CAREER BRIEF

Cyber Risk Management Analyst
Information Security Analyst

Information Security Analyst plan, implement, upgrade, or monitor security measures for the protection of computer networks and information. They assess system vulnerabilities for security risks and propose and implement risk management strategies and ensure appropriate security controls are in place that will safeguard digital files and vital electronic infrastructure. An information security analyst is responsible for predicting what cyberattack might come next and then taking intel and strengthening the organization's network to prevent attacks.

EDUCATION

The cyber risk management analyst role is a more advanced role that requires training and experience. Not typically considered an entry-level position, most information security analysts have a bachelor's degree or equivalent in a computer-related field. In addition to technical skills, they should have strong analytical and problem-solving skills and because they work to anticipate future cyberattacks, they must stay up to date on the latest technologies, trends, and tools.

WHERE THEY WORK

Digital transformation, the Internet of Things (IoT), cloud computing, and big data are exciting advances, but also create major challenges for organizations. As massive amounts of data are collected, shared, and stored every business becomes vulnerable to personally identifiable information (PII), intellectual property, or other sensitive data being exposed. Organizations of all sizes and in all sectors need to protect their assets. While future technology automation will help organizations protect their data and infrastructure, humans will still be needed, and information security analysts will be critical in predicting future cyberattacks.

FUN FACTOIDS

Connected IoT devices will reach 75 billion by 2025.

One of the most damaging attacks in history was the WannaCry ransomware attack, which first appeared in 2017. The virus infected more than 230,000 machines in 150 countries, causing damage of at least $4 billion.

Common cyber-related crimes include identity theft, fraud, and scams. In addition to identity theft, every year millions of people are victims of fraud, which often start with an email, text message, or phone message that appears to be from a legitimate, trusted organization. According to Symantec's Internet Security Threat report, a name or birthday can be worth up to $1.50 on the black market while a passport or driver's license number can be worth up to $45.00

National Consumer Protection Week is held each year the first full week in March to help people understand their consumer rights and avoid frauds and scams.

WHERE TO FIND OUT MORE

Bureau of Labor Statistics Occupational Outlook Handbook I Informational Security Analyst [www.bls.gov]. CompTIA Career Pathways I Cybersecurity Analyst [comptia.org]. INFOSEC Career roles I Info Risk Analyst [infosecinstitute.com]

Federal Trade Commission National Consumer Protection Week [ftc.gov]

National Initiative for Cybersecurity Education I Workforce Framework for Cybersecurity [www.nist.gov/nice]

WHAT'S THE SALARY?
$103,590 per year/$49.80 per hour
Bureau of Labor Statistics 2020 Median Pay

DOL RELATED OCCUPATIONS
Computer Systems Analyst, Computer Network Architect, Software Quality Assurance Analyst, Web and Logistics Analyst

COMMON JOB TITLES
ISSO, Cybersecurity Auditor, Cybersecurity Assessor, IT Security Analyst, Security Operations Analyst, Security Analyst, Risk Analyst, Security Controls Assessor

COMMON CERTIFICATIONS
(ISC)2 CAP, CompTIA Cloud+, ISACA CISA, ISACA CRISC, CompTIA CASP, CCIP, GIAC GCTI, ECSA, CompTIA CySA+, CISSP, CISM

NICE FRAMEWORK WORK ROLES
Cyber Risk Management and Information Security Analyst may have one or more work roles as described in the Workforce Framework for Cybersecurity. Some common work roles might include Security Controls Assessor and System Security Analyst