The Ultimate Guide to Cybersecurity Planning for Businesses

TechTarget

In this guide:

This in-depth cybersecurity planning guide provides information and advice to help organizations develop a successful strategy to protect their IT systems from attacks.

In this guide:

The ultimate guide to cybersecurity planning for businesses

CRAIG STEDMAN, INDUSTRY EDITOR

Effective cybersecurity is crucial to businesses -- and it's becoming even more important as digital transformation initiatives, cloud computing and remote work expand in organizations. Those trends make IT networks and systems, and the data they contain, more vulnerable to cybersecurity threats that can harm business operations, inflict substantial costs and damage a company's reputation.

Malicious attackers are increasingly targeting internet-connected systems and web applications that aren't properly protected, particularly with more people still working from home because of the COVID-19 pandemic. For example, in an annual survey of cybersecurity professionals conducted in late 2021 and published in 2022 by professional association ISACA, 43% of the 2,031 respondents said their organization was experiencing an increase in attempted cyber attacks -- up by eight percentage points from the previous survey. Similarly, technology research firm ThoughtLab said a survey of 1,200 cybersecurity executives it conducted in late 2021 and early 2022 found that there was an average of 26.2 cybersecurity incidents in organizations during 2021, a 15% increase from 22.7 the year before.

In this guide:

As a result, it's no surprise that many organizations are increasing their investments in cybersecurity. In a survey on 2022 IT spending plans done by Enterprise Strategy Group (ESG), TechTarget's technology analysis and research division, 69% of 344 respondents involved in cybersecurity efforts said their organization expected to increase spending on cybersecurity technologies year to year. That topped the list of planned spending increases for all of the different technologies in the survey.

But spending that money wisely is a must. To help with that, this comprehensive guide to cybersecurity planning explains what cybersecurity is, why it's important to organizations, its business benefits and the challenges that cybersecurity teams face. You'll also find an overview of cybersecurity tools, plus information on different types of cyber attacks, cybersecurity best practices, developing a solid cybersecurity plan and more. Throughout the guide, there are hyperlinks to related TechTarget articles that cover the topics more deeply and offer insight and expert advice on cybersecurity efforts.

WHAT IS CYBERSECURITY?

At heart, cybersecurity is the process of protecting IT networks, systems, applications and data from attacks, intrusions and other cyberthreats. Those threats mostly come from external attackers, but some cybersecurity incidents involve employees and other insiders who may act maliciously or inadvertently cause security problems. In its most recent annual

In this guide:

report on data breaches in businesses, released in May 2022, Verizon said 18% of the 5,212 breaches it confirmed during 2021 involved internal actors.

Cybersecurity programs incorporate a variety of processes and tools designed to help organizations deter, detect and block threats. They're typically run by a cybersecurity department or team that's led by the CISO, the CSO or another senior executive. However, a maxim among security professionals is that everyone in an organization is responsible for information security.

That makes organization-wide cybersecurity awareness and employee training vital to successful programs, as explained in an article on building a cybersecurity culture in businesses by technology writer Mekhala Roy. Security teams first need to make security risks and what needs to be done to protect the organization against them relatable to C-suite executives, then take a human-centric approach to the cybersecurity program, including awareness training. "People think of security as boring and are reluctant to care about it, so it is important to create an emotional connection to make it effective," said Jinan Budge, a principal analyst at Forrester Research.

WHY IS CYBERSECURITY IMPORTANT IN BUSINESS?

Weak or faulty cybersecurity protections can result in serious business problems. Data breaches that gain access to customer records and other sensitive information are a high-profile consequence of network intrusions and attacks. Some prominent examples include the following:

- a 2021 incident in which data on 533 million Facebook users was leaked in a hacking forum, an exposure that the company said was the result of attackers scraping the data from its social network before it updated a feature to prevent such actions in 2019;
- a breach disclosed by Microsoft in 2020 that resulted in 250 million customer service and support records from a 14-year period being exposed online;
- a multiyear breach at Marriott International Inc. that, it said, exposed personal data from as many as 383 million guest records;
- a 2017 breach at consumer credit rating agency Equifax that affected 147 million people in the U.S.; and
- two major breaches at Yahoo, one in 2014 involving records from 500 million user accounts and the other exposing all 3 billion accounts the company had when it occurred in 2013.

