FUTURE IN CYBERSECURITY

Large companies and government organizations all need cybersecurity professionals to protect their systems, networks, and data. The financial, government, education, and retail sectors are some of the most prominent players because of their size. But nearly all organizations need some form of cybersecurity, and the need crosses all industries.

The following list highlights some industries with high demand for cybersecurity professionals. Computer technology, Finance and banking, Healthcare and pharmaceuticals, Education, Retail and e-commerce, Gaming, Transportation and logistics, Energy and utilities, Government and public sector, Manufacturing, Media and entertainment, Telecommunications, Hospitality and tourism, Insurance, Real estate, Nonprofit and social sector, Agriculture, Construction, Automotive, Aerospace and defense.

Cybersecurity job opportunities will grow 32% by 2032, much faster than the average growth rate for all occupations. Estimates indicate that 5.5 million cybersecurity professionals are working worldwide, and 4 million are still needed. US News & World Report compiled a list of America’s 100 best jobs based on earning potential, job satisfaction, and job openings. Information security engineers, or cybersecurity engineers, are ranked #7.

The high demand for cybersecurity means that jobs are plentiful in this field. Cybersecurity careers are some of the fastest-growing careers worldwide. According to LinkedIn, cybersecurity roles such as cybersecurity engineers, managers, analysts, and specialists are among the fastest-growing careers across many countries.

A cybersecurity analyst, or cyberanalyst, stays one step ahead of cybercriminals to protect computer systems and networks from cyberthreats. Tasks and responsibilities: The scope of this role can be broad; typically, a cyberanalyst’s primary responsibility is to protect an organization’s systems, networks, and data from threats. They monitor systems for unusual activities or potential security breaches. When they find these issues, cyberanalysts act to resolve them before serious harm occurs. They also create defensive strategies to keep the organization’s data safe. Position: Depending on an organization’s structure, a cybersecurity analyst can be an entry-level, mid-level, or advanced role.

A cybersecurity engineer safeguards computer systems and networks from threats. Tasks and responsibilities: A cybersecurity engineer’s primary responsibility is to design, build, and maintain security architectures to protect sensitive information from cyberthreats. They constantly monitor the infrastructure for unusual activities, investigate security breaches, and ensure that data remains safe from potential attacks. They also conduct routine testing and simulations to identify and mitigate vulnerabilities, ensuring that digital infrastructure remains secure against evolving cyberthreats. Position: A cybersecurity engineer is typically a mid-level or advanced role.

A network security architect is like the architect of a building but for an organization’s computer network. Tasks and responsibilities: A network security architect designs a secure computer network that can withstand various cyberthreats. This work involves developing and implementing network security measures and regularly updating them as new threats emerge. They also help to recover the network if a security breach occurs. Position: A network security architect is typically a mid-level or advanced role.

A security software developer designs and develops secure software to protect it from potential cyberthreats. Tasks and responsibilities: A security software developer integrates security measures into all stages of the software development lifecycle (SDLC). They’re also responsible for updating and patching existing software to reinforce its defenses as new threats emerge. Position: A security software developer is typically a mid-level or advanced role.

A penetration tester, or pen tester, is a type of offensive security researcher or ethical hacker. Tasks and responsibilities: As their title implies, a pen tester performs penetration testing: they simulate real hacking techniques to find vulnerabilities in an organization’s digital systems that attackers can exploit. They confirm that vulnerabilities identified in vulnerability scans are real weaknesses worth addressing. They also uncover any other vulnerabilities missed by vulnerability scans and other assessments. After pen testing is complete, they report their findings to the organization so that it can address discovered vulnerabilities before attackers target them. Position: Depending on an organization’s structure, a pen tester can be an entry-level, mid-level, or advanced role.

Like a security software developer, an application security engineer is concerned with software security. But while a security software developer develops the software directly, an application security engineer examines and maintains the systems and processes used to develop and run that software. Tasks and responsibilities: An application security engineer works closely with developers throughout the SDLC, implementing security measures at every stage to ensure that all software is secure before being deployed to production. They also review, scan, and test code directly to identify vulnerabilities. Position: An application security engineer is typically a mid-level role.

