
Recruiting
Cybersecurity Talent
What You Need to Know About
Overcoming the Cyber Skills Shortage
HIREVELOCITY

Introduction

Almost every day we hear about a new data breach. They happen everywhere, from small startups to huge, globally recognized companies. No one, it seems, is safe from the growing threats of hacking and cybercrime. The data revolution has escalated the problem as well, with more and more sensitive information residing in the cloud, tantalizingly close for anyone with the tech know-how to crack the encryption or break through a firewall. Companies need better cybersecurity strategies, but building a secure technology environment isn't as straightforward as it used to be.

Cybersecurity in 2018 is a different animal from the strategies most companies used just ten years ago. Defensive strategies based on network management have become less practical with decentralized networks that include Internet of Things technology and Bring Your Own Device policies. Each device or object that connects to the network comes with a potential for new threats.

What You'll Learn...

Understanding the Threat

Companies are vulnerable, and they know it. One study found that 63% of CEOs are concerned about cyber threats. That's higher than the percentage concerned about over regulation, geopolitical uncertainty, or terrorism. Another report indicated that a whopping 82% of IT decision makers are concerned about a shortage of cybersecurity skills. At the same time, however, companies also worry about losing competitive advantage to competitors with better technology, so they keep investing in new technology capabilities like machine learning, AI, and IoT even as their IT teams scramble to provide adequate cyber protection.

82% of IT decision makers worry about a shortage of cybersecurity skills

That's why demand for cybersecurity talent is on the rise. As of 2015, estimates placed the number of global cybersecurity job openings at one million, and that number can be expected to increase with the rapid evolution of technology.

The two questions companies must answer are: what kind of cybersecurity do we need, and whom should we hire to meet that need?

Recent security breaches like the 2017 Equifax hack have exposed personal information belonging to millions of consumers, and it's enough to make even the savviest online shopper pause. As companies depend more heavily on SaaS models and cloud infrastructure to conduct daily business, their security concerns become the concerns of their customers as well. Today's security measures must protect not only the company's assets and data, but also those of their clients and customers, and they must do so in an environment where cyber attacks continue to become more sophisticated and more adept at overcoming traditional protective measures.

That means cybersecurity must address several layers of threats. Let's start with that first question: **what kind of cybersecurity do you need to protect your network and data?**

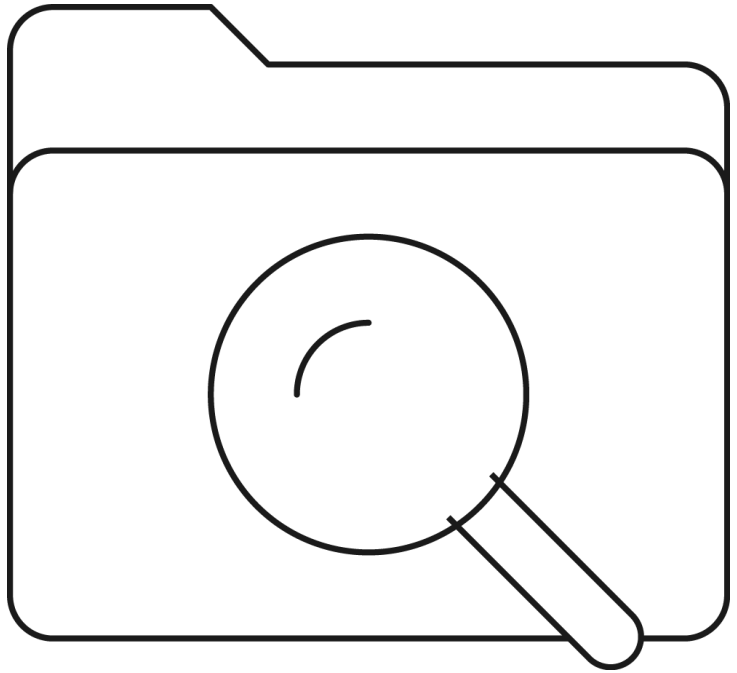
Know the Enemy: Cyber Threats That Put Your Data at Risk

As any military strategist (or lawyer) knows, planning a successful defense requires deep knowledge of the enemy. While it may not be possible to prevent every cyber attack, you can counter them effectively when you know what to prepare for. Let's take a look at 9 types of cyber attacks that threaten your network and data:

