The number of cyberattacks has exploded in recent years and organizations all over the world are at risk. In 2016 alone, technology giants like Verizon, Dropbox and Oracle were attacked by hackers, which directly affected millions of their users. Even powerful government institutions like the U.S. Department of the Treasury and the Federal Bureau of Investigation were victims of security breaches. While the increasing rate of cyberattacks has been a challenge for organizations around the world, it has created incredible employment opportunities for cybersecurity experts with in-demand skills.

The growing field of cybersecurity is vastly different from most professions. While many high paying careers still require a four-year degree from an accredited college, cybersecurity experts develop their skills on-the-job and validate their expertise through certifications. This departure from traditional education has a few benefits that include accelerated learning and reduced costs. Although the path to becoming a cybersecurity expert is getting easier, millions of positions still go unfilled as organizations compete for qualified talent.
A report from Cisco puts the global figure at one million cybersecurity job openings. Per Michael Brown, CEO at Symantec, the world’s largest security software vendor, demand is expected to rise to 6 million globally by 2019, with a projected shortfall of 1.5 million.

Embarking on a career in cybersecurity is both exciting and lucrative. Even entry-level positions provide excellent opportunities to earn a living while gaining valuable work-related experience. In a January 2016 Forbes article, author Steve Morgan says,

“A knack for cat and mouse play may indicate that you have an aptitude for cybersecurity. It’s a field where the good guys—cybersecurity professionals—are pitted against the bad guys—cybercriminals a.k.a. hackers.”

He adds, “Assuming you’d want to be the good guy—a career can mean a six-figure salary, job security, and the potential for upward mobility.”

A passion for learning and time-management skills also are important traits to have considering most cybersecurity professionals are required to train while maintaining their most essential duties at work. If you’re considering a career in cybersecurity, use this career guide to plan your development.
Becoming a cybersecurity expert requires work-related experience. After all, nobody is going to hire someone to protect their organization's most valuable assets without a proven track record. For many aspiring cybersecurity practitioners, gaining experience involves taking administrator positions in networking, systems and database support. These positions provide associate-level experience that cybersecurity experts need. Although these careers aren’t as lucrative as careers in cybersecurity, they still offer excellent pay.

On-the-job training is an ideal way to gain experience, but not everyone is ready for the demands of an IT career. For those without any experience, entry-level training courses that provide employment in desktop support and networking are suggested. Certifications like CompTIA A+ and CompTIA Network+ teach desktop and networking fundamentals and provide entry-level employment opportunities. Even the highest paid cybersecurity experts in the field today had to start somewhere.

Work-related experience for careers in cybersecurity can be developed in the following positions:

- Desktop support
- Network administration
- Systems administration
- Database administration
Cybersecurity certifications validate practitioners’ skills when they work toward promotions or apply for new opportunities. These certifications are much more valuable than a diploma from a four-year college, because they confirm in-demand skills that are desperately needed in today’s hostile hacking environment. Certification vendors provide opportunities for aspiring cybersecurity practitioners to successfully complete high-stakes exams that cover specific skillsets.

Cybersecurity Career Guide

Preparing for certification exams can be accomplished in a few different ways. The most traditional method is boot-camp style training where students attend live, instructor-led classes for a duration three to five days. However, a fundamental understanding of the material is highly recommended before attending. Online training is much more flexible and allows students to absorb information at their own pace. This type of training is, by far, the most common and is ideal when balancing a work and training schedule.
There are a number of certifications an aspiring cybersecurity practitioner can achieve. Additionally, there are different vendors to choose from. The certifications students choose ultimately define their careers. Therefore, careful consideration should be given before embarking down a specific path. Aspiring cybersecurity practitioners should consider the following certification options:

**COMPTIA SECURITY+**

**Vendor:**
CompTIA is a vendor-neutral, certifying body that specializes in entry-level certifications.

**Description:**
CompTIA Security+ is a great certification for anyone beginning a cybersecurity career, as it covers the fundamentals of security. Topics include network security, cryptography and risk management. Although this certification is a popular option for those working in the private sector, it’s a requirement for many cybersecurity practitioners working in government.

