Enterprise cybersecurity: A strategic guide for CISOs

June 2025

TechTarget

In this guide:

Effective enterprise cybersecurity has become even more important as organizations extend their efforts in digital transformation, cloud computing, hybrid work and AI technologies. CISOs and others responsible for safeguarding an organization's systems, networks and data need to manage day-to-day threats while also planning strategically for what's ahead. This comprehensive guide to enterprise cybersecurity explains what's at stake and how CISOs and other security leaders can spend wisely and effectively to meet the many challenges that cybersecurity teams face.

In this guide:

Enterprise cybersecurity: A strategic guide for CISOs

PHIL SWEENEY, INDUSTRY EDITOR | CRAIG STEDMAN, INDUSTRY EDITOR

Effective enterprise cybersecurity has become even more important as organizations extend their efforts in digital transformation, cloud computing, hybrid work and AI technologies. Those trends make IT networks and systems -- and the data that ceaselessly moves through them -- more vulnerable to cybersecurity threats that can harm business operations, inflict substantial costs, knock a company out of compliance with regulations and damage its reputation.

Cybercriminals increasingly target systems and applications that aren't properly protected. As enterprise cybersecurity staffers scramble to shore up vulnerabilities, hackers and attackers seek out those same weak points. It can sometimes feel like a race, and security groups often don't feel like they are winning.

In an annual survey of cybersecurity professionals conducted in 2024 by IT professional association ISACA, only 40% said they were completely or very confident in their cybersecurity team's ability to detect and respond to threats; that's down slightly from the prior year, when 42% expressed those same degrees of confidence.

In this guide:

Security perennially sits at the top of IT spending priorities for most organizations. Enterprise Strategy Group, now part of Omdia, reported in its annual technology spending survey that 72% of respondents said their organization would spend more on cybersecurity in 2025 than in 2024; 26% indicated security spending would be about the same as the previous year.

But spending money on security doesn't necessarily mean a business has improved its security posture. To help with that gap between writing checks and solving problems, this comprehensive guide to enterprise cybersecurity explains what's at stake and how CISOs and other security leaders can spend wisely and effectively to meet the many challenges that cybersecurity teams face.

THE IMPORTANCE OF ENTERPRISE CYBERSECURITY

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 result from employees and other insiders acting with maliciousness or carelessness.

Enterprise 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

In this guide:

senior executive. Even so, a maxim among security professionals is that everyone in an organization is responsible for information security.

That makes building a strong cybersecurity culture through organization-wide security awareness and employee training vital to successful programs. Security teams need to promote individual responsibility and accountability for cybersecurity, encourage collaboration between different departments on security planning, and reinforce the crucial importance of enterprise cybersecurity to business success.

Weak or faulty cybersecurity protections can ignite serious business problems, from data breaches exposing sensitive customer records to regulatory fines for noncompliance, theft of intellectual property and ransomware attacks demanding a payment to restore encrypted data files or not publicly disclose them. A 2024 report from IBM put the average cost of a data breach at $4.88 million. In the case of a ransomware attack, even businesses that have securely isolated their data backups and decide not to pay a ransom will still need to rebuild systems to get operations up and running again. In addition to the tangible financial impact of faulty cybersecurity, enterprises face potential lost business because of bad publicity and damaged customer relationships. Effective cybersecurity is tantamount to business survival.

In this guide:

WHAT ARE THE BUSINESS BENEFITS OF CYBERSECURITY?

The key benefit a strong security posture provides is the ability to avoid business disruptions. 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.

The significance of cybersecurity extends beyond the day-to-day operations of the business. In a potential merger or acquisition, executives and their representatives conduct due diligence to see how the two entities might function as one. That analysis should include the cybersecurity ramifications of such a transaction.

WHAT CYBERSECURITY CHALLENGES DO BUSINESSES FACE?

Enterprise cybersecurity is inherently difficult, and CISOs and their colleagues must contend with constantly evolving security threats and attack methods. Even what appears to be a well-designed strategy can be undone when cybercriminals uncover a single point of weakness. While security professionals are under pressure to stop every attack, their adversaries can be successful by breaching defenses just once.