- **Malware**—Malware refers to any code that is designed to steal data or cause harm. It is a broad category that includes Trojans, viruses, worms, wipers and other malicious code.
- **Ransomware**—Ransomware uses a malicious virus or Trojan to encrypt data until the user pays a ransom. Well-designed ransomware is nearly impossible to decrypt without the decryption key. The code may also threaten to publish sensitive data or block access to it.
- **Data Sabotage**—Because data has become the lifeblood of organizational decision-making and strategy, new ransomware attacks not only hold data for ransom but also may manipulate or destroy the data. In some cases, attackers will change data for their own profit, but in others they change data randomly leaving companies with the difficult task of verifying its integrity.
- **Botnets**—Botnets take malware to the next level, creating a network of private computers that are infected with malicious code. They can be used to steal data, drop off ransomware, or access devices remotely and may affect hundreds or thousands of machines. Some botnet creators will rent their networks to others, making them even more persistent threats for security professionals to address.
- **Phishing**—Phishing attacks steal personal information by enticing users to click on a link that takes them to a website masquerading as a legitimate company. They have gotten much more sophisticated in recent years, and it can be hard to tell the difference between the dummy site and the real deal.
- **Denial-of-Service (DOS)**—DoS attacks disrupt network service by flooding the network with connection requests and overloading the system. Distributed denial-of-service (DDoS) attacks send the traffic from many different sources, making it more difficult to stop the attack or track it to its source.

- **Man in the Middle (MITM)**—MITM attacks covertly intervene in communications between two parties. The attacker may steal information transferred between the two end users or may alter the information that is relayed.
- **Drive-By Downloads**—Drive-by downloads use malicious code to download programs to the user's device without consent. The malware may go into effect when a user clicks on a website, email message or pop-up window.
- **Rogue Software**—Rogue software leads users to believe that they need a malware removal tool to remove a virus from their device. It can be used to download malicious code or to fraudulently solicit money.
- **Malvertising**—Malvertising downloads malware onto a person's computer when they click on an ad. These ads often appear in legitimate advertising networks or websites, making them difficult to differentiate from legitimate content.

Many of these threats have been made possible by the explosion of data that floods into our homes and work places every day and by new connective technology such as the Internet of Things. As connections between devices proliferate, protecting each of those access points becomes more difficult, and that places data at risk.



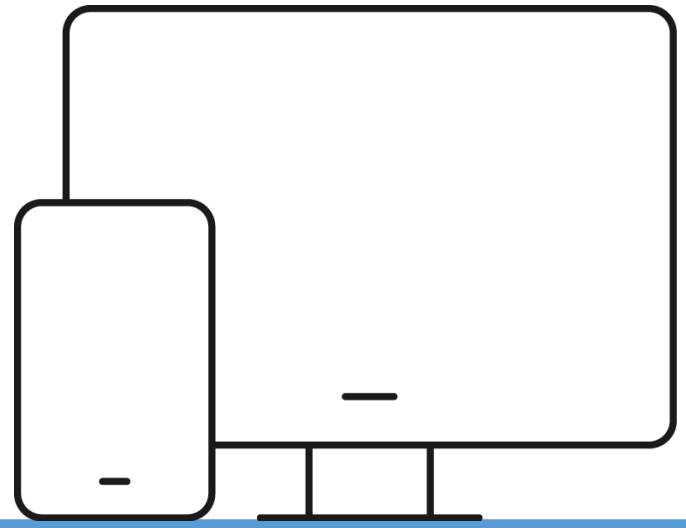
Social Media Threats

Social media threats deserve their own discussion, because these threats target users differently than those delivered by email or website attacks. Here are three types of social media attacks users should watch for:

- **Compromised Personal Information**—Social media channels ask for personal identifiable information like addresses or phone numbers so they can verify your account. Hackers can access this information and use it.
- **Single Login**—As they add more accounts, many users take advantage of a single social login to access all of their social media. This puts every account at risk if a hacker identifies that single password.
- **Phishing Links**—If an account is compromised, scammers can use it to send links and attachments with viruses or malware embedded.