**Certification requirements:**
While there are no prerequisites to take the exam, some IT experience is recommended. Simply pass the exam to earn this certification.
Vendor:
Cisco is the world leader in network technology and is recognized in countries throughout the world.

Description:
Cisco Security certifications range from the associate level (CCNA) to the expert level (CCIE.) This certification track includes topics like network security, troubleshooting and monitoring of network devices. Cisco Security certifications are ideal for aspiring cybersecurity practitioners who want to protect large enterprise networks.

Certification requirements:
The Cisco Certified Entry-Level Technician (CCENT) is the prerequisite for the associate-level, CCNA Security. The CCNA is the prerequisite for the Cisco Certified Network Professional Security (CCNP Security). The CCNP is the prerequisite for the expert-level, Cisco Certified Internetwork Expert Security (CCIE Security). Successful completion of the exams qualifies for certifications up to CCNP. However, the CCIE level requires the successful completions of both a lab and written exam.
Vendor:
The EC-Council is a certifying body, specializing in IT security.

Description:
The CEH certifies the ability to perform penetration tests on computer infrastructures. Organizations all over the world hire cybersecurity experts to find the vulnerabilities in their enterprise systems before the hackers do. This is an ideal certification for anyone interested in pursuing a career where hacking is rewarded.

Certification requirements:
Preparing for the CEH can be accomplished by either attending an Accredited Training Center or through self-study. Candidates opting for self-study must have two years of security work experience before taking the exam. Successful completion of the exam constitutes certification.
Vendor:
ISACA is a nonprofit association, dedicated to the advancement of industry-leading practices for information systems.

Description:
The Certified Information Systems Auditor (CISA) validates advanced skills required to audit large enterprise systems, assess vulnerabilities, report on compliance, and initiate controls. Much like the CEH, the CISA is an ideal certification for anyone interested in testing an organization’s weaknesses to cyberattacks.

Certification requirements:
While there are no prerequisites for taking the exam, the following must be completed for certification:

1. Successfully write the CISA examination
2. Submit the application for CISA certification
3. Adhere to the Code of Professional Ethics
4. Adhere to the Continuing Professional Education Program
5. Comply with the Information Systems Auditing Standards
Vendor:
ISACA is a nonprofit association, dedicated to the advancement of industry-leading practices for information systems.

Description:
The Certified Information Security Manager (CISM) certification validates international security practices utilized by leading cybersecurity professionals. Those who achieve this certification design and oversee the security for large enterprise systems. CISM is an ideal certification for IT professionals with a background in enterprise system management.

Certification requirements:
While there are no prerequisites for taking the exam, the following must be completed for certification:

1. Successfully complete the CISM examination
2. Submit the application for CISM certification
3. Adhere to the Code of Professional Ethics
4. Adhere to the Continuing Professional Education Program
5. Comply with the Information Systems Auditing Standards
Vendor:
(ISC)² is a vendor-neutral certifying body for many security certifications and remains dedicated to a safe and secure cyber world.

Description:
The Certified Information Systems Security Professional (CISSP) is highly regarded throughout the world and validates a high level of competence in securing large enterprise systems. Like the CISM, this is an ideal certification for IT professionals with a background in enterprise system management.

Certification requirements:
1. Complete five years of full-time work experience in two or more of the eight domains of the (ISC)² CISSP CBK®
2. Pass the exam
3. Complete the endorsement process
Cybersecurity careers are among the most lucrative in the IT industry and provide employment opportunities all over the world. While many of the job titles associated with this industry are explicit, some are a little vague. Ultimately, experience and certifications define the practitioner’s role and salary potential.

Robert Half recently published the 2017 Salary Guide for Technology Professionals and the numbers are impressive for those in cybersecurity.

Cybersecurity Job titles and salaries:

- **Data Security Analyst** - $118,250 - $169,000
- **Systems Security Administrator** - $110,500 - $157,500
- **Network Security Administrator** - $107,750 - $155,250
- **Network Security Engineer** - $115,500 - $162,500
- **Information Systems Security Manager** - $136,000 - $191,750

**Summing It Up**

Cybersecurity offers amazing opportunities for those willing to gain the experience and certify their expertise. If you're considering a career in cybersecurity, reach out to the friendly representatives at KnowledgeNet: The Live Learning Company. They're available to get you on the path to your next career.