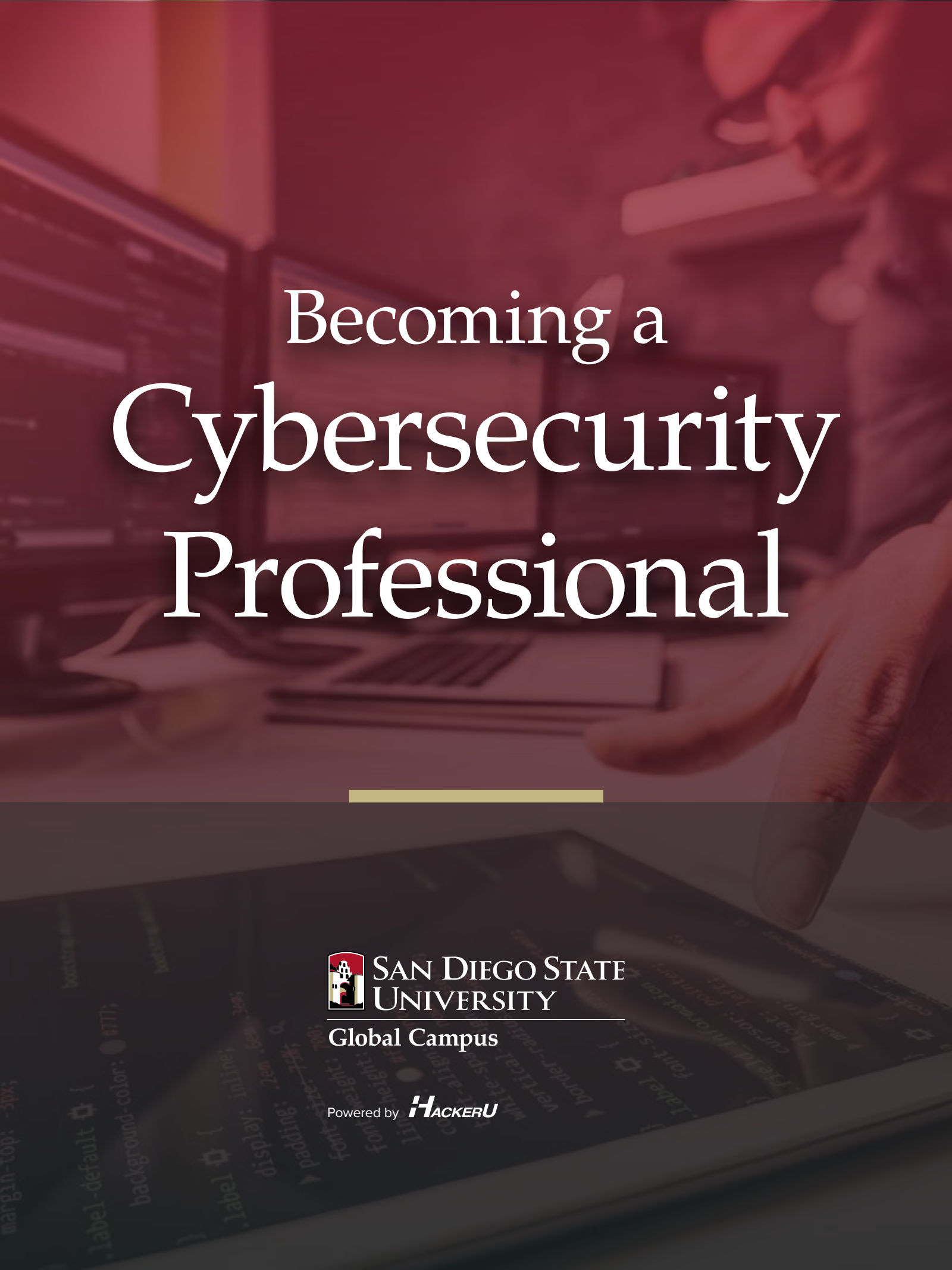


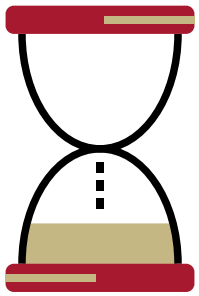
Becoming a Cybersecurity Professional

San Diego State University
Global Campus

Powered by HackerU

Becoming a Cybersecurity Professional

Powered by HACKERU



History of
Information Technology

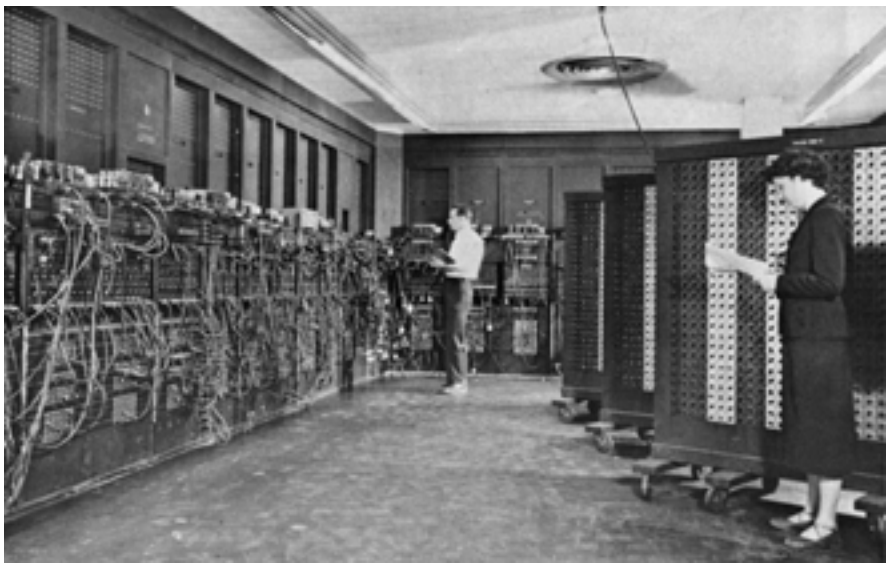
History of Information Technology

A major component of the IT landscape is cybersecurity.[1]

IT cybersecurity professionals make sure the systems used by organizations for storing, retrieving, and sending information are secure. While recent advancements moved information to a digital space, IT security professionals have been around for millennia, with people monitoring, gathering, transferring, and securing information as far back as ancient Mesopotamia[2].

It wasn't until the late 1950s that the term Information Technology or IT was officially coined in the Harvard Business Review by Harold J. Leavitt and Thomas L. Whisler. The term was meant to describe the new professions arising from the up-and-coming computing and networking systems that consisted of hundreds of miles of wiring, tape, and blinking lights.

