



Security career

2016 Cybersecurity Skills Gap

Too Many Threats

\$1 BILLION:
PERSONALLY IDENTIFIABLE INFORMATION (PII) RECORDS STOLEN IN 2014¹

97% 
BELIEVE APTs REPRESENT CREDIBLE THREAT TO NATIONAL SECURITY AND ECONOMIC STABILITY²

MORE THAN 1 IN 4 
ORGANIZATIONS HAVE EXPERIENCED AN APT ATTACK³

\$150 MILLION:
AVERAGE COST OF A DATA BREACH BY 2020⁴

1 IN 2
BELIEVE THE IT DEPARTMENT IS UNAWARE OF ALL OF ORGANIZATION'S INTERNET OF THINGS (IOT) DEVICES⁵

74%
BELIEVE LIKELIHOOD OF ORGANIZATION BEING HACKED THROUGH IOT DEVICES IS HIGH OR MEDIUM⁶

Too Few Professionals

2 MILLION:
GLOBAL SHORTAGE OF CYBERSECURITY PROFESSIONALS BY 2019⁷

3X 
RATE OF CYBERSECURITY JOB GROWTH VS. IT JOBS OVERALL, 2010-14⁸

84%
ORGANIZATIONS BELIEVE HALF OR FEWER OF APPLICANTS FOR OPEN SECURITY JOBS ARE QUALIFIED⁹

53% 
OF ORGANIZATIONS EXPERIENCE DELAYS AS LONG AS 6 MONTHS TO FIND QUALIFIED SECURITY CANDIDATES¹⁰

77% OF WOMEN
SAID THAT NO HIGH SCHOOL TEACHER OR GUIDANCE COUNSELOR MENTIONED CYBERSECURITY AS CAREER. FOR MEN, IT IS 67%.¹¹

89%  OF U.S. CONSUMERS BELIEVE IT IS IMPORTANT FOR ORGANIZATIONS TO HAVE CYBERSECURITY-CERTIFIED EMPLOYEES.^{12**}

Cyberattacks are growing, but the talent pool of defenders is not keeping pace.

Although attacks are growing in frequency and sophistication, the availability of sufficiently skilled cybersecurity professionals is falling behind. Cybersecurity Nexus (CSX) is addressing this gap by creating a skilled global cybersecurity workforce. From the Cybersecurity Fundamentals Certificate for university students to CSXP, the first vendor-neutral, performance-based cybersecurity certification, CSX is attracting and enabling cybersecurity professionals at every stage of their careers.

SOURCES: 1. 2015 Cost of Data Breach Study: Global Analysis, IBM and Ponemon Institute, May 2015. 2. ISACA 2015 APT Study, October 2015. 3. ISACA 2015 APT Study, October 2015. 4. The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation, Juniper Research, May 2015. 5. SACA 2015 IT Risk/Reward Barometer-Member Study, September 2015. 6. ISACA 2015 IT Risk/Reward Barometer-Member Study. 7. UK House of Lords Digital Skills Committee. 8. Burning Glass Job Market Intelligence: Cybersecurity Jobs, 2015. 9. State of Cybersecurity: Implications for 2015, ISACA and RSA Conference, April 2015. 10. State of Cybersecurity: Implications for 2015. 11. Securing Our Future: Closing the Cyber Talent Gap, Raytheon and NCSA, October 2015. 12. 2015 ISACA Risk/Reward Barometer-Consumer Study, September 2015.

** "Employees" refers to data security professionals at organizations that potentially have access to survey respondent's personal information.



Want a sure-fire well-paid job? Train to fight computer hackers



BY TIM JOHNSON

tjohnson@mcclatchydc.com

WASHINGTON — Want a career with zero chances of going jobless?

Try the booming field of cybersecurity. Companies can't hire fast enough. In the United States, companies report 209,000 cybersecurity jobs that are in need of filling.

It'll only get worse. By 2019, according to the [Cybersecurity Jobs Report](#), the workforce shortfall may reach 1.5 million. Globally, the shortage could hit 6 million, it added.

“The internet is growing faster than the growth of people to protect it,” said Michael Kaiser, chief executive of the National Cyber Security Alliance.

It is a problem with the [full attention of the White House](#), which in July called for “immediate and broad-sweeping actions to address the growing workforce shortage and establish a pipeline of well-qualified cybersecurity talent.”

One Million Cybersecurity Job Openings In 2016



Steve Morgan, CONTRIBUTOR

I write about the business of cybersecurity. [FULL BIO](#) ✓

Opinions expressed by Forbes Contributors are their own.

