.

Passion for learning

Cybersecurity experts should continuously learn the latest trends, technologies and security challenges facing organizations. They must be passionate about learning and professional growth to be successful.

Determination

Cybersecurity professionals must be persistent in the ever-changing threat landscape. They must see a solution through to completion and never stop until the challenge is solved.

Collaboration

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

Analytical and critical thinking

Skilled cybersecurity professionals are 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 hackers will exploit the network and its applications.

What Cybersecurity Leaders Have in Common

The role of cybersecurity experts is to support the mission of their organization by ensuring that risks are managed. Since no enterprise is immune to cyberthreats, organizations need to be prepared for when a breach happens. The end goal is resilience and identifying and minimizing the impact of an incident to allow business continuity as effectively as possible.

Cybersecurity leaders who excel in attaining these goals share the following traits:

They think like a business leader to transform cybersecurity from a support function to a business-enabler to promote reputation, revenue, brand equity and customer relations. Part of the leadership is the promotion of partnerships, both internal and external, to ensure business needs are always met while managing associated risks in a most effective manner.

They build and practice strong cyber hygiene because it mitigates the majority of the cyberattacks.

They protect access to critical assets based on the principle of least privilege while building a strong identity and access management system.

They protect email against phishing since email is one of the most broadly used means of organizational communication.

They apply a Zero Trust approach to securing the supply chain that places control around the data assets and increases the visibility into how they're used across a digital ecosystem.

They prevent, monitor and respond to emerging cyberthreats by developing a robust risk-based approach tailored to the organization's business context.

They develop and practice a comprehensive crisis management plan, a critical component of any security program in today's world.

They build a robust and tailored disaster-recovery plan to protect the organization from potential cyberattacks. They instruct on how to react in the case of a data breach while reducing the amount of time it takes to identify breaches and restore critical services.

They advocate a culture of cybersecurity that puts users in the first line of defense and recognizes the critical role all employees play in the organization's security.

How CISSP Positions You as a Leader

Among all certifications available in the market, the (ISC)² Certified Information Systems Security Professional (CISSP) is the one that provides the knowledge required to perform tasks effectively and link your knowledge back to the organization's needs.

A skilled professional with the vendor-neutral credential is an organization's most valuable security asset. Having a broader understanding of security incidents, the practitioner can make accurate and timely impact assessments based on the changing threat and technology environment. By implementing security controls aligned with the organization's goals, the cybersecurity leader can help minimize security risks, benefiting the organization in many ways and helping to establish trust with its customers and partners.

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.

1. 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.

2. Asset Security

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.

3. 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 threats from bad 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.

4. Communication and Network Security

As a cybersecurity 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.

5. Identity and Access Management

Cybersecurity leaders should understand the components of a secure network, secure design and the models for secure network operation. In addition, they should be knowledgeable about layered defense, secure network technologies and management techniques to prevent threats across a number of network topologies and converged networks.

6. Security Assessment and Testing

Cybersecurity leaders should know the activities involved in security assessment and testing to continuously verify that security controls are performing optimally and efficiently to protect information assets.

7. Security Operations

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

8. 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.

Benefits of CISSP Certification

CISSP proves you have what it takes to effectively design, implement and manage a best-in-class cybersecurity program.

The benefits are many including:

- **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.** Acquiring versatile, vendor-agnostic skills that can be applied to different technologies and methodologies shows you understand how security works together to create an in-depth defense.
- **Credibility.** Acquiring a breadth of knowledge can help you build a solid foundation to be better prepared to mitigate and respond to cyberattacks.
- **Self-confidence.** You'll develop skills to reach a broader and deeper understanding of cybersecurity challenges and solutions.
- **Recognition.** You'll differentiate yourself from your peers, gaining respect and recognition from a community of security professionals.
- **Broader understanding of the connection between business and cybersecurity.** You'll develop a thorough understanding of existing and emerging security technologies.
- **Trust and confidence from your business partners.** You'll be able to speak competently about current security trends and risks and how they directly impact the organization, partners and customers.
- **Higher salaries.** (ISC)²-certified professionals report 35% higher salaries than non-certified practitioners.
- **Membership in a strong peer network.** You'll become an (ISC)² member, unlocking exclusive resources, educational tools and peer-to-peer networking opportunities.