In addition to potential lost business because of bad publicity and damaged customer relationships, such breaches can have a tangible financial impact. For example, in July 2019 Equifax agreed to pay up to $700 million in fines and restitution to victims of its breach, as

part of a settlement with U.S. agencies and state governments. Jamil Farshchi, who was hired as the company's CISO in the aftermath of the breach, said in a session during *MIT Technology Review*'s CyberSecure 2020 virtual conference, held that December, that Equifax had also spent $1.5 billion on cybersecurity improvements since the breach.

Other types of attacks directly aim to extract money from organizations. These include ransomware programs, which attackers use to encrypt data files and then demand payments to decrypt them. Distributed denial-of-service (DDoS) attacks that shut down websites and other online systems are also used to try to get companies to pay money to the attackers.

WHAT ARE THE BUSINESS BENEFITS OF CYBERSECURITY?

The biggest benefit that strong network security and other cybersecurity protections provide is the ability to avoid business problems. Organizations can continue to operate smoothly without any disruptions or financial hits from attacks enabled by lax cybersecurity. Security teams should track various metrics on cybersecurity -- such as detected intrusion attempts, incident response times and performance comparisons against industry benchmarks -- to help show business executives and board members how security initiatives contribute to that outcome.

Effective cybersecurity efforts can also pay off more broadly by helping companies achieve their strategic and operational goals. In addition to preventing data breaches and other attacks, building a sustainable cybersecurity program helps support an organization's business objectives, including the environmental, social and governance initiatives that have become priorities in many companies.

WHAT CYBERSECURITY CHALLENGES DO BUSINESSES FACE?

Cybersecurity is inherently challenging -- and even what appears to be a well-designed strategy can be undone by a single weak point. Another maxim among security professionals is that they need to stop all attacks to be successful, while attackers only need to break through an organization's defenses once. In trying to prevent that from happening, cybersecurity teams face a number of challenges:

- constantly evolving security threats and attack methods;
- increasing opportunities for attacks as data volumes, digital operations and remote work grow;
- a large attack surface due to the proliferation of systems, applications, mobile devices and other endpoint technologies;
- new security needs driven by expanding use of the cloud and IoT;
- sophisticated and well-funded adversaries, including state-sponsored cybercrime efforts;

- the use of AI and machine learning technologies to automate attacks;
- budget, staffing and resource limitations;
- a shortage of workers with cybersecurity skills; and
- a lack of cybersecurity awareness among business users.

In an article on the top cybersecurity challenges that organizations face, SearchSecurity executive editor Sharon Shea also cited supply chain attacks, the growth of remote work and hybrid workforces, an ongoing spike in ransomware attacks and more. They all need to be addressed, but there's no magic formula for fully protecting networks, systems, applications and data, Shea noted. "If anything, the pace and scale at which threats and challenges compound will only expand the threat landscape and overwhelm current enterprise defenses more quickly than ever," she wrote.

Another alternative is outsourcing cybersecurity operations to a managed security service provider (MSSP) in an effort to reduce costs and offload the challenges and complexities. In another article, technology writer Mary K. Pratt outlines 15 benefits of cybersecurity outsourcing, as well as the potential drawbacks of managed services and some best practices for working with an MSSP. Outsourcing can be extended to include information security leadership responsibilities through CISO as a service offerings.

CYBERSECURITY SYSTEMS AND SOFTWARE

The cybersecurity technologies that security experts have said organizations should consider using to meet today's challenges of protecting networks and systems include the following:

- a zero-trust security framework that enforces strict authentication requirements on users and devices;
- multifactor authentication to verify users, which most commonly involves two-factor authentication approaches;
- tokenization of sensitive data to better protect it from being exposed if a breach occurs; and
- separate tools for endpoint management and protection, data loss prevention and user behavior monitoring.

That's in addition to widely used technologies such as antivirus software, firewalls, virtual private networks (VPNs) and tools that support access control, email filtering, data encryption, network security monitoring, intrusion prevention, vulnerability scanning, penetration testing and other cybersecurity functions. The available tools include a plethora of free cybersecurity software options, 20 of which are highlighted in an article that provides capsule descriptions of them.

Programming languages are also important components of the cybersecurity toolkit. In an article on the value of coding for security pros, Mike Chapple, teaching professor of IT,

analytics and operations and academic director of the master's program in business analytics at the University of Notre Dame's Mendoza College of Business, details the potential cybersecurity uses of five popular programming languages and how to get started on learning them.