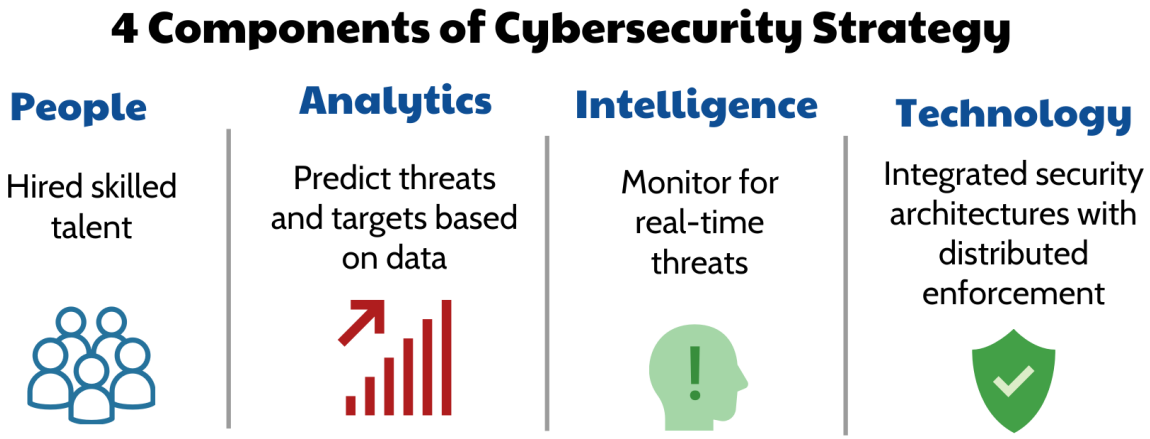
Social media security experts recommend that users carefully protect their information, provide only the minimum details required to open an account, and be wary of unexpected links or attachments—even if they seem to be legitimate messages from friends. But many users aren't aware of the threat. That puts not only their own information at risk, but also network and data belonging to their employer if they inadvertently download malware onto a machine at work.

That brings us to our second question: **What kind of talent do you need to address these risks and protect your network?**



What Your Cybersecurity Strategy Needs to Keep Hackers at Bay

As company networks and the devices connecting to them spread outwards, cybersecurity measures must include defensive strategies that will protect every “node” where a device or machine might access company infrastructure. For that reason, effective cybersecurity strategies should comprise a mixture of people, analytics, intelligence, and technology. Information security professionals must address many different kinds of threats aimed at different potential weak points of the network, and they need a multi-pronged approach that includes not only defensive layers and employee education, but also offensive strategies like identifying abnormalities in the IT environment and increasing physical security around devices and machines.



Within this context, cybersecurity strategies should include threat monitoring and identification, regular audits for devices and access points, an incident response plan, a remediation strategy, and a plan for adapting and innovating as technology continues to evolve.

To develop a well-executed security protocol, companies need Chief Information Security Officers (CISOs) with a high-level understanding of strategy that looks beyond individual threat incidents and views the IT landscape as a whole. They need board members and executives who will support new security initiatives designed to address both current and emerging threats. And they need talented data scientists, software engineers, cybersecurity engineers, security consultants, and IT personnel who can implement strategy.

Simply put, if you don’t have people on your team who understand today’s cybersecurity landscape, you’re a sitting duck.

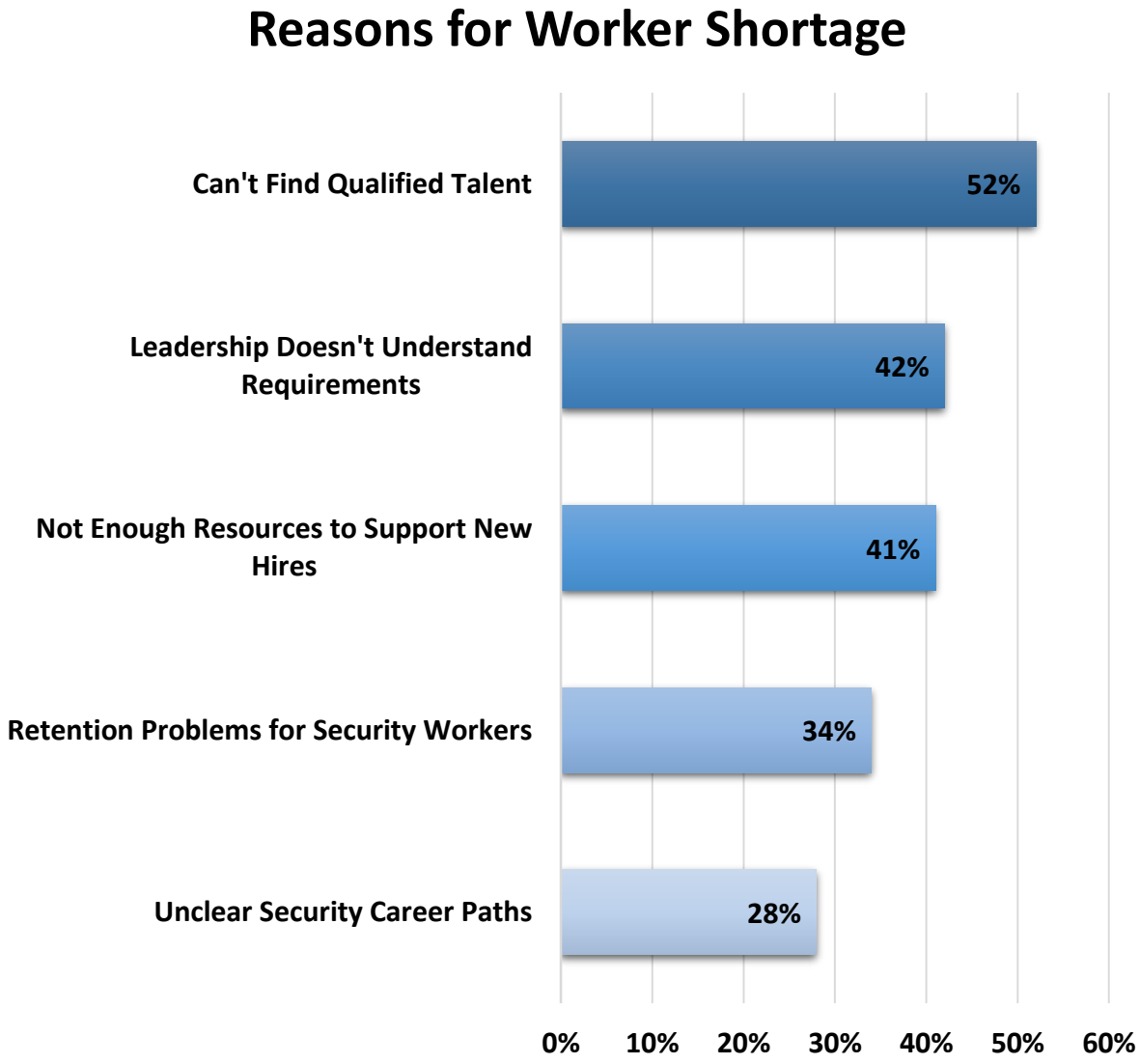
What's Driving Cybersecurity Demand: Top Industries and Job Titles

