JUNE, 2023

Top Five High-Paying Job Positions You Can Pursue with a Cybersecurity Maturity Model Certification

In today's increasingly interconnected environment, information is constantly exposed to various risks. Cyber threats, such as ransomware and phishing attacks, are becoming more sophisticated and prevalent, posing significant challenges for organizations to implement and update effective information security controls and processes.

To address these challenges, the Department of Defense (DoD) has developed and oversees the Cybersecurity Maturity Model Certification (CMMC). This cybersecurity framework serves as DoD's response to mitigate the risks associated with potential breaches of sensitive information within the Defense Industrial Base (DIB) systems and networks. It verifies and evaluates organizations' maturity in safeguarding sensitive information, including Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

CMMC consists of five levels, each representing a different level of cybersecurity maturity. Level 1 is the least mature level, while Level 5 is the most mature.

PECB's Cybersecurity Maturity Model Certification (CMMC) Training Courses, led by experienced trainers, are designed to assist you in expanding your professional knowledge and enhancing your skills in implementing and assessing CMMC requirements. PECB is approved as a Licensed Partner Publisher (LPP) by the Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) for the Cybersecurity Maturity Model Certification (CMMC).

With the guidance of PECB experts, you can streamline your certification process and successfully obtain one of our esteemed PECB certifications.

TOP FIVE U.S. HIGH-PAYING JOBS IN THE CYBERSECURITY INDUSTRY

1. Chief Information Security Officer (CISO)

The average U.S. annual salary of a CISO is **$237,025**.

The primary responsibilities of a Chief Information Security Officer (CISO) include:

- ✓ Implementing cybersecurity programs
- ✓ Reporting on cybersecurity matters
- ✓ Managing business continuity and disaster recovery efforts
- ✓ Collaborating with all organizational units to identify potential risks
- ✓ Preventing internal breaches or misuse of data
- ✓ Preparing regular feedback reports on cybersecurity

To fulfill these responsibilities, a CISO should possess the requisite competence, knowledge, and expertise in the field of information security. Additionally, a CISO should have practical experience in risk management and auditing. Hence, they should also possess planning and strategic management skills, along with supervisory skills, and a comprehensive understanding of complying with regulations and standards.

2. Cybersecurity Architect

The average U.S. annual salary for a Cybersecurity Architect is **$163,224**.

The main responsibilities of a Cybersecurity Architect include:

- ✓ Developing and implementing a comprehensive security strategy aligned with the organization's goals
- ✓ Developing incident response plans and procedures to effectively respond to and manage security incidents
- ✓ Developing security awareness programs
- ✓ Conducting training sessions for employees
- ✓ Conducting periodic security audits and assessments to evaluate the effectiveness of security controls
- ✓ Staying up to date with the latest cybersecurity trends

A Cybersecurity Architect plays a critical role in establishing a secure environment and ensuring the confidentiality, integrity, and availability of an organization's information assets. A Cybersecurity Architect should have compliance and regulatory knowledge. They should also have knowledge of the latest cybersecurity threats and attack vectors. Familiarity with security standards and frameworks would also help them in their daily work.

3. Cybersecurity Engineer

The average U.S. annual salary for a Cybersecurity Engineer is **$147,461**.

A Cybersecurity Engineer is mainly responsible for:

- ✓ Identifying potential vulnerabilities and threats to an organization's IT infrastructure and conducting risk assessments to evaluate the impact and likelihood of those risks
- ✓ Designing and implementing security controls and measures to protect the organization's digital assets
- ✓ Performing regular vulnerability assessments
- ✓ Monitoring the organization's systems and networks for suspicious activities, security breaches, and potential threats
- ✓ Investigating security incidents, analyzing the root cause of breaches, and conducting digital forensics to gather evidence and support legal proceedings if necessary

A Cybersecurity Engineer should possess a range of skills and qualifications to effectively carry out their responsibilities in protecting computer systems and networks. Some of the main skills of a Cybersecurity Engineer include technical expertise, threat intelligence, problem-solving skills, and so on.

4. Application Security Engineer

The average U.S. annual salary for an Application Security Engineer is **$140,000**.

An Application Security Engineer is mainly responsible for:

- Conducting threat modeling exercises to identify potential security threats and vulnerabilities
- Performing security testing, such as penetration testing and vulnerability assessments
- Providing guidance and training to development teams
- Maintaining documentation related to application security
- Ensuring that applications comply with relevant industry regulations and standards

Strong analytical and problem-solving abilities to assess complex security challenges, investigate security incidents, and develop effective solutions, are some of the main skills of an Application Security Engineer. Experience in conducting vulnerability assessments and prioritizing vulnerabilities based on risk would also be needed to perform a good job.

5. Cybersecurity Manager

The average U.S. annual salary for a Cybersecurity Manager is **$128,870**.

The main duties of a Cybersecurity Manager include:

- Establishing and maintaining a strong security governance framework
- Maintaining accurate records of security incidents
- Collaborating with partners and stakeholders to evaluate and select security solutions
- Overseeing day-to-day security operations
- Overseeing and managing a team of cybersecurity professionals
- Conducting risk assessments to identify potential threats and vulnerabilities

A Cybersecurity Manager has a very important role when it comes to the establishment and maintenance of a robust security posture and the mitigation of cybersecurity risks. A Cybersecurity Manager should have the ability to develop and execute a comprehensive cybersecurity strategy aligned with organizational objectives.

The PECB CMMC training courses are designed to provide individuals with the knowledge and skills for the implementation of an information security system that is based on a risk management approach.

Note: The salaries of the above-mentioned positions are not definitive and they may change with time and industry development.

CLICK TO SEE HOW PECB CAN HELP

→

+1-844-426-7322

customer@pecb.com

www.pecb.com

PECB