Soon after these systems were set in place, it became clear that protecting the sensitive information being passed through was just as crucial as maintaining the systems themselves.



From K. Kempf, "Historical Monograph: Electronic Computers Within the Ordnance Corps" The ENIAC, in BRL building 328. Left: Glen Beck

1 https://it.toolbox.com/blogs/chrispentago/history-of-information-technology-070416

2 https://www.forbes.com/sites/gilpress/2013/04/08/a-very-short-history-of-information-technology-it/#33faf5b32440

3 https://www.experience.com/advice/careers/ideas/top-10-jobs-in-information-technology/

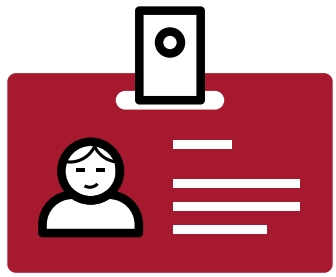
4 https://www.sandiegobusiness.org/sites/default/files/Cybersecurity%20in%20the%20San%20Diego%20Region%20-%20WEB.pdf

Today, IT cybersecurity professionals are tasked with developing, securing, and maintaining an organization's computer and networking systems[3]. Roles in cybersecurity can range anywhere from Cybersecurity Consultants, Cloud Security Architects, and Network Security Specialists, all the way to Computer Forensics Investigators, and Security Software Engineers, just to name a few.