TYPES OF CYBER ATTACKS

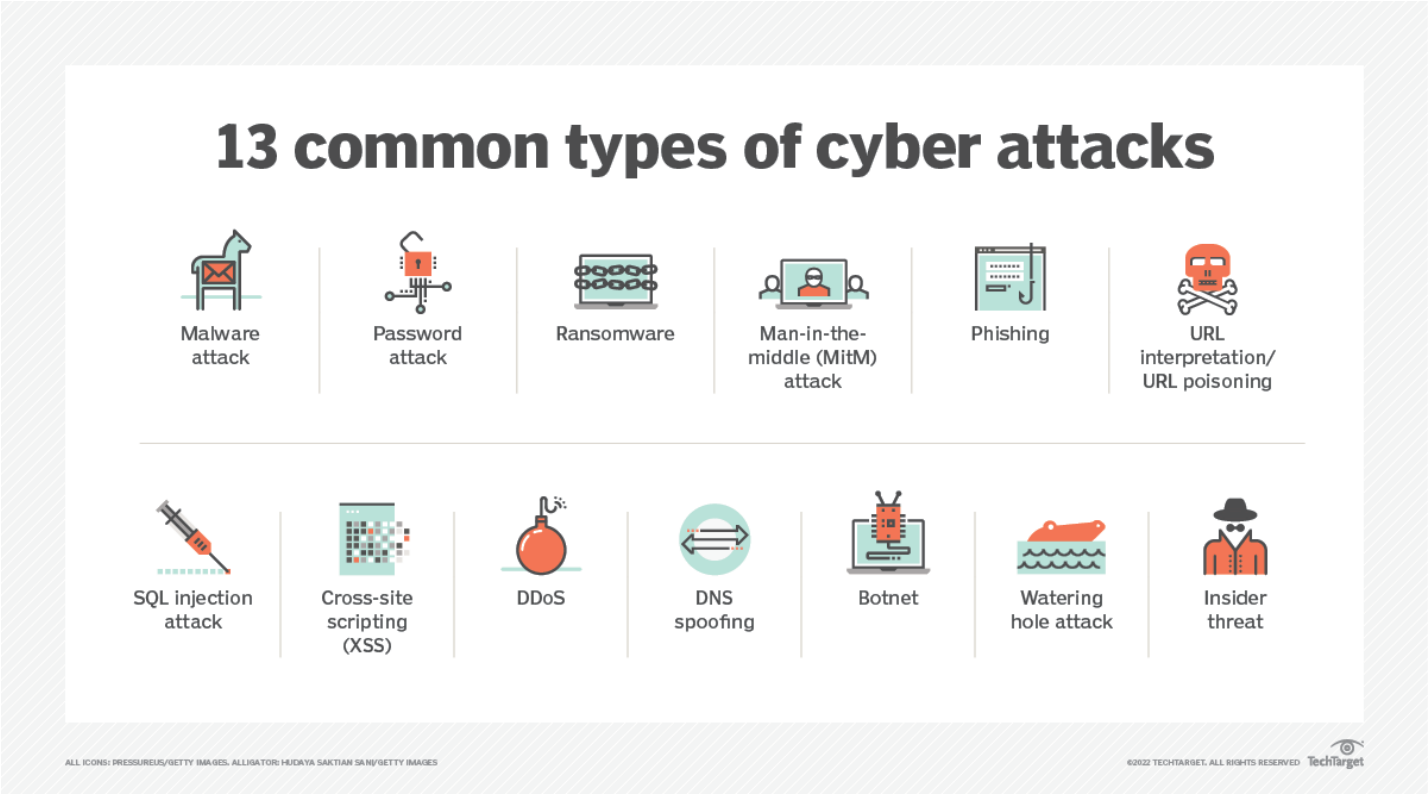
In addition to financial gains from stolen bank account and credit card numbers, ransom payments and intellectual property theft, cyber attacks may aim to disrupt the operations of targeted organizations or be a form of protest against government and corporate policies. One of the complicating factors in preventing cyber attacks is that there also are many different types to guard against.

In an article on the most damaging types of cyber attacks, security author Michael Cobb explains 13 common ones, including the following among them:

- **Malware.** Malicious software programs use social engineering tactics and other measures to fool users and evade security controls so that they can install themselves surreptitiously on systems and devices. Examples include rootkits, Trojan horses, spyware and ransomware. The latter has become the most prominent type of malware and is separately covered by Cobb in more detail.