Compared with today's sophisticated cyber threats, the worms, viruses, and phishing attacks of just ten years ago seem almost quaint. Companies now need to consider industry-specific strategies to address a broad range of threats, and they need not only IT gurus but also data specialists and executive-level talent to create and advocate for continually evolving cybersecurity plans.

Demand for talent has mushroomed and many companies still don't feel confident that they have enough security measures in place. Frost & Sullivan found that 68% of organizations in North America don't think they have enough IT security professionals. They predict a shortfall of 1.8 million jobs by 2022. There are many reasons for the workforce gap, but some of the most commonly cited are shown on the right and include the inability to find qualified talent and unclear paths for security professionals.

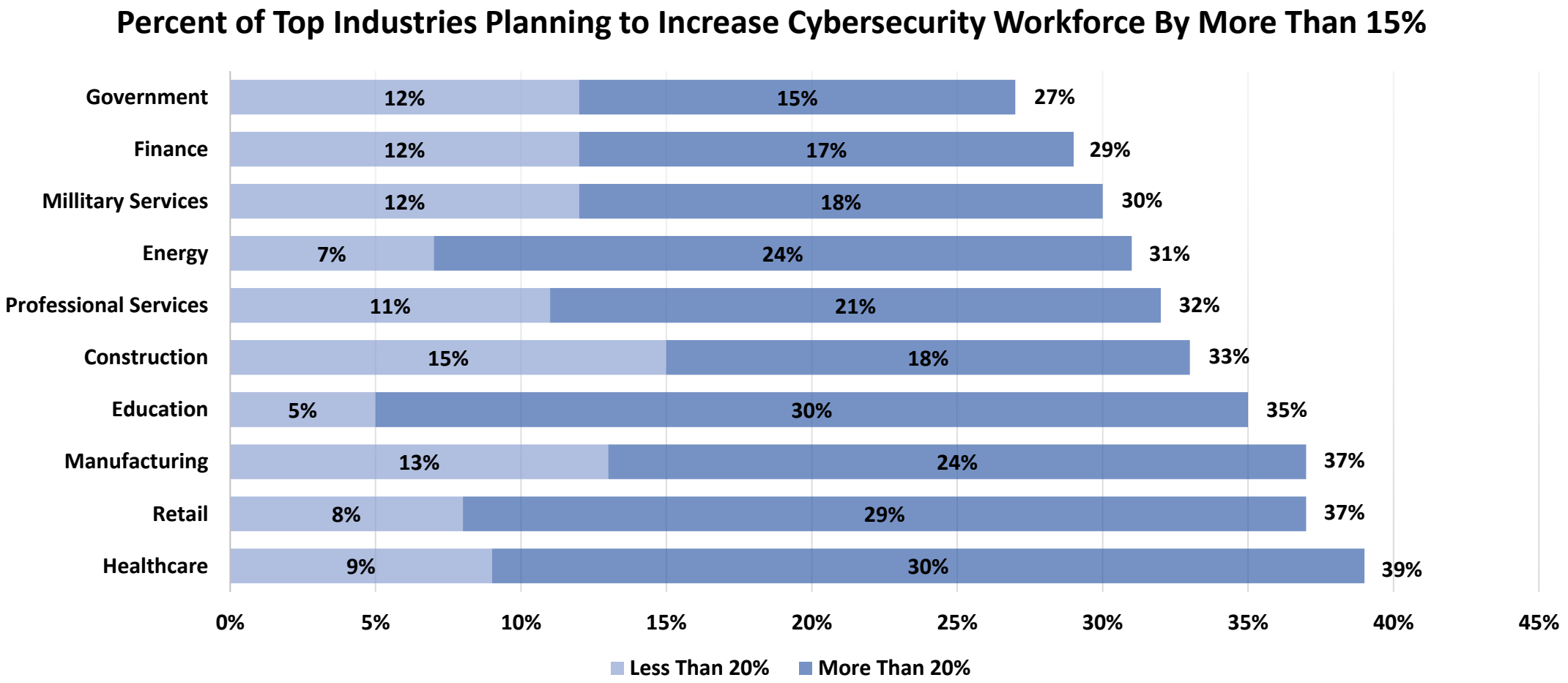
Last year, 70% of hiring managers said they planned to increase their cybersecurity workforce and almost one in three said they wanted to expand by at least 20%.