A malware analyst is someone specifically trained to deal with malware threats. Tasks and responsibilities: A malware analyst investigates suspicious files or programs that they think might be malware. They closely study potential malware to determine how it works and how to stop it. This kind of work requires a deep knowledge of computers and programming languages and an aptitude for problem solving. You’ll also need to keep informed on the latest malware threats and controls. Position: A malware analyst is typically a mid-level or advanced role.

A digital forensics investigator is like a digital detective! Tasks and responsibilities: A digital forensics investigator retrieves, examines, and analyzes digital evidence to investigate cybercrimes. Their work starts after the cybercrime is committed. They use forensic tools and a deep understanding of attack frameworks to examine digital data, recover lost or damaged files, and trace digital footprints back to the cybercriminal. Position: Depending on an organization’s structure, a digital forensics investigator can be an entry-level, mid-level, or advanced role.

Cybersecurity careers span many different industries and roles. You can find various cybersecurity jobs that revolve around preserving the confidentiality, integrity, and availability of systems, networks, and data. If this work interests you, you should start building the skills that you need. Cybersecurity professionals need many types of skills and knowledge. Let’s break them into three categories: Baseline, Workplace, Specialized.

If you want to work in cybersecurity, you must be adept at working with technology and security tools. Although you might not need to know multiple specialized security technologies, having experience in information technology (IT) support is helpful. You’ll also need baseline or technical skills and knowledge specific to and practical for cybersecurity. Specifically, you should have skills and knowledge in the following areas. The order in which these skills are listed does not indicate their importance or priority. To help you understand how someone might use each skill in their job, you’ll explore examples from a day in the life of Liv, a cybersecurity professional at an international company.

*Information security and assurance*: Liv starts her day by checking the company’s IT infrastructure. She does so by using her information security and assurance skills. Information security and assurance involves protecting and ensuring the confidentiality, integrity, and availability of data from unauthorized access, use, or modification. Liv ensures that all data remains confidential, intact, and available. If she detects suspicious activity, she uses her technical expertise to trace its source and implement measures to prevent future occurrences.

*Security assurance*: Liv performs security assurance throughout the day. Security assurance involves verifying that security controls effectively protect networks and devices from threats. Liv verifies that security controls such as firewalls, intrusion detection systems, antimalware software, and encryption protocols are up-to-date and functioning effectively to prevent potential attacks.

*Threat analysis*: During her day, Liv performs threat analysis. Threat analysis involves identifying, analyzing, and evaluating potential threats to systems or organizations. Liv identifies potential threats. And by evaluating them in terms of their likelihood and potential impact, Liv can prioritize a response and apply any necessary countermeasures effectively.

*Cryptography*: Liv uses her cryptography skills to encode sensitive data that her department must share with other departments. Cryptography involves securing information by converting it into a code that only authorized people or systems can decode. Liv transforms the confidential data into a ciphertext. Only parties with the decryption key can revert this ciphertext into the original, human-readable form.

*Authentication*: Liv reviews authentication logs to ensure that access to the company’s resources is limited to authorized users. Authentication involves verifying the identity of a person or system trying to access protected resources to ensure that they are who they say they are.

*Risk management and assessment*: In the afternoon, Liv uses her risk management and assessment skills in a security meeting. Risk management and assessment involves identifying, assessing, and limiting risks that organizations face. She presents the findings of her recent risk assessment and identifies potential risks and vulnerabilities in existing systems. She also outlines her plan to analyze these threats further to determine the likelihood and potential impact of the threat actors attacking.

*Network security*: Liv concludes her day by meeting with Mario, the network administrator. She serves as a network security consultant, advising Mario on maintaining and updating network security controls. Network security involves identifying and implementing controls to protect networks and network devices from unauthorized access or attacks.