If you are thinking about a career change in 2016, then you might want to have a look at the burgeoning cybersecurity market which is expected to grow from \$75 billion in 2015 to [\\$170 billion by 2020](#).

A knack for cat and mouse play may indicate that you have an aptitude for cybersecurity. It is a field where the good guys — cybersecurity professionals — are pitted against the bad guys — cybercriminals a.k.a. hackers. Assuming you'd want to be a good guy — a career can mean a six-figure salary, job security, and the potential for upward mobility.

More than [209,000 cybersecurity jobs](#) in the U.S. are unfilled, and postings are up 74% over the past five years, according to a 2015 analysis of numbers from the Bureau of Labor Statistics by Peninsula Press, a project of the Stanford University Journalism Program.

**What is a
security professional?**

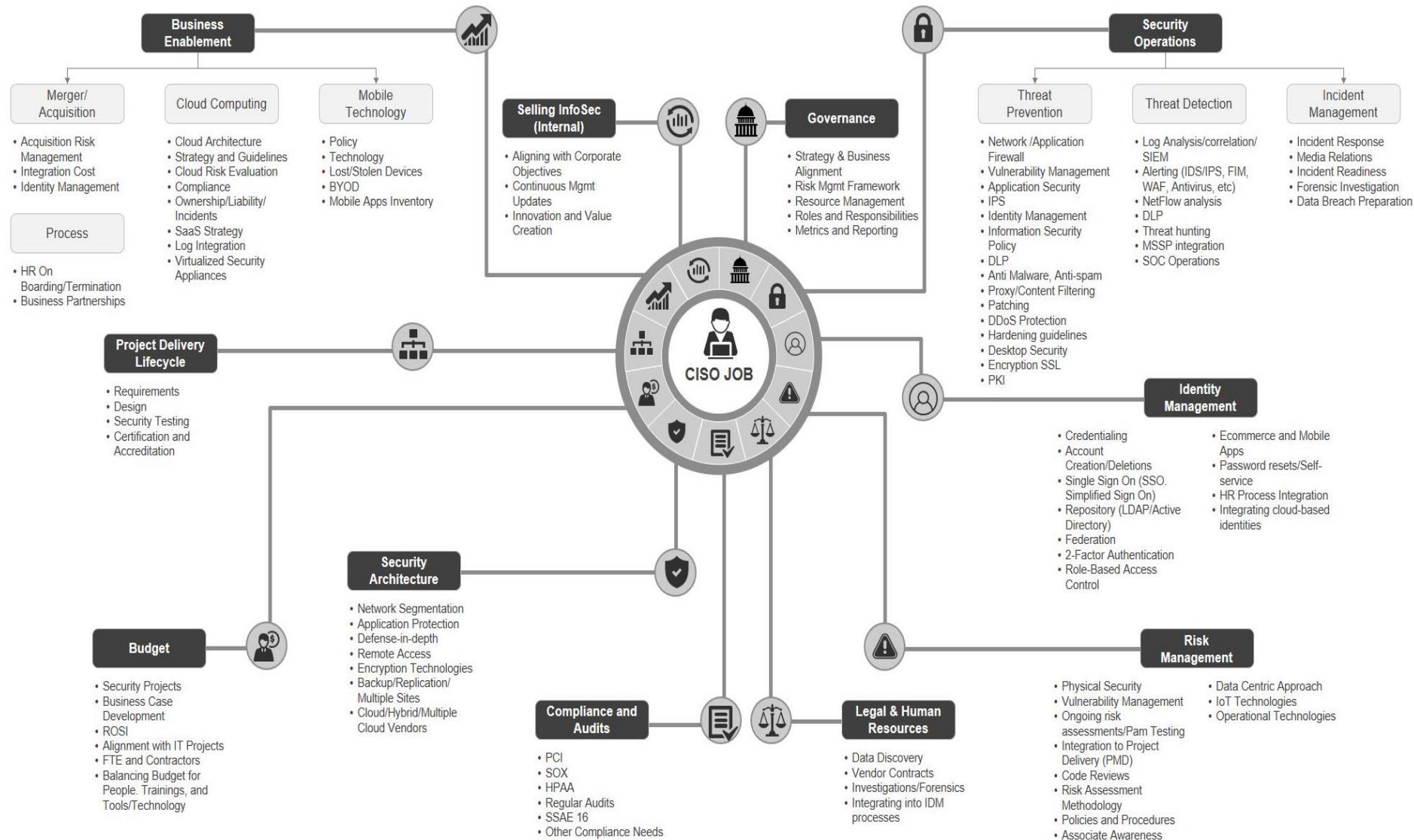
A strategic thinker able to interpret the changing threat landscape, understand the implications of changing technology, and enable the business to achieve it's goals.