Everyone is looking to hire, but where are the most pressing shortages?



Top Industries Planning to Hire Cybersecurity Talent

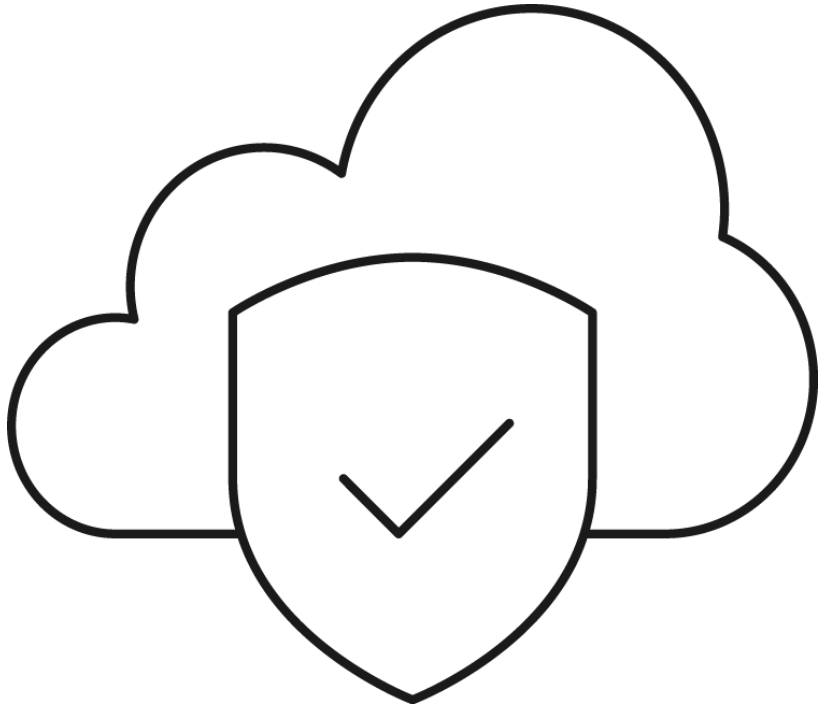
Not surprisingly, the finance and retail sectors were among the top ten industries looking to bolster their information security workforce, but plenty of other organizations feel the pressure to increase protection as well:



Source: [Frost & Sullivan 2017 Global Information Security Workforce Study]