Employers are searching for candidates with more than just baseline skills. Whether your cybersecurity role focuses on risk management, cryptography, or another area, your role will also require good workplace skills. Workplace skills are general, non-technical skills helpful for getting and succeeding in most jobs. Some employers refer to these skills as employability, soft, or professional skills. Cybersecurity professionals need an experienced mix of baseline and workplace skills. To thrive in cybersecurity, you’ll need the following workplace skills. The order in which these skills are listed does not indicate their importance or priority. To help you understand the importance of each skill in a cybersecurity job, you’ll explore examples from a scenario involving Arianna, a cybersecurity professional at a startup company.

*Critical thinking*: Arianna, a cybersecurity professional at a startup company, receives an alert from her network monitoring tool indicating a new, unknown security threat in the company’s network. Arianna analyzes the situation and identifies the nature of the threat and its potential impact. Critical thinking involves analyzing complex cybersecurity challenges, identifying potential threats, and making informed decisions about how to address them.

*Attention to detail*: Arianna spots a vital clue in a log file, which leads to her determining the threat’s origin. Using attention to detail, you should carefully observe and analyze security measures, processes, and data. A subtle clue in a log file or intelligence source might be the key to identifying the cause of a data breach.

*Problem solving*: Arianna determines an effective solution to neutralize the threat, ensuring that data and systems remain protected. The solution involves a technical fix and a change in process. Many known and unknown issues arise that can cause threats to an organization’s cybersecurity. To keep data and systems safe, you’ll need problem-solving skills to identify the source of each potential security issue and resolve it.

*Communication*: Arianne can’t resolve the issue alone; she needs to persuade others to accept her assessment of the problem and help her implement her solution. Arianna conveys complex technical information about the threat and her proposed solution to her coworkers. She creates a report about the threat and presents her findings and recommendations in a meeting. Communication with team members and other stakeholders is inevitable and sometimes even critical. You must also be able to convey information, ideas, and thoughts clearly and understandably to technical and non-technical audiences.

*Collaboration*: Arianna works with her team on the issue. She also collaborates and communicates with other members of the security and network teams and with consultants and external vendors. Together, they resolve the issue and take measures to prevent similar incidents in the future. Depending on your organization and role, you’ll collaborate with members of a cybersecurity team or IT department, and you’ll probably work with other stakeholders, too. You’ll need to share knowledge with everyone involved and collaborate effectively to improve the organization’s security.

*Creative thinking*: Arianna wants to ensure that the updated security measures will effectively prevent breaches such as the one that the organization just experienced. To do so, she creates a simulated cyberattack. She uses her creativity to anticipate all the ways that someone might attack the new defenses. You must use creative thinking to think like attackers do and address all potential vulnerabilities that they might exploit. And when a data breach occurs, you should be able to brainstorm solutions quickly to stop and contain it.

*Adaptability*: A few months after the breach, Arianna discovers that her company is shifting to additional cloud-based services. She immediately familiarizes herself with the technology, its vulnerabilities, and the best ways to secure data in the cloud-based environment. Technology evolves at an incredible rate. You must adapt to emerging technologies and new processes that impact cybersecurity and implement both effectively.

Baseline and workplace skills aren’t always enough to get a cybersecurity job. Some employers look for experience in specific frameworks, tools, programming languages, or operating systems. For example, the Linux operating system runs on most network devices, security applications, and cloud-based servers. You might need to know Linux to strengthen the security or collect the security data of these devices, applications, and servers. You might also need specialized knowledge and skills specific to the roles or industries you are most interested in. For example, if you are interested in working in healthcare, you might need a deeper knowledge of cybersecurity laws and regulations relating to healthcare, such as the Health Insurance Portability and Accountability Act (HIPAA) in the US.

As you grow in cybersecurity basics, you might consider exploring some of the following specialized skills: Malware analysis, Computer networking, Cloud computing and security, System security, including operating systems such as Linux and Windows, Programming languages such as Python, DevOps and DevSecOps, Cybersecurity governance and compliance, Incident response, Threat hunting, Penetration testing, Digital forensics.