**What is a
security professional not?**



**What does a
security professional do?**

CISO Mind Map: Overview of the responsibilities and ever expanding role of the CISO



What are employers looking for?

Employers are looking for


- **Passion**
- **Demonstrated interest**
(informed on current events & trends)
- **Practical experience**
(implementing and configuring security tools – home lab)
- **Security Certifications**

**How can you gain security
skills and demonstrate your
abilities?**

Be informed on current events & trends

Websites / Blogs

- OCIO Security News Digest
- threatpost.com
- securityweekly.com
- Reddit (/r/netsec & /r/AskNetsec/)
- krebsonsecurity.com
- darkreading.com



Read something
security-related
every day!

Training

- formal classroom-based (eg. SANS)
- online courses, webcasts
 - opensecuritytraining.info
 - cybrary.it
 - coursera.org

Get familiar with the basics

- risk
- security awareness
- secure coding and systems
- networking

Information security

From Wikipedia, the free encyclopedia

Information security, sometimes shortened to **InfoSec**, is the practice of defending **information** from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).^[1]

Overview [edit]

IT security

Sometimes referred to as **computer security**, information technology security is information security applied to technology (most often some form of computer system). It is worthwhile to note that a **computer** does not necessarily mean a home desktop. A computer is any device with a **processor** and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the **technology** within the company secure from malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal systems.

Information assurance

The act of providing trust of the information, that the Confidentiality, Integrity and Availability (CIA) of the information are not violated. E.g., ensuring that **data** is not lost when critical issues arise. These issues include, but are not limited to: natural disasters, computer/server malfunction or physical theft. Since most information is stored on computers in our modern era, information assurance is typically dealt with by IT security specialists. A common method of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arise.

Threats [edit]

Information security threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. Most people have experienced software attacks of some sort. **Viruses**,^[2] **worms**, **phishing attacks**, and **Trojan horses** are a few common examples of software attacks. The **theft of intellectual property** has also been an extensive issue for many businesses in the IT field. **Identity theft** is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information. Theft of equipment or information is becoming more prevalent today due to the fact that most devices today are mobile.^[citation needed] **Cell phones** are prone to theft, and have also become far more desirable as the amount of data capacity increases.^[citation needed] **Sabotage** usually consists of the destruction of an organization's **website** in an attempt to cause loss of confidence on the part of its customers. Information extortion consists of theft of a company's property or information as an attempt to receive a payment in exchange for returning the information or property back to its owner, as with **ransomware**. There are many ways to help protect yourself from some of these attacks but one of the most functional precautions is user carefulness.^[citation needed]

Be informed on current events & trends

Social media

- LinkedIn
- Facebook
- Twitter
- YouTube



Groups & meetups

- Victoria Cyber Security Hackers Group
(<http://www.meetup.com/Victoria-Cyber-Security/>)
- ISACA Student Membership

Videos & Conferences

- DEFCON
- BlackHat
- Security B-Sides
- Privacy & Security Conference (Victoria)
- CanSecWest
- RSA Conference

Job experience

Co-op

Shadowing / On-loan

Mentoring

Internship

Leadership Development Program

Volunteer

⋮



Security certifications

CSX:F	Cybersecurity Fundamentals Certificate
CISSP	Certified Information Security Professional
C EH	Certified Ethical Hacker
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
PCI QSA	PCI Qualified Security Assessor
CCSP	Certified Cloud Security Professional
GSEC	GIAC Security Essentials
Security+	CompTIA Security+
LPT	Licensed Penetration Tester

Security+ is good for beginners and CISSP/CISM/CISA are most requested by employers

Education

- while there are diplomas and masters programs there is presently no 4 year undergraduate degree in cybersecurity
- while many security professionals have education in computer science or engineering it is a popular misconception that this is a requirement for all roles
 - for many IT focused roles it is certainly easier if you meet these requirements
- for other roles psychology, criminology, or business may be equally relevant educational programs

Security professionals come from all walks of life

Background

- consider what existing security professionals share in common...
- many have gathered significant experience across a variety of roles
- effective security professionals are well-versed in a variety of areas
- some have many years on a helpdesk familiarizing with a variety of problems and their solutions
- many have the 'hacker mindset' – continual curiosity and tendency to use things in ways they weren't intended

Background

- **successful security professionals will value confidentiality, integrity, and availability (CIA)**
- **a strong sense of doing the right thing and leading by example**
- **historically security professionals were seen as wanting to secure everything to 'Fort Knox' levels**
- **presently security professionals will adopt a risk-based approach balancing with business needs**

Take the first step... get educated... get involved...