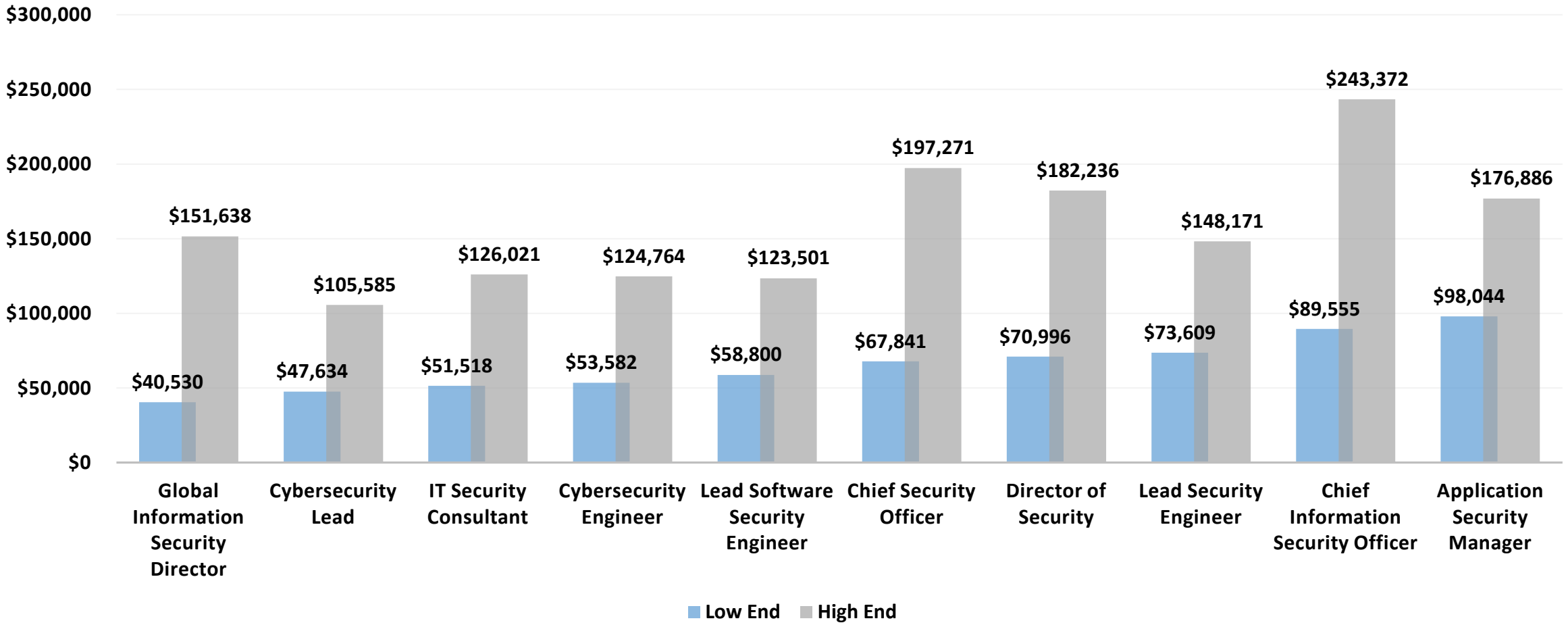
These industries face a growing diversity of cyber threats that put vital information, processes and equipment at risk. Some of the most pressing cybersecurity risks include:

- **Healthcare**—Access to electronic health records, patient names and personal information, and financial details. Threats include ransomware attacks, IoT vulnerabilities related to medical devices, and hacking attempts.
- **Retail**—A widely distributed attack surface that puts employee information and customer data at risk. Threats include hacking, data theft, and information breaches at ATMs, POS contacts, websites, and employee computers.
- **Manufacturing**—Industrial espionage attempts to steal trade secrets and access customer information. Threats include phishing attempts, drive-by downloads, and malicious activity that exploits IoT, network, and supply chain vulnerabilities.
- **Finance**—Access to client personal information, bank account numbers, and private financial data. Threats include ransomware, distributed denial-of-service, and sophisticated phishing attempts.
- **Government**—Theft of personal information, classified information, public funds, and intellectual property. Threats include network vulnerabilities, service disruptions, ransomware, and hacking attempts.



Top Cybersecurity Jobs by Salary Range

To protect sensitive information belonging to themselves and their customers, companies need to hire a range of leaders, specialists, and data management professionals who can create and implement robust cybersecurity strategies. And they're willing to pay top dollar for the right people. These are the top ten IT security jobs by salary range:



Cybersecurity Certifications

As cyber threats continue to multiply, hiring the right people is becoming more difficult. Companies need people with the motivation and knowledge to address threats effectively, but they also need to know those people have the right skills for the job. Cybersecurity certifications have become an increasingly common way to sift through candidate applications to find the best matches.

Let's take a look at five of the most sought-after certifications:

CISA (Certified Information Systems Auditor)

Offered by the global IT nonprofit ISACA, CISA validates skills in audit control, assurance and security. It is globally recognized and provides an excellent foundation for those seeking a cybersecurity position.