If you’d like to pursue a career in cybersecurity, getting an industry-recognized certification can help accelerate your learning and career. Check out the following resources to familiarize yourself with certifications by some of the leading providers:

The Computing Technology Industry Association (CompTIA) is a well-respected IT trade organization. It offers a variety of IT certifications that employers take seriously, including certifications in cybersecurity. Employers often prefer or require cybersecurity job applicants to have one or more relevant CompTIA certifications. CompTIA offers the following cybersecurity certifications: CompTIA Security+, CompTIA Cybersecurity Analyst (CySA+), CompTIA PenTest+, CompTIA Advanced Security Practitioner (CASP+)

The International Information System Security Certificate Consortium (ISC2)(opens in a new tab) is a nonprofit organization focusing on cybersecurity. It offers professional training and certifications in cybersecurity. The following list highlights some of the organization’s most well-known cybersecurity certifications: Certified in Cybersecurity (CC), Certified Information Systems Security Professional (CISSP), Certified Cloud Security Professional (CCSP)

The International Council of E-Commerce Consultants (EC-Council) is another well-respected cybersecurity certification organization. The following list highlights the organization’s most well-known cybersecurity certifications: Certified Ethical Hacker (C|EH), Certified Penetration Testing Professional (C|PENT), Computer Hacking Forensic Investigator (C|HFI)

Professional organizations to consider:

The National Institute of Standards and Technology (NIST) has a program to implement practical cybersecurity and privacy through outreach and effective application of standards and best practices necessary for the US to adopt cybersecurity capabilities.

The National Cyber Security Centre (NCSC) is the UK’s leading authority on cybersecurity issues. The website contains a lot of advice, documents, and guidance for specific industries.

The Open Web Application Security Project (OWASP) is a worldwide nonprofit organization focused on improving software security. It provides an unbiased source of information on best practices and actively advocates for open standards.

The Information Systems Security Association (ISSA) is a nonprofit organization for the information security profession. It is committed to promoting a secure digital world. Most resources from ISSA are for members. You can review the benefits of becoming a member and discover the local chapter nearest to you. If a local chapter is nearby, explore its website.

Women in Cybersecurity (WiCyS) is a US-based nonprofit membership organization dedicated to bringing together women in cybersecurity from academia, research, and industry to share knowledge, experience, networking, and mentoring.

The Forum of Incident Response and Security Teams (FIRST) is a global forum and recognized global leader in incident response. FIRST provides up-to-date resources on best practices.

News and blogs to stay current: Security Intelligence is an IBM site that provides analysis and insights from across the cybersecurity industry. You will find articles, research, and podcasts reporting the latest news in cybersecurity. Cybercrime Magazine is a cybersecurity publication from Cybersecurity Ventures. Cybersecurity Ventures is the world’s leading researcher for the global cybereconomy and a trusted source for cybersecurity facts, figures, and statistics. Its magazine provides the latest cyber economic market data, insights, and ground-breaking predictions to a global audience of cybersecurity professionals. Wired Threat Level is a series of cybersecurity articles from Wired magazine. Krebs on Security is a collection of blogs about computer security and cybercrime authored by Brian Krebs, an American journalist and investigative reporter. Graham Cluley is a collection of blogs about the latest computer security news, opinions, and advice authored by Graham Cluley, a British speaker and independent analyst. The Recorded Future blog provides cyberthreat intelligence analysis, industry perspectives, Recorded Future company updates, and more.

There is a great need for people with cybersecurity skills to help organizations protect their systems, networks, and data. A job in cybersecurity can lead to many opportunities for career growth. Cybersecurity professionals help many organizations and businesses solve problems across nearly every industry, from finance and banking to schools and even government organizations.Some of the most in-demand cybersecurity roles include the following positions: Cybersecurity analyst, Cybersecurity engineer, Network security architect, Security software developer, Penetration tester, Application security engineer, Malware analyst, Digital forensics investigator. You should build baseline or technical skills as well as workplace skills such as communication, problem solving, critical thinking, collaboration, and adaptability. You might need specialized knowledge and skills specific to the roles or industries that you’re most interested in.