CAREERS IN IT SECURITY

The necessity to protect digital assets and network devices will continue to grow as hackers keep developing new tools and strategies. Cybersecurity professionals are responsible for keeping information safe, secure, and accessible to the right people. They do this by creating the processes and tools designed to protect sensitive information. They are responsible for creating and writing the security protocols of an organization in addition to overseeing the day-to-day management of those protocols. The U.S. Bureau of Labor Statistics estimates that the need for Information Security Analysts will grow by 32% through 2028, much faster than the average growth rate for all occupations. By 2026, there should be nearly 130,000 new IT Security Analyst positions created. If you have an analytical mindset and like to get to the root cause of a problem, this highly in-demand career path could be a perfect match for you!

What's the Difference Between Information Security and Cybersecurity?

Information security and cybersecurity are often used interchangeably, but technically, information security refers to the protection of any information, whether it resides on a hard drive, in the cloud or in a filing cabinet. Cybersecurity strictly refers to the protection of electronic information. Within cybersecurity, there are several disciplines, including network security, internet security, endpoint security, cloud security, and application security. For the sake of simplicity, we will only use the term "cybersecurity" below.

INCIDENT RESPONDER

Protect & Defend

An incident responder is the first line of defense against threats and security incidents. They also identify the causes of the incidents, reduce any damages, exhaustively research the situation and recommend solutions to address any breaches in the current security protocols of the organization. An incident responder is a detective, figuring out what went wrong in a company's security protocol and ensuring that similar breaches do not happen again. They need to have excellent problem-solving skills and an analytical mindset.

Entry-level roles: Network Administrator, Systems Engineer, Systems Administrator

Next steps: Penetration & Vulnerability Tester, Disaster Recovery Specialist, Incident Response Engineer, Audit Project Manager, Security Consultant, Security Analyst, Computer Forensic Technician, Cybercrime Investigator

Skills required:
Information Security, Project Management, Information Systems, Linux, Network Security, Technical Support, Intrusion detection, UNIX, Security Operations

Certifications:

- Certified Information Systems Security Professional (CISSP)
- SANS/GIAC Certification
- GIAC Certified Incident Handler (GCIH)
- CompTIA Security+
- IT Infrastructure Library (ITIL) Certification

CYBERSECURITY SPECIALIST
Operate & Maintain

A cybersecurity specialist is an information security professional that performs many functions including designing, developing and implementing secure network solutions to defend against advanced cyberattacks, hacking and persistent threats. Cybersecurity specialists create and oversee the operation of security architecture and protocols to defend against hackers, malware and DDoS attacks. They also research and execute the most up-to-date security standards and best practices while performing vulnerability testing, security assessments and risk analysis.

Entry-level roles: Security Administrator, Systems Administrator, Network Administrator

Next steps: Security Engineer, Security Analyst, Penetration Tester, Security Consultant, Security Architect

Skills required:

Information Systems, Information Assurance, Network Security, Security Operations, Vulnerability Assessment, Project Management, Linux, NIST Cybersecurity Framework

Certifications:

- Certified Information Systems Security Professional (CISSP)
- SANS/GIAC Certification CompTIA Security+
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)

CYBERSECURITY ANALYST
Investigate & Analyze

The role of a cybersecurity analyst involves analyzing weaknesses in the IT infrastructure (hardware, software, networks) of an organization and reporting on any invasion attempts and false alarms with the goal of creating a more powerful security framework. Security analysts resolve or prevent cybersecurity-related breaches by uncovering vulnerabilities, examining evidence and overseeing a risk analysis of the organization's network infrastructure. In essence, they are continually testing and evaluating the security architecture and protocols that security engineers and specialists have created.

Entry-level roles: Networking, Systems Engineering, Financial & Risk Analysis, Security Intelligence, Security Technician

Next steps: Security Consultant, Security Administrator, Security Engineer, Security Architect

Skills required:

Computer Forensics, Linux, Information Security, Consumer Electronics, Hard Drives, Information Systems, Forensic Toolkit, UNIX, Malware Engineering

Certifications:

- SANS/GIAC Certification
- Certified Ethical Hacker (CEH)
- Certified Information Systems Security Professional (CISSP)
- EnCase Certified Examiner (EnCE)
- GIAC Certified Forensic Analyst
- GIAC Certified Incident Handler (GCIH)

IT AUDITOR
Oversee & Govern

An IT auditor's primary responsibility is to lead projects that improve internal performances and processes. They spend a substantial amount of time collecting and reviewing data from software programs, databases and information management systems. They then analyze that data, expand internal controls, and report issues connected with IT services and systems. As an auditor, your responsibility is not to fix problems detected during your audit but to evaluate and observe the security controls and protocols.

Entry-level roles: Networking, Systems Engineering, Financial & Risk Analysis

Next steps: Cybersecurity Consultant, Penetration & Vulnerability Tester

Skills required:

Internal Auditing, Audit Planning, Information Systems, Sarbanes-Oxley (SOX), Accounting, Risk Assessment, Information Security, COBIT, Business Process

Certifications:

- Certified Information Systems Auditor (CISA)
- Certified Information Systems Security Professional (CISSP)
- Information Systems Certification Certified Information Security Manager (CISM)
- IT Infrastructure Library (ITIL) Certification