Requirements: One year of experience in information systems or a qualifying degree, knowledge of vulnerability assessment and compliance reporting, adherence to the ISACA Code of Professional Ethics, adherence to the CPE program, and compliance with Information Systems Auditing Standards.

Salary Range (Payscale): $60,829 – $122,089

Available Positions (Indeed): 5,212

CCNA Security (Cisco Certified Network Associate)

This certification verifies network security skills and is a good choice for those pursuing a career in network security. Cisco CCNET, CCNA Routing and Switching, or a CCIE certification may serve as a prerequisite for CCNA Security certification.

Requirements: Proficiency in security objectives such as SIEM technology, cloud and virtual networks, BYOD, Identity Service Engine, authentication, Cisco FirePOWER and Cisco Advanced Malware Protection.

Salary Range (Payscale): $51,471 – $96,068

Available Positions (Indeed): 5,975

CISM (Certified Information Security Manager)

A management-focused certification that validates cybersecurity management skills and international security practices. Anyone may take the exam, but must participate in annual continuing education to retain certification.

Requirements: Knowledge of access control, identity management, security management, policies and procedures, intrusion prevention, network and physical security protocols, security tools, and current trends. To retain certification, recipients must complete 20 hours of continuing education annually and comply with ISACA's Code of Professional Ethics.

Salary Range (Payscale): $77,941 – $148,441

Available Positions (Indeed): 3,367

CompTIA Security

This certification is mandated for many government positions, and it's also a common requirement in many other industries as well. That makes it a good choice for those just entering the cybersecurity field.

Requirements: Knowledge of network security, compliance and operational security, threats and vulnerabilities, data and host security, access control and identity management, and cryptography.

Salary Range (Payscale): $42,128 – $95,829

Available Positions (Indeed): 3,821

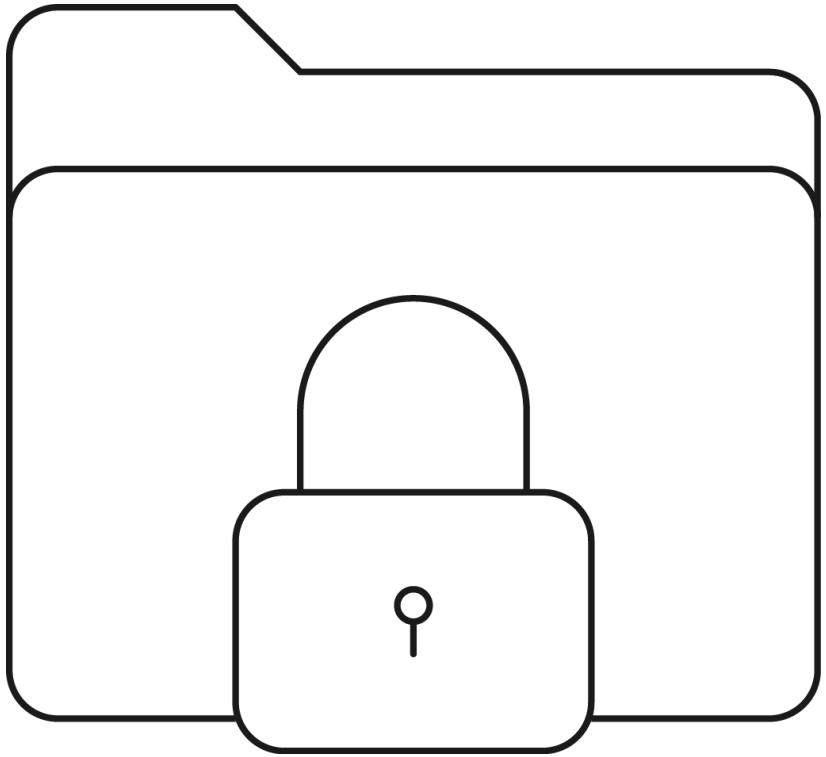
CISSP (Certified Information Systems Security Professional)

This is an advanced certification offered by (ISC)², one of the world's leading IT security professional organizations. It is intended for cybersecurity leaders who oversee enterprise-level security initiatives. It may require many years of work and is globally recognized as an indication of advanced knowledge in the cybersecurity field.

Requirements: At least five years of full-time experience in two of eight qualifying security domains, which must be documented by (ISC)². Recipients must be able to design, engineer, implement, and manage full-scale enterprise-level security programs.