- **Password attacks.** Obtaining end-user and administrator passwords enable attackers to get around security protections and access systems. Examples of methods used to discover passwords include brute-force attacks, which use generic passwords or automated password-cracking tools; dictionary attacks, which employ a library of often-used words and phrases; and social engineering tactics, such as sending personalized emails to users from a fake account.
- **DDoS.** These attacks seek to overwhelm targeted websites, servers and other systems with a flood of messages, connection requests or malformed packets. They can be used both for ransom demands and to disrupt business operations.
- **Phishing.** Usually done via email, phishing involves an attacker posing as a reputable person or entity to trick victims into disclosing valuable information. Spear phishing targets specific individuals or companies, while whaling goes after senior executives.
- **SQL injection.** This type of attack uses malicious SQL queries to target databases. In a SQL injection attack, a query can be written to create, modify or delete data in a database or to read and extract data.
- **Cross-site scripting.** Known as XSS for short, cross-site scripting injects malicious scripts and code into web applications and website content. It can be used to steal session cookies, spread malware, deface websites and phish for user credentials, among other things.
- **Botnets.** A botnet is a group of computers and devices that have been infected with malware and are controlled remotely by attackers. Common uses include email spamming, click fraud campaigns and generating traffic for DDoS attacks.

In this guide:



The other types of cyber attacks detailed in the article include man-in-the-middle attacks, in which messages between two parties are intercepted and relayed; URL interpretation and poisoning attacks that modify the text of URLs to try to access information; DNS spoofing to send users to fake websites; watering hole attacks that embed malicious code in legitimate websites; and insider threats.

WHAT ARE CYBERSECURITY BEST PRACTICES FOR BUSINESSES?

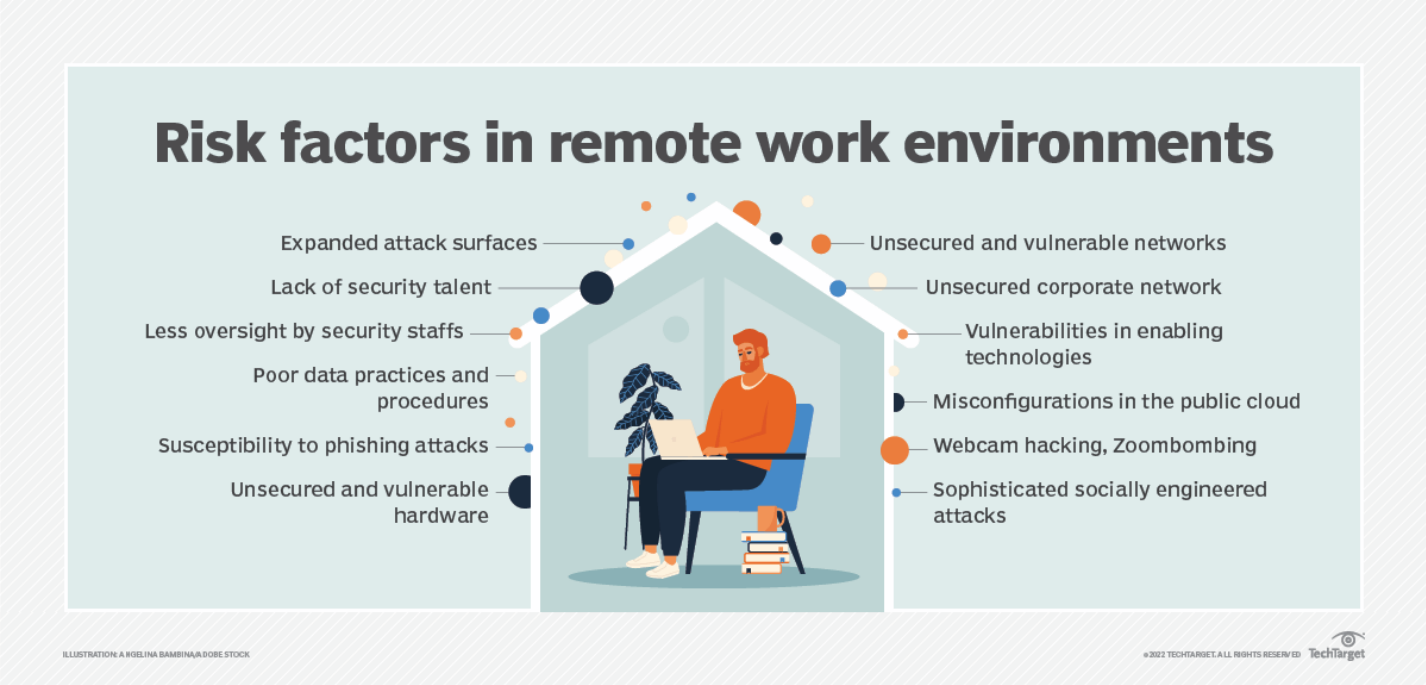
Karen Scarfone, principal consultant at Scarfone Cybersecurity, lists these best practices for cybersecurity teams in an article that also includes tips for business users on how to avoid being victimized by attacks:

1. Update cybersecurity policies and practices as needed.
2. Require strong authentication methods for all users.
3. Refresh network security controls to keep them up to date.
4. Prepare for compromises and other security incidents.
5. Keep your knowledge of security topics and technologies current.
6. Improve security awareness among employees.

On the last item, Scarfone noted that security awareness programs often "are just an hour a year of sitting through the same presentation, plus an occasional email." That kind of box-checking exercise can be a waste of time, she warned. "What's needed is a broader cultural shift to understanding the importance of security and the need for everyone to do their part."

To that end, cybersecurity training for employees should include engaging content and materials and be updated regularly to include information on new threats and operational requirements. An ongoing security awareness program is also a must because of the increased number of remote workers in many organizations. That's one of the best practices

cited in an article by Pratt on managing cybersecurity for remote workers, along with steps such as implementing VPNs and other fundamental security controls for people working remotely and strengthening data protection policies.



In addition, a cybersecurity initiative should have a defined process for managing the attack surface in an organization, which Cobb said should include continuous mapping of the attack surface and automation of data classification and protection measures. He also

recommended that the security team think like attackers to help identify potential points of attack in IT systems.

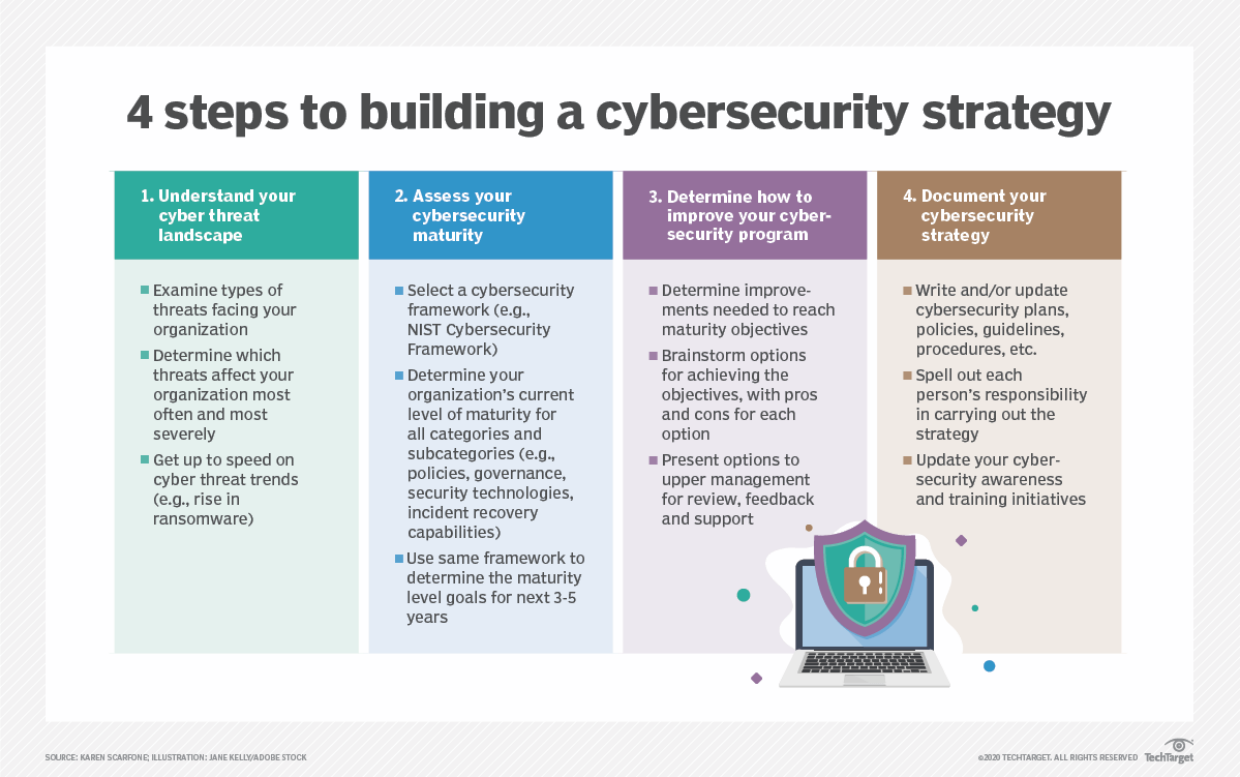
A strong program for governing cybersecurity efforts is also required, as explained by Pam Nigro, vice president of security and security officer at healthcare management software vendor Medecision. Nigro, who also is currently ISACA's board chair, outlined a series of six steps that organizations should take to establish and improve their cybersecurity governance.