With a growing number of companies depending on computers and networking systems, the need for capable cybersecurity professionals is growing. With San Diego's cyber employment expected to grow by 75% in the next 12 months[4], the possibilities for growth and contribution are endless.

"It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it."

Stéphane Nappo
Global Chief Information Security Officer
Société Générale International Banking



Cybersecurity and IT

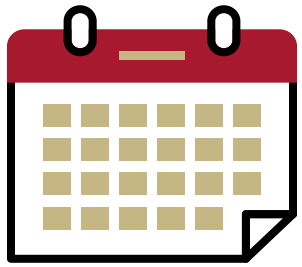
One of the Most Rewarding Fields to Work In

Cybersecurity and IT – One of the Most Rewarding Fields to Work In

Whether you're more into software or hardware, cybersecurity deals with the hands-on basics of computer security. The roles are so diverse, it can feel like there is a cybersecurity job for everyone. It's this love for computers and networking that plays a big part as to why cybersecurity and IT professionals are some of the happiest — and usually, the least stressed —workers in any organization.

Instead of being burdened with daunting corporate tasks, cybersecurity professionals often focus on maintaining and securing the hardware and software available on the network, which can make this field more rewarding for those wanting to make a positive impact. Cyber professionals in San Diego have a particularly unique opportunity with the Navy's Space and Naval Warfare Systems Command (SPAWAR) being the cornerstone of the regions' cybersecurity industry. 63% of cyber firms work directly or indirectly for the Federal government, including the Department of Defense, making San Diego a hot spot for cyber talent.

Hardware and software are always changing, meaning cyber threats are continually progressing and leaving cybersecurity professionals to face new challenges every day. It's this stimulating environment that keeps them on their toes, reduces boredom and repetitiveness, and contributes to a happy workspace.



A Day in the Life:
IT Security Manager

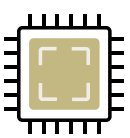
A Day in the Life: IT Security Manager

IT Security Managers are responsible for securing and maintaining companies' local and national network infrastructures.

They've been known to cover an array of tasks, including basic software setup, firewalling, coding, designing framework architectures, and managing employee network permissions and access.

At the end of the day, IT Security Managers are the go-to employees in any workplace, functioning as a digital beacon that serves as the first line of defense against external and internal cyber threats. For the crucial small business population of San Diego especially, it's necessary to have the resources to keep precious data secure.

IT Security Manager – Primary Responsibilities:



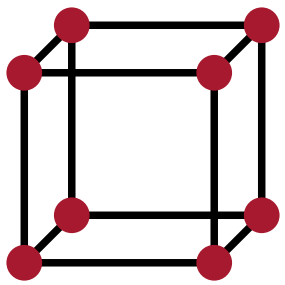
Setup & maintenance of all voice, video, and data connections

Regularly checking & analyzing backups, server hardware, and disaster recovery systems

Fixing and troubleshooting day-to-day issues

Maintaining company networks and securing them from external threats

In addition, IT Security Managers are also able to explore new ways to improve current systems and decrease costs. IT Security Managers can also contribute to their company's data management strategy, producing reports, interacting with SQL databases, and writing and rewriting queries.[5]



IT Fields of Expertise

IT Fields of Expertise

01

Network Security Administrator

Network Security Administrators make sure a company's computer networks, consisting of multiple computers or software platforms, are up to date on security protocols and running smoothly.

A Network Security Admin's job depends on the organization and how complex its networks are. In general, a Network Security Administrator is responsible for the following tasks, according to ONET, an online database containing hundreds of occupational definitions:

- Installing network and computer systems
- Maintaining, repairing, and upgrading network and computer systems
- Diagnosing and fixing problems or potential threats and backdoors within the network
- Monitoring networks and systems to improve performance

In short, Network Security Admins need to keep everything balanced. Since they manage both the back-end—networks, software, and hardware—and the front-end— maintaining and supporting the end-user experience, they're often working on several projects simultaneously, jumping between roles and teams.