Salary Range (Payscale): $69,490 – $151,148

Available Positions (Indeed): 11,495



8 Strategies For Building Your Cybersecurity Team

Most companies know they need help with cybersecurity. The problem isn't knowledge; it's talent availability. With nearly 2 out of every 3 CIOs desperate to hire skilled IT professionals and cyber threats growing at an alarming rate, the global competition for cybersecurity workers is fiercer than ever—even more so than for other types of IT talent. And the strategies commonly used for identifying and hiring other kinds of talent may not work for professionals in this field.

So how can you win the people you need to keep your data safe and out of the wrong hands? Here are our top tips for sourcing, engaging, and hiring cybersecurity professionals:

1. **Consider strategic goals.** Different industries—and different types of companies within the same industry—need different cybersecurity skills. Talk to your IT managers before creating your job description and emphasize the specific skills you need to accomplish your goals, whether that's information security, e-commerce, or network engineering.

2. **Seek out cyber-specific social media networks.** Cybersecurity professionals tend to guard their personal information more carefully because they know exactly how dangerous it is out there on the web. Look for them in carefully vetted forums and discussion groups that focus on specific topics of interest.

3. **Grow your own talent.** You may already have up-and-coming IT talent on your team. If so, consider grooming these individuals to be your cybersecurity specialists. Offer training and certification, and present the need as an opportunity for challenging, exciting work.

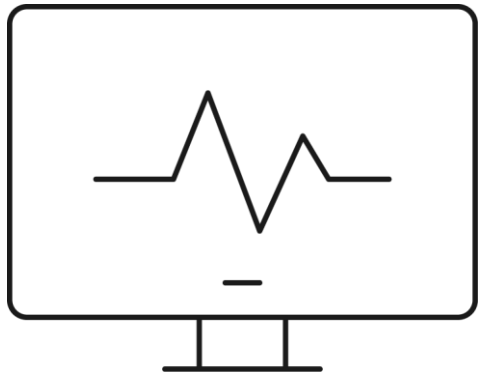
4. **Highlight interesting opportunities at your company.** Brand yourself as an interesting place to work by highlighting the tools, technology, and projects you offer.

5. **Follow marketing best practices.** Marketing depends on matching the right message to the right person, and you can put that methodology to work in your recruiting department as well. Get to know the interests of your ideal hires and frame your job descriptions in a way that piques their interest.

6. **Consider salary, but not exclusively.** Cybersecurity skills command substantial paychecks, so don't be stingy. But keep in mind that professionals in this space also want challenging, interesting work. The right projects or leadership opportunities may be enough to swing a candidate's interest in your favor, even if your salary package can't compete with Google.

7. **Encourage referrals.** One of the best ways to discover new IT talent is to solicit referrals from your current IT team. They likely interact with other professionals in their field more frequently than you do, so ask them to refer people they think would be a good fit for your company (and offer incentives for doing so).

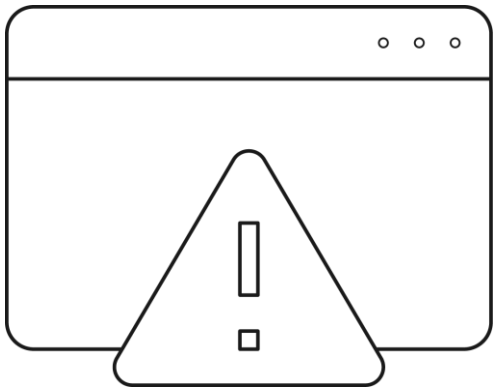
8. **Reach out to passive candidates.** We beat this drum frequently, but don't let that diminish its importance. In the IT community, passive candidates comprise the largest pool of qualified potential talent. Reach out to your network, ask for referrals, attend conferences, and find other ways to connect with passive candidates who may be open to a new opportunity.



Qualified cybersecurity talent is the Holy Grail in the IT space. Without the right people on your team, your organization will be vulnerable to everything from phishing scams to industrial espionage.

At Hire Velocity, we partner with you to secure top talent for your team using:

- Recruitment process outsourcing (RPO)
- Full- or partial-cycle recruiting
- Industry-specific recruitment solutions
- Executive search
- Assessment consulting
- Employer and talent branding
- Talent analytics
- Technology evaluation



Don't put your data at risk. Let's build your cybersecurity team together.

About Hire Velocity

Hire Velocity designs talent strategies that build great teams and great businesses. We are a proven leader in Human Capital Solutions and trusted by companies for customized Recruitment Process Outsourcing (RPO), Search, and Talent & Digital Advisory solutions. Hire Velocity partners with clients across nearly every industry to solve recruiting challenges and achieve sustained outcomes. Consistently recognized as a partner that goes the ‘extra mile’, we are devoted to delivering outstanding service.