HOW CAN YOU DEVELOP A CYBERSECURITY PLAN?

The planning process should start with a cybersecurity risk assessment that identifies key business objectives, essential IT assets for achieving those goals and potential cyber attacks -- as well as how likely the attacks are to occur and what kinds of business impacts they could have. Cobb outlined the following five-step process to assess cybersecurity risks:

1. Scoping the assessment
2. Risk identification
3. Risk analysis
4. Risk evaluation and prioritization
5. Documentation of risk scenarios

Next, an organization can move on to developing a cybersecurity strategy, which Scarfone describes as a high-level plan for the next three to five years -- although, she wrote, "you'll almost certainly have to update your strategy sooner than three years from now." Scarfone specifies four strategy development steps: understanding the threat landscape, assessing your current and desired cybersecurity maturity levels, deciding what to do to improve cybersecurity, and documenting the plans, policies, guidelines and procedures that are part of the strategy.



An effective security plan also requires a budget, of course. Read about creating a cybersecurity budget, including advice on allocating resources to different aspects of the security process and some overall budgeting best practices, in an article by cybersecurity podcast host and writer Ashwin Krishnan.

WHAT IS THE FUTURE OF CYBERSECURITY IN BUSINESS?

As mentioned above, one of the biggest trends affecting cybersecurity is the increase in remote work. That was already an issue before the COVID-19 pandemic, but the coronavirus outbreak has significantly increased the number of remote workers -- and exacerbated the cybersecurity risks posed by employees working from home. In a list of seven top cybersecurity trends in 2022, Gartner cited the expanded attack surface resulting from the growing ranks of remote workers and several other factors as a major area of concern for organizations.

Other trends that are shaping future cybersecurity needs and challenges include the following items, as explained by Karen Scarfone:

- **Increased security automation.** While AI and machine learning can aid attackers, they can also be used to automate cybersecurity tasks. For example, AI tools can quickly detect potential threats in security event data and identify patterns of malicious activities that humans might not see.