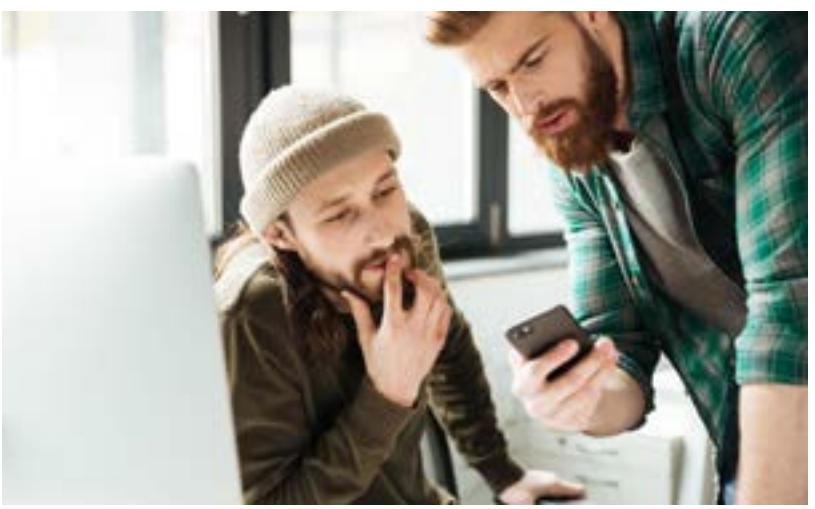
02

Network Security Manager

Network Security Managers can choose from two different paths: they can manage an organization's IT networking team in-house, or they could work for a third-party IT consultant firm that offers similar support.[5]

In general, a Network Security Manager is responsible for:

- Assessing the company's or client's computing requirements and vulnerabilities
- Developing and testing network upgrades to meet the company's or client's needs
- Putting in place Network Security measures
- Instilling preventative measures through scheduled maintenance
- Monitoring network performance and usage
- Supervising technical staff
- Planning backup and recovery systems
- Managing network development and growth



Network Security Managers work very closely with the entire IT department, as well as with prominent members of the managerial team to ensure all systems are secure and working efficiently.

[5] https://www.cwjobs.co.uk/careers-advice/profiles/network-manager

03

System Security Administration

Computer networks are critical parts of almost every organization, and someone needs to be responsible for maintaining the day-to-day operations of these networks.

To meet user needs, System Security Administrators may acquire, install, or upgrade computer components and software for:

- Routine automation
- Maintaining and upgrading security measures
- Troubleshooting
- Training new staff
- Supervising current staff
- Technical support for new and ongoing projects

System Security Administrators, or SysAdmins, are responsible for the upkeep, configuration, and continuing operation of computer systems, such as servers that house multi-user computers.[6] SysAdmins also help ensure uptime, performance, resources, and security of the organization's computers. As a result, they meet the needs of the users while adhering to a set budget.

In short, SysAdmins are the gatekeepers and protectors of a company's digital efforts. Whether it's something as simple as setting up a new employee user profile or helping support the company's next big project, a System Administrator will definitely be present.

---

6 https://en.wikipedia.org/wiki/System_administrator

04

Network Security Engineering

Network Architects, also referred to as Network Security Engineers, manage a company's local computer network and ensure a safe and productive digital work environment for all employees to use.

These data networks can include:

- Local Area Networks (LANs)
- Wide Area Networks (WANs)
- Intranets (Internal Network Connections)
- Extranets (External Network Connections)

Networks can vary in complexity from company to company. One company might only need one dedicated engineer to maintain and support its network, while a bigger company might need an entire team of globally connected engineers reporting to the company's Chief Technology Officer (CTO) or Chief Information Security Officer (CISO).