CISSP®

Certified Information Systems Security Professional

An (ISC)² Certification

Flexible Training for CISSP

As the world's largest nonprofit association of certified cybersecurity professionals, we offer Official (ISC)² Training for CISSP. We also work with leading training partners around the world.

When you choose Official (ISC)² Training, you benefit from:

- **Top-notch instruction** from authorized instructors who are (ISC)²-certified, average 15–20 years of industry experience and complete a rigorous process to teach the CBK®.
- **Comprehensive exam prep** covering all current exam topic areas with a focus on real-world learning activities and scenarios.
- **Most up-to-date content** for deep awareness and understanding of new threats, technologies, regulations and best practices.

Everyone has their own style of learning. That's why we offer three options to help guide you to CISSP certification. Find Training Today!

1. Self-Paced

Your self-guided tour toward certification

- Learn online at your own pace
- Download videos from an (ISC)² Authorized Instructor
- Access instructor support (48-hour email response time)

2. Online Instructor-Led

Your guided group tour toward certification

- Learn live virtually from an (ISC)² Authorized Instructor
- Collaborate with team members
- Prepare with the Official (ISC)² Student Training Guide

3. Classroom-Based

Your guided small group tour (10 or more students) toward certification

- Learn in-person at your office or a private venue near you
- Interact with an (ISC)² Authorized Instructor and students
- Coordinate training around your schedule

Next Step:

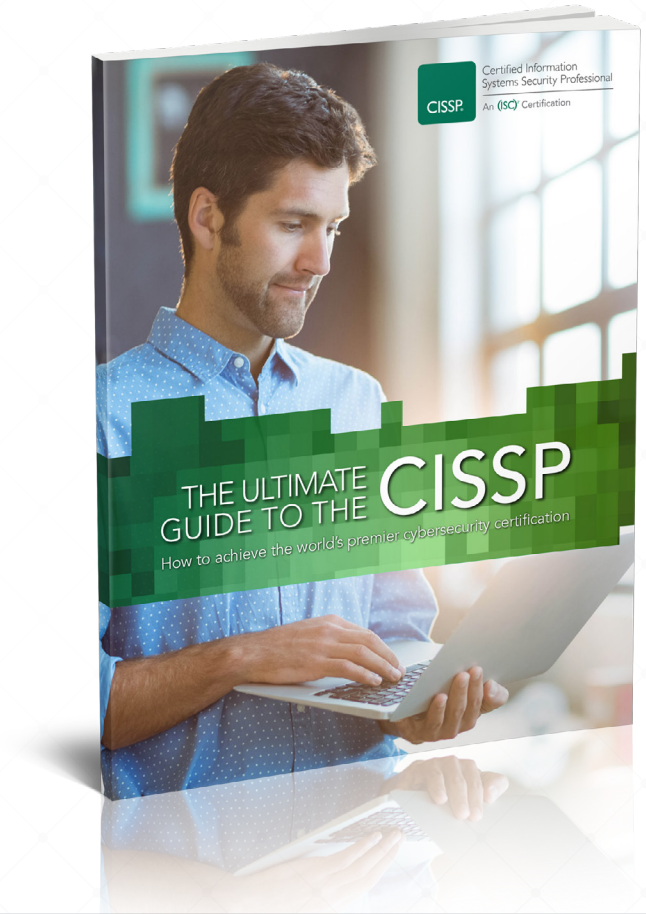
Get The Ultimate Guide to the CISSP

Take the next step toward cloud security certification with The Ultimate Guide to the CISSP. It covers everything to know about the world's leading cloud security credential. Find out how CISSP and (ISC)² can help you discover your certification path, create your plan and acquire the knowledge and skills to become a leader in cybersecurity.

It's All Inside!

- Is CISSP Right for Me?
- CISSPs Around the Globe
- Fast Facts about CISSP
- Benefits of CISSP Certification
- Benefits of (ISC)² Membership
- CISSP Exam Overview
- Official CISSP Training
- Pathway to CISSP Certification
- Free CPE Opportunities

Get Your Guide



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 168,000 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 general public through our charitable foundation – The Center for Cyber Safety and Education™.

Learn more at www.isc2.org or follow us on Twitter or connect with us on Facebook and LinkedIn.