USA TODAY CLASSIFIEDS BLOG

HOW TO START A SUCCESSFUL CAREER IN CYBERSECURITY

BLOG:

Auctions
Automotive
Business
Business Spotlight
Careers
Education
Marketplace
Notices
Real Estate
Services
Sports and Recreation
Travel

Do you love computers and the constantly evolving world of modern technology? Then you're ready to start your journey towards becoming a cybersecurity expert.

The Bureau of Labor Statistics reports that cybersecurity jobs will grow by 28 percent between 2016 and 2026. Industry insiders estimate that there are one million unfilled cybersecurity jobs worldwide. This number should reach 1.5 million by 2019.

What Does a Cybersecurity Expert Do?

Cybersecurity experts work with organizations to keep computerized information systems secure. They determine which members of an organization have clearance to see confidential information. Cybersecurity professionals recognize web threats that can compromise confidential information.

Cybersecurity experts recommend new software or firewall installation to prevent data leaks. They can also create solutions to avoid data loss from computer networks.

Cybersecurity professionals are also important partners in data loss and data leakage prevention. Data leaks and data loss are the biggest security vulnerabilities that organizations have.

Data leaks occur when someone outside the company receives confidential data. These leaks occur when someone removes files from the company's premises. A data leak is also as easy as someone remembering or repeating something they saw in a confidential file.

Data loss occurs when stored data is gone or missing. It may or may not be recoverable. A data loss can either be an accident or intentional if someone deletes files on purpose.

Both data leaks and data loss are prime examples of compromised confidential information.

Who Hires Cybersecurity Experts?

Government agencies, healthcare organizations, and financial systems all rely on cybersecurity experts. These industries store confidential records like medical records and bank account information that are at risk for data loss or data leak breaks. Cybersecurity professionals use their training to help protect these sensitive records against theft.

What Are the Different Cybersecurity Roles/Positions?

Cybersecurity responsibilities get divided into different professional levels with specific skills and training. The following are examples of the different cybersecurity job titles and duties:

Chief Information Security Officer (CISO)

The CISO implements security processes to protect a company from threats. The CISO is the primary leader of an organization's computerized systems.

Lead Software Security Engineer

This position manages other security experts that analyze risk and identify vulnerabilities.

Security Architect

A security architect analyzes security threats and recommends solutions. They may develop security software and train staff on company security policies.

Information Security Crime Investigator/Forensics Expert

These investigators study patterns left by hackers to identify flaws in the system. They use reverse engineering to track and detect malware events.

Information Security Analyst

Information Security Analysts develop organizational plans and strategies for preventing cyberattacks. They ensure compliance with policies to protect the organization against such attacks.

Penetration Tester

Penetration testers are in charge of identifying an organizations network vulnerabilities. They do this by testing the network with various tools and software.

Incident Responder

The Incident Responder is the first responder to a breach incident. This professional makes sure that further damage does not escalate.

Education/Experience/Certification Requirements for Cybersecurity Pros

Cybersecurity professionals need a combination of current computer expertise and educational qualifications. The following is a summary of what those qualifications entail:

Education

Penetration Testers generally don't need a bachelor's degree to get their job. An Associate degree may meet the qualifications for this position. The other positions need a bachelor's degree in either computer science or a related discipline.

Chief Information Security Officers and Lead Software Security Engineers need a Master of Business Administration (MBA) degree. These programs provide an extra two years of studying business and computer-related courses.

Experience

Many employers hire cybersecurity professionals with direct work experience in the same field as the one they protect. For example, if employers need a database security candidate, they may hire a database administrator.

Don't underestimate undergraduate and graduate internships for showing experience on your resume. Internships will expose you to a professional environment and network with other professionals.

Cybersecurity professionals should know about system architectures and operating systems. They should also have coding experience and be familiar with coding languages such as C++, Java, Ruby, and Python. A comprehensive understanding of IT systems gives them the big picture to see where vulnerabilities lie.

Certification

There are many certification options that cybersecurity professionals can earn to prove their expertise. Certifications are also a great way to learn new skills. They can help you show that you're serious about staying current on emerging threats.

Some of these certifications include:

CISSP – The Certified Information Systems Security Professional. The Department of Defense requires this certification. CISSP certification is also required for higher level leadership positions at increased pay.

CISM – Certified Information Security Manager. This certification shows skills in risk management and compliance.

CISA – Certified Information Systems Auditor. This certification outlines skill in auditing and controlling information systems.

GIAC – Global Information Assurance Certification. This certification emphasizes hands-on technical capabilities such as intrusion detection and forensics.

CEH – Certified Ethical Hacker. CEH certification is for entry-level applicants and helps to land an entry-level position.

OSCP – Offensive Security Certified Professional. OSCP teaches penetration testing methodologies by attacking various live machines in a lab.

CompTIA – Computing Technology Industry Association. This certifies entry-level personal computer service professionals to install and maintain personal computers.

Conclusion

Demand for cybersecurity experts is on the rise. Cybersecurity professionals are our first line of defense against cybercrime. We need them to keep our internet as safe as it can be.

Still unsure if this career field is right for you? You can find more career advice on our career blog to help you choose the path that's right for you.