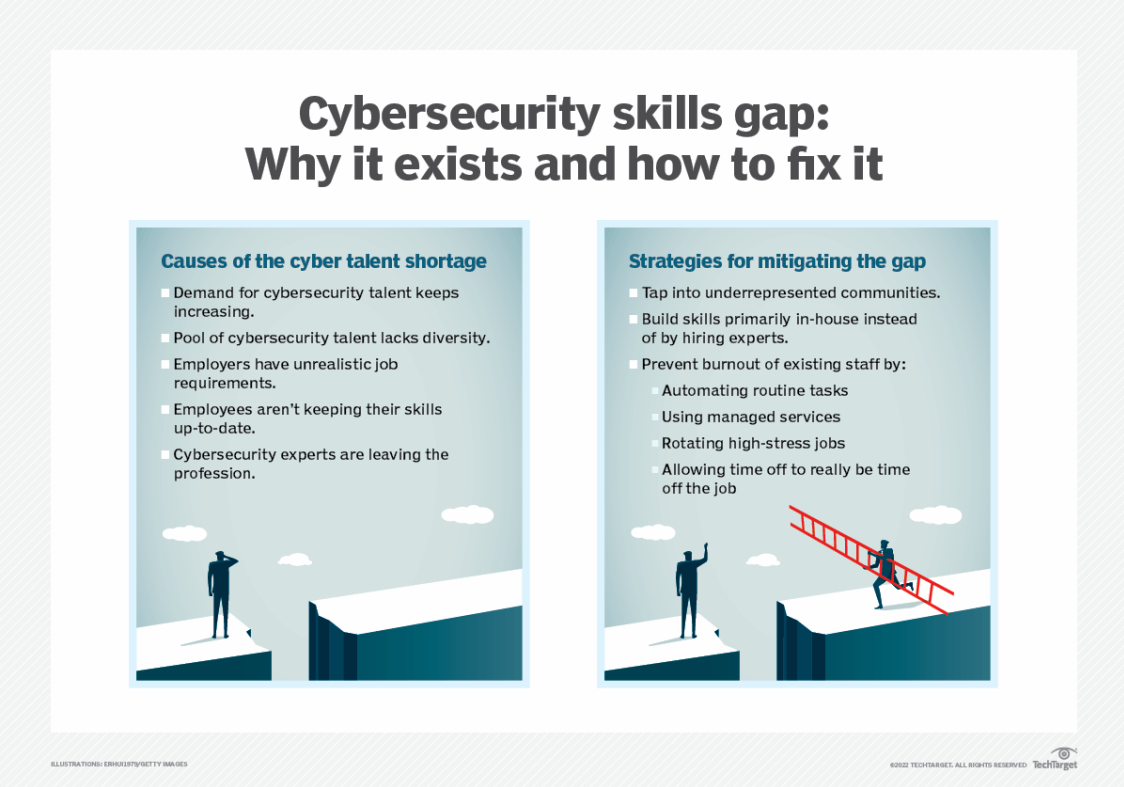
- **Zero-trust security adoption.** Zero-trust principles assume that no users or devices should be considered trustworthy without verification. Implementing a zero-trust approach can reduce both the frequency and severity of cybersecurity incidents, along with other zero-trust benefits.
- **Continued improvements in response capabilities.** In particular, Scarfone cited the need for organizations to be prepared to respond to large-scale ransomware attacks so that they have a strategy in place for handling such incidents before they occur.
- **Recognizing supply chain security risks.** The massive SolarWinds backdoor attack against government and enterprise networks, discovered in December 2020, illustrates the potential cybersecurity risks that supply chains pose -- a danger that calls out for improvements in security strategies and technologies.

Increased adoption of secure access service edge technology -- better known by its acronym, SASE -- and security operations centers are also among the expected trends in cybersecurity, as are emerging measures to help organizations defend themselves against possible attacks driven by quantum computing. Another emerging concept is a cybersecurity mesh architecture, outlined by Gartner, that applies a multilayered approach to help manage security in complex IT environments.

CYBERSECURITY SKILLS AND CAREER PATHS

According to a July 2021 research report published by TechTarget's ESG division and International Systems Security Association (ISSA) International, 57% of 489 surveyed ISSA

members said their organizations have been affected by the shortage of skilled cybersecurity professionals. The vast majority of these cyber professionals believe the skills gap has not improved over the past several years, and 44% of respondents said the cybersecurity skills shortage has gotten worse -- a problem that can be mitigated, Scarfone advised, by looking to groups of people who are underrepresented in IT now, building skills in-house and better supporting existing security staffers.



The ongoing skills shortage means there are lots of job opportunities for prospective cybersecurity workers. Technology writer Rahul Awati provides a breakdown of the most in-demand cybersecurity positions in organizations by role level, salary, education requirements and skills.

In an article based on input from a group of experts in the cybersecurity field, technology writer Steve Zurier lists 10 key skills for cybersecurity professionals to possess -- a combination of technical and soft skills that organizations should look for in job candidates. Related articles detail common cybersecurity job interview questions -- and how to answer them -- and outline a five-step career path in cybersecurity.

CYBERSECURITY CERTIFICATIONS AND ONLINE COURSES

Experienced cybersecurity professionals looking to advance their careers, and new workers hoping to get into the field, can bolster their skill sets and résumés by obtaining certifications offered by various industry groups and IT vendors. In another article, Zurier provides details on the top cybersecurity certifications that are available, including what they involve, how much they cost and the jobs they fit.

Online courses are another avenue for bolstering cybersecurity knowledge and skills. A large number of free and paid courses are available. A final article by Zurier contains information

on useful cybersecurity online courses recommended by a panel of security pros, including courses offered by courseware providers, industry groups, academic institutions and U.S. federal agencies.