In trying to prevent that from happening, cybersecurity teams face challenges that include the following:

- Attacks enabled by AI or generative AI (GenAI), such as highly convincing phishing attempts.
- Staffing challenges, such as hiring experienced security analysts.
- Ransomware, a persistent threat that now includes tactics such as double extortion, in which cybercriminals encrypt and extract data, and triple extortion, which could also ensnare customers and suppliers.
- Regulatory complexity, which varies by industry and geography. Financial institutions in the EU, for example, must contend with strong, enforceable risk management regulations through the Digital Operational Resilience Act. Companies doing business in Europe are also subject to stringent rules over data security and privacy as part of the GDPR's requirements. In the U.S., publicly traded companies must file Form 8-K within four days of a security incident. And that's just the beginning.

Other challenges run the gamut from stolen credit card information to sorting through deepfakes to maintaining communications security.

AI ASSISTS ATTACKERS AND DEFENDERS

Increasing enterprise use of AI in general -- and GenAI, in particular -- opens a whole new world of cybersecurity concerns. For example, end users might inadvertently enter sensitive data or code into a GenAI tool, which could then expose the data to competitors or attackers. In addition, AI applications pose regulatory compliance risks and could enable data poisoning attacks that affect the behavior of AI models, among other issues. Organizations must now factor management of AI and GenAI security risks into their cybersecurity programs and policies.

AI is seen as a weapon for both cybercriminals and cyberdefenders alike. GenAI is especially appealing to threat actors, who use it to enhance their phishing attempts and create more effective malware. AI-powered attacks are a new risk, and they are expected to grow more effective as bad actors exploit AI's capabilities.

Security products that incorporate AI can help fend off the onrush of threats, detecting attacks in real time and potentially acting on their own to stop them. In fact, some experts suggest the technology's speed and power make AI the only tool capable of meeting the AI threat.

For now, at least, AI in security serves as a supplement to other defenses. Companies use it most often to automate threat detection and response, secure endpoints, handle routine security tasks and detect fraud.

SECURING AI ADOPTION

Whether companies can reap the benefits of AI while mitigating the risks is an open question. The rapid push to adopt AI across the business in nonsecurity uses has been done without much thought about how secure those uses might be. According to ISACA's "2024 State of Cybersecurity" survey, 45% of security professionals said no one on their team was involved in how their organization developed or implemented AI products. Similarly, 41% said no one on the security team played a role in the development of a policy governing their company's use of AI.

Todd Thiemann, a security analyst at Enterprise Strategy Group, sees the possibility of deepfakes and other AI trickery routinely being used to fool IT staff and systems involved in areas such as identity validation. For example, a seemingly legitimate request from an employee needing help resetting their password might be an AI-generated scam. "That's something that security folks are quite concerned about in terms of credential reset -- making sure you're not resetting it for an adversary," Thiemann said.

In this guide:

RISE OF AGENTIC AI AND THE EXPANDING ATTACK SURFACE

Developments in agentic AI are another growing concern in the security community.

Agentic AI holds great promise, Thiemann said, but only if it is implemented in ways that protect data.

"Agentic AI, to really show the value, is going to tap into a lot of those enterprise data stores," he said. The benefit of crossing data boundaries also carries risks. "When you have agents calling agents calling agents, there's going to be an opportunity for data loss."

As such, agentic AI represents a broadening of the attack surface, which adds to the challenge of crafting an effective attack surface management strategy that addresses the following areas:

- Digital attack surfaces, which include cloud applications and APIs.
- Physical attack surfaces, which can be everything from desktops to server rooms.
- Human attack surfaces, which involve phishing, smishing and compromised email accounts.
- Third-party attack surfaces, which could involve supply chains and cloud providers.

SECURITY TALENT SHORTAGE

An ongoing challenge in enterprise cybersecurity is finding and retaining skilled personnel. Workers with experience in certain in-demand roles, such as security analysts and engineers, are not easy to recruit. Experienced cybersecurity specialists command high salaries, and people with a mix of technical expertise and managerial soft skills are sometimes difficult to find and retain.

