



Cyber Security Risk Analyst

Job Description

A cyber security risk analyst's main responsibility is to defend enterprises against online assaults and act quickly to restore security if it is breached. To do this, they must carry out a variety of activities, including evaluating and assessing potential weaknesses in an organization's digital infrastructure, documenting and reporting on any attempted cyber-attacks, and rapidly addressing security breaches or attacks by locating the attack's origin. According to the organization, cyber security analysts may provide advice, evaluation, or analysis services, but most of their job is preventative.

Identification, analysis, and mitigation of cyber hazards are the responsibilities of cyber security risk analysts. They collaborate with a range of stakeholders to find potential weaknesses and dangers in the networks and systems of a company.

Key Responsibilities

- Looking out for suspicious activity on the network, such as unauthorized user logins or attempts to access sensitive data.
- Investigating security breaches, identifying their root causes, and making recommendations for ways to stop them from reoccurring.
- Creating security policies and guidelines, such as those concerning employee behavior, system use, and data access.
- Utilizing penetration testing or vulnerability scanning technologies, checking security measures to make sure they are sufficient.
- Monitoring security precautions to make sure they remain effective over time.
- Creating security awareness training courses for staff on subjects like phishing attacks and social engineering techniques.
Recommending security policies and procedure upgrades based on newly discovered threats or weaknesses.

Qualifications Needed

- Bachelor's degree in computer science, information security, or a closely related discipline is required.

- Experience in risk management, information security, or a related sector.
- CISM or another pertinent certification, such as CISSP
- Knowledge of security standards like ISO 27001/27002, NIST 800-53.
- Solid familiarity with security concepts like non-repudiation, authentication, secrecy, integrity, and availability.
- Thorough understanding of security threats and weaknesses, such as malware, social engineering, and DDoS attacks.
- Knowledge of security technologies and techniques, such as firewalls, intrusion detection/prevention systems, and encryption.