Network Security Engineers need to have a sixth sense for analyzing and predicting how communication flows and what types of communication should be used and proposed to management.[7]

Deficit of Workers

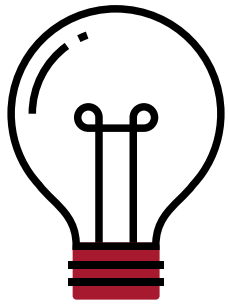
When looking at the job landscape, there is a deficit of skilled cybersecurity professionals, despite there being 58,000 technology specialists in San Diego. As companies continue to invest in newer and faster technologies and networks, their need for day-to-day operations creates an overwhelming necessity for the roles mentioned above. The demand for cybersecurity roles is projected to increase without signs of slowing down any time soon, and the starting salaries for these positions are some of the highest around, ranging from $97k to $109k, according to the San Diego Business.

There just aren't enough candidates out there for the positions, and there isn't a lot that organizations can do about it, besides increasing their scope by offering more money.[8]

---

7 https://www.snagajob.com/job-descriptions/network-engineer/

8 https://www.monster.com/career-advice/article/tech-talent-gap-survey-0816



How to Solve the Problem

How to Solve the Problem

What Workers Are Doing

There are two mainstream ways to break into Cybersecurity and Information Technology:

- A computer science degree
- Extensive training with certification

Relevant Cyber Security certifications include:

- CCNA - Cisco Certified Network Associate Certificate
- CompTIA Network+ Global Certificate
- CompTIA Security+ Global Certificate

So, a Computer Science Degree or Cybersecurity Certification?

The answer is really up to you. You can join the Defense or Aerospace Technology field, a particularly viable path in the San Diego cybersecurity community, or any number of the growing cyber fields. It all depends on where you are in your career and what your career goals are.[8]

More recently, to help ease the financial strain and cut down the time it takes to complete a standard four-year degree, more people are opting for training courses, bootcamps, and evening classes. These courses usually offer an extensive training regimen, hands-on simulations, and career services, to prepare you for a thoroughly certified cybersecurity career.

8 https://learningnetwork.cisco.com/blogs/certifications-and-labs-delivery/2017/01/06/certification-vs-degree-what-do-i-need-to-succeed

Training Programs Can Equip You for Real-World Scenarios

The most notable difference between a traditional degree and certification training is typically the educational material.

There is a massive gap between the topics focused upon in four-year degree programs versus career-focused training courses. In fact, four-year degrees mostly concentrate on computer science and theory. Training courses usually include a healthy mix of theory and, more importantly, the hands-on training valued most by employers. Training courses also bring on industry professionals as lecturers, citing real scenarios and case studies in order to simulate real-world working environments and procedures.

College can help teach you about IT and cybersecurity, but a training course provides experiential knowledge and hands-on experience that helps get you ready for a career in cybersecurity and IT.

Employers Look at Experience, Not Just Education

While there is a significant lack of competent candidates for cybersecurity positions, employers are sifting through mounds of candidates, and they can be very picky. Research found that **close to 50% of employers** are looking for a potent combination of skills, education, and experience.

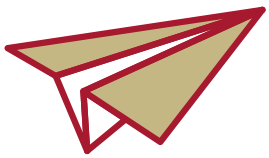
According to data collected by both IT companies and HR hiring experts, there's a definite advantage over the competition—especially in security—when you have the right certification.

Some employers might require a Computer Science degree, where some others might put more value on certifications and job experience for Network or Systems Administrator positions.

Additionally, Cisco and other types of certifications can help make your resume stand out to HR recruiters. In a lot of cases, certification can be a crucial qualifier for a position, as being recently certified can demonstrate current competency in the field.

Overall, when looking at the short-term, certification training delivers a higher return on investment. Certification training takes a substantially shorter period of time to complete (ranging from a few weeks up to a year), where a degree can last as long as 4 years or more.

More premier training facilities offer introductory courses that cover more high-level aspects of Information Technology and Cybersecurity before delving into the nitty-gritty of the course. This allows students to try out the program before committing.



To learn more about how to get qualified for a career in defensive or offensive cybersecurity, contact us to schedule a call with one of our Cyber Admissions Advisors.

SAN DIEGO STATE UNIVERSITY
Global Campus

Powered by HACKERU

(619) 839-3030

5250 Campanile Drive
San Diego, CA 92182-1920

digitalskills.sdsu.edu