Only 38% of security managers surveyed by ISACA in 2024 said their teams were appropriately staffed. This was a slight improvement over the prior year but nonetheless an indication that the industry hasn't resolved its problems with getting the right people into the right jobs.

What job seekers should know

For those seeking a job in enterprise cybersecurity, it is good to consider what a potential career path might look like, which online courses could be helpful, which skills employers consider most valuable and how to be ready for that job interview.

It might also be helpful to review the many certification options in the security field to see if those might help advance career progression.

TOP CYBERTHREATS FACED IN THE ENTERPRISE

What makes cybersecurity such a complex effort is that defenders are asked to prevent so many different types of attacks. Even well-understood threats continue to evolve and emerge in new variations. Defenses continually adjust to threats, and threats continually adjust to defenses.

The following are some of the most common -- and potentially damaging -- cyberthreats:

- **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. Ransomware has become the most prominent type of malware, striking nearly 60% of businesses,

according to Sophos' "The State of Ransomware 2024" report. Other examples include rootkits, Trojan horses and spyware.

- **Password attacks.** Obtaining end-user and administrator passwords enables attackers to get around security protections and access an organization's IT 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*, 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.

One of the more pernicious cyberthreats is when attackers sneak into a victim's systems and linger, usually undetected, for extended periods of time. Users of these living-off-the-land (LOTL) attacks exploit the networks and applications they encounter, enabling them to launch malicious commands from the inside, achieve lateral movement and avoid external-facing defenses. To prevent an LOTL attack, security teams must actively collect and analyze event logs, use threat detection tools to monitor endpoints and tighten access controls.

In more conventional and less subtle attacks, threat actors will sometimes disguise the sources of their malicious activity by using domain generation algorithms. Because these algorithms create multiple pseudo-random domains, security tools can't identify and block a specific IP address that's the source of a cyberattack.

In situations where data theft is the goal, hackers might engage in advanced persistent threat, or APT, activity. This method of attack relies on a group gaining and then maintaining access to a target's systems for weeks or months. An APT attack is a sophisticated and patient effort, typically undertaken by nation-state groups. The intention is to extract as much sensitive information as possible, as opposed to inflicting direct harm or demanding a ransom.

Other common cyberthreats 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; DNS tunneling that uses malicious data in messages to evade security controls; watering hole attacks that embed malicious code in legitimate websites; eavesdropping attacks, which capture data from poorly secured communications traffic; and birthday attacks, a brute-force technique that can enable attackers to obtain encryption keys and user credentials.

ENTERPRISE CYBERSECURITY SYSTEMS AND SOFTWARE

Cybersecurity teams have a range of technologies at their disposal to protect networks and systems. What they don't possess is readily available in an active and lively security tools market that spans dozens of product categories.

Products exist to address any conceivable threat and to bolster any security weakness. These include the following:

- **Zero-trust security framework.** The zero-trust approach enforces strict and continuous authentication requirements on users and devices, upending the traditional practice of trusting anyone who's able to sign in.

- **Multifactor authentication.** With MFA and passwordless authentication methods, user identities are less hackable than those that rely only on a password.
- **Threat detection and response technologies.** Managed detection and response services and extended detection and response software -- commonly referred to as MDR and XDR, respectively -- help remediate security threats and risks across an entire IT environment.
- **Endpoint management.** This type of product helps an organization configure, patch and otherwise manage devices.
- **Data loss prevention.** With these tools, a security team can better monitor data as it comes and goes on an organization's network.
- **User behavior monitoring.** User and entity behavior analytics tools help detect anomalous network patterns, potentially providing an early warning of a security incident.
- **SIEM.** Security information and event management software collects and analyzes data from multiple sources in an IT environment, pulling it into a unified management console.
- **IDS.** An intrusion detection system checks networks for signatures of known attacks or activity that deviates from norms.

These products are deployed alongside widely used technologies, such as antivirus software, firewalls, VPNs and tools that support access control, email filtering, data encryption, vulnerability management, penetration testing and other cybersecurity

functions. The available tools include a plethora of free cybersecurity software options that organizations can use in addition to or as an alternative to commercial software products.

On the downside, this profusion of products can become a burden. An organization's security environment is likely a customized arrangement of tools from various vendors amassed over many years. Managing all that -- and getting the elements to work together -- can be difficult for some security teams.

Being satisfied with vendors and purchases means being clear about what you have and what you need. A carefully prepared request for proposal, sent to cybersecurity vendors, can save time and trouble later. Use the RFP to clearly inform vendors about the scope of the work, the technical requirements, the preferred timeline and other essential details.

With that RFP in hand, vendors can more accurately assess whether their products might be appropriate for the project.

As a next step, it's smart to invest some time in vendor evaluation. This isn't easy, especially for smaller businesses that might not have in-house expertise -- nor is it cheap. Integrating a new product with tools already in place is not always seamless. In some product categories, big-name vendors compete with scores of startups and

lesser-known players. So, how do you choose a tool that meets your needs, fits your budget and works alongside your existing infrastructure?

A thorough vetting of cybersecurity vendors should include plenty of questions, including the following:

- What's the vendor's track record?
- How prepared is a vendor for incident response?
- How does the vendor secure sensitive data?
- How specific are the contracts and service-level agreements?
- Is the vendor's support service responsive?

With so much at stake, from defending against attacks to making good use of a fought-for budget, choosing a cybersecurity vendor that meets your particular requirements is a big step.

Security teams are increasingly looking to confront some of the tool complexity in their organizations. One goal in this effort is to make better use of what's already in place. A process sometimes described as *tool consolidation* or *tool unification* might help reduce costs, simplify product management, eliminate overlapping features and possibly close some gaps in capabilities.

In this guide:

ENTERPRISE CYBERSECURITY STRATEGY: HOW TO GET STARTED

Begin with a cybersecurity risk assessment that identifies key business objectives, essential IT assets for achieving those goals and potential cyberattacks the organization faces -- as well as how likely the attacks are to occur and what the business repercussions might be.

Next, an organization can move on to developing a cybersecurity strategy, which should be a high-level plan for the next three to five years -- although such strategies often must be updated sooner than that. Strategy development can be boiled down to the following steps:

- Understanding the threat landscape.
- Assessing the organization's current and desired cybersecurity maturity levels.
- Deciding what to do to improve cybersecurity.
- Documenting specific plans, policies, guidelines and procedures.

An effective security plan also requires a budget, of course. CISOs and other security leaders should allocate sufficient resources to key aspects of the security process, including compliance, training and ongoing risk assessments, while also ensuring that security programs can support new business initiatives and changes in business priorities.

WHO IS RESPONSIBLE FOR ENTERPRISE CYBERSECURITY STRATEGY?

Putting up a vigorous defense against cyberthreats requires the participation, or at least the cooperation, of everyone in an organization. Every phishing scam or compromised password is a potentially dangerous spark that ignites a cybersecurity fire.

The daily duties of stopping threats belong to the security team, typically led by a CISO or CSO. These specialists carry the load, locking down systems, securing networks, handling identity and access, and meeting compliance requirements, among other critical functions.

CISOs and their teams have the additional task of being the link between rank-and-file staffers and those with ultimate responsibility: owners, boards of directors and senior business management.

In this guide:

Senior business executives and board members likely understand the *importance* of cybersecurity, but only a few of them understand the *mechanics* of cybersecurity. Leaders with business experience and dealmaking acumen might typically lack insight into their organization's efforts to manage identities, secure systems, safeguard data and conduct effective incident response. Board members understand risk, but many are still learning what questions to ask about security tactics and effectiveness.

It's up to the security leaders within the organization to explain what's being done, what went right and what went wrong. Security leaders should keep senior management aware of what's being done, as well as what remains to be done. The challenge is knowing what important information to share and how to share it with those who don't speak the language of enterprise cybersecurity.

CISO REPORTING AND BUDGETING GUIDANCE

When updating senior leaders -- or requesting funds -- CISOs and security managers should present information in terms of business goals and strategies. Most operational details and metrics won't resonate with executives whose expertise is outside the security realm. In other words: Do board members really need to know how many patches the security team made last quarter?

As Gartner analyst Pete Shoard recently wrote on Cybersecurity Dive: "They are more concerned with how these security incidents could affect the company's

financial health, reputation and operational capabilities. By linking technical data to business-relevant insights, you can best map security measures to business objectives."

"The CISOs I see that are most effective can translate that technical cyber-risk into business risk language, engage with the C-suite, engage with the board," said Matt Gorham, leader of PwC's Cyber & Risk Innovation Institute. "Those that do that are much more successful than their peers, both in terms of the scope of the value they bring to the organization but also getting the resources they need."

CISOs should also take time to educate boards about relevant cybersecurity metrics. Boards are increasingly interested in cybersecurity, at least from the perspective of risk and resilience. Frequent contact is becoming the norm. "The days of a board having a yearly cyber update are gone," Gorham said.

Experts recommend CISOs carefully prepare a cybersecurity board report to guide them through these interactions.

Senior executives and board members understandably will want to know what's being done to protect the organization from cyberattacks, whether customer data is safe, how prepared the business is for a ransomware incident and so on. A key element in these conversations between leadership and a CISO will be cybersecurity budget justification. Corporations spend significant sums on security tools and staff. It is

natural that those making funding decisions will want to know how effective previous investments have been and whether CISOs can defend their requests for additional spending.

Showing security ROI can be tricky. After all, when security works, bad things don't happen -- but it's hard to prove a negative. Experts suggest CISOs discuss ROI metrics for cybersecurity in terms of time saved and money saved.

THE DEMANDING CISO ROLE

To be a CISO is to find yourself in a series of difficult positions. CISOs bear the burden of stopping bad things from happening, and they face the blame when something does go wrong. With organizational support and generous budget allocations, CISOs can accomplish a lot. But even a well-funded security initiative will be challenged by relentless and innovative bad actors. Making one security effort a priority inevitably means deprioritizing others. What seems secure today might be vulnerable tomorrow. The job is never done.

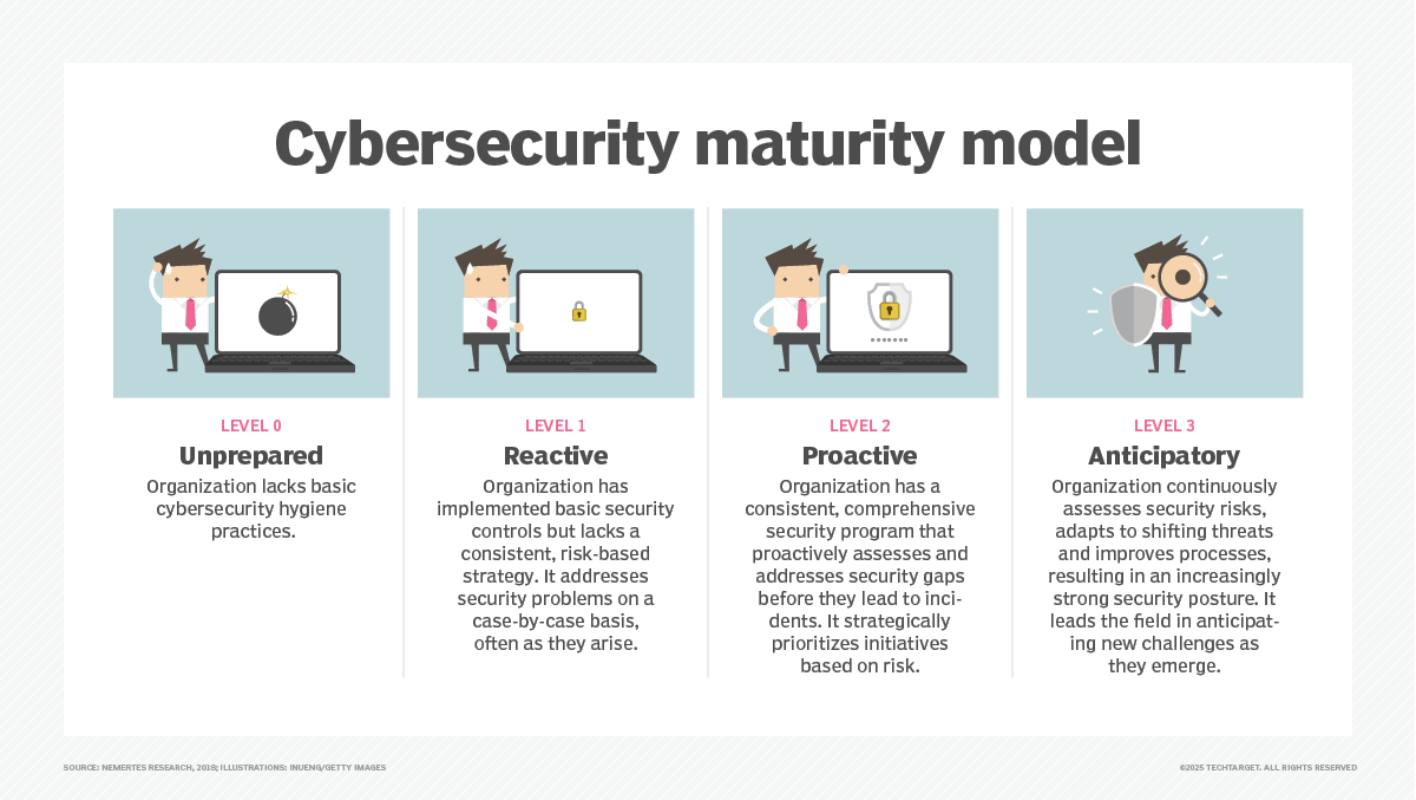
These factors contribute to a high rate of burnout among CISOs. It's a pressure-packed role that requires wisdom to allocate limited budgets in ways that smartly shore up existing weak spots without weakening other defenses. CISOs also need to anticipate where an attack might come from next.

In this guide:

The complexities CISOs confront might require new approaches and structures. A [cybersecurity maturity model](#), for example, provides a framework for an enterprise to define effectiveness. This type of model can help with the following objectives:

In this guide:

- Identify gaps in a company's security controls and capabilities.
- Establish benchmarks so that an organization can better compare its security programs with others.
- Prioritize spending by using awareness of gaps and benchmarked strengths and weaknesses.



CYBERSECURITY TEAMS, RESPONSIBILITIES AND SKILLS

Enterprise cybersecurity can be enhanced by creating an environment for good decision-making, proper planning and competent execution. A well-organized cybersecurity team creates a structure for successful cyberdefense, or at least an increased likelihood of success. Experts recommend that a team define roles for governance and compliance, incident response planning, accountability and other essential functions so that responsibilities are clear and collaboration becomes possible.

Effectiveness also depends on how a security team approaches risk management. While fundamental to cybersecurity, risk management is not always addressed in a systematic way. To do so, a business will need its security team to, among other things, possess an objective understanding of the organization's vulnerabilities, the skill to assemble and manage systems to mitigate those vulnerabilities, and the capacity to respond effectively to security incidents.

Effective cybersecurity risk management includes a mix of important practices, including the following:

- Performing regular security assessments.
- Establishing comprehensive policies.
- Using the right tools, such as intrusion detection and antimalware products.
- Training all employees to recognize common security threats.

When it succeeds, cybersecurity risk management involves collaboration among cross-departmental staff, senior executives, the security team and third-party vendors.

Some teams choose to approach risk in a more sophisticated way by employing what's called *cyber-risk quantification*. With CRQ, a business can systematically measure changes in the threat landscape and the potential business effects of those risks. Organizations consider the CRQ approach a way to limit costs, mitigate the effects of security threats and potentially boost ROI.

STAYING ON TOP OF TECHNOLOGY CHANGE

A key concern among many business leaders -- those both in and out of security -- is the pace of change in IT. It can be difficult to know whether the organization is keeping pace with developments in cloud computing, AI, supply chains, data management and so forth. Each digital transformation initiative requires corresponding security measures; otherwise, new projects simply create new vulnerabilities. For these reasons, decision-makers need to consider cybersecurity as an element in larger digital transformation efforts.

Insurance. Another challenge CISOs and other executives face is ensuring that the business is well insured against cyberthreats. Cyber insurance is an essential protection, but knowing exactly which threats a policy covers and under which circumstances the insurer will pay a claim is no small challenge. As with most things

related to cybersecurity, the cyber insurance market changes continuously and swiftly. CISOs and other leaders need to stay current on the trends in cyber insurance.

Metrics. Savvy security groups are good at tracking metrics -- especially ones that demonstrate real value to the business. Key metrics and KPIs for cybersecurity include the following:

- Mean time to detect, which clocks how long it takes to realize an incident has occurred.
- Mean time to contain, which measures the amount of time necessary to limit a problem from growing.
- Mean time to resolve, which is the length of time needed to recover from a security incident.
- Intrusion or attack rate, which tallies attempted breaches and intrusions.
- Vulnerability escape rate, which counts vulnerabilities that go undetected during software development.

CISO FOR RENT

Finally, the expertise required for the CISO role isn't always readily available within an organization, and recruiting and retaining individuals for these positions is a challenge. Some businesses choose instead to outsource the job to specialists in the

field of CISO as a service. Another avenue an organization might consider is the use of a virtual CISO, or vCISO. Hiring a service to manage its security program provides a business with access to talent and resources that it might not otherwise be able to afford. As always with outsourcing, a business might worry about the effectiveness of the managed service and whether its specific needs are being well served.

More aggressively, an organization can hire a managed security service provider to handle entire segments of its security program. For some businesses, outsourcing security can deliver important benefits and efficiencies.

CYBERSECURITY BEST PRACTICES AND FRAMEWORKS FOR ENTERPRISES

The following are some best practices for cybersecurity teams to help ensure that their organization isn't victimized by cyberattacks:

- Erect multiple layers of defense.
- Secure the software supply chain.
- Isolate or air-gap backups.
- Test employees' security awareness.

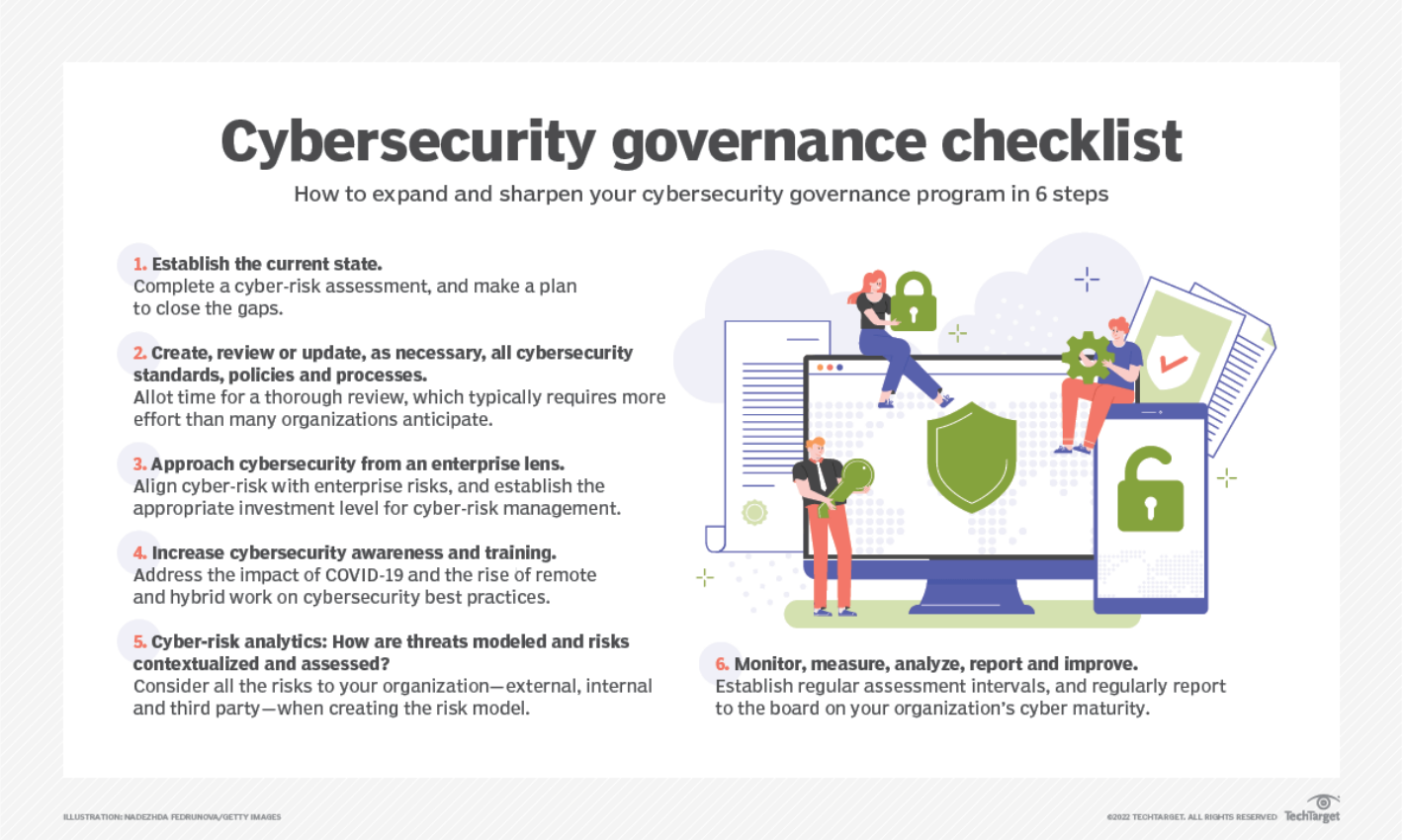
Security awareness programs won't be effective if they're done perfunctorily, such as a short presentation repeated annually. Cybersecurity training for employees should be engaging and updated regularly.

An ongoing security awareness program is also relevant in an era when so many employees work from home at least part of the time. Teams need to implement specific security practices for managing cybersecurity for remote workers to be sure data is handled safely, work isn't being done on inadequately secured hardware and networks, and remote and hybrid employees are not falling victim to AI-based attacks.

Another important element of a cybersecurity program is to have an incident response plan. When a cyberattack occurs, an organization won't have time to decide who should do what and how. A thorough -- and thoroughly tested -- incident response playbook will define key roles and responsibilities, and it should minimize the severity of a security incident.

A program for governing cybersecurity efforts also strengthens an organization's defenses. Effective cybersecurity governance helps ensure that everyone in the business is working toward common goals and adhering to the organization's security policies and procedures.

In this guide:



A well-conceived cybersecurity governance program also helps a business find and fix security weaknesses, manage risk effectively and meet its regulatory requirements.

The NIST Cybersecurity Framework 2.0, released in 2024, provides detailed resources and guidance for governance and planning.

The Mitre ATT&CK framework, a free knowledge base that documents threat actor behaviors and tactics, can also help security teams harden their defenses against attacks. Other security frameworks and standards, including those from ISO, might be applicable as well.

Programming is also an important component of the cybersecurity toolkit. Team members should understand the potential cybersecurity uses of key programming languages and learn the ones they need to know to do their jobs.

WHAT IS THE FUTURE OF ENTERPRISE CYBERSECURITY?

The effort required to secure an organization, its systems and its data must be sustained, as new challenges continue to arise.

Consider the trends shaping the future of cybersecurity:

- **Post-quantum cryptography.** Computational security forms the foundation of current cryptographical standards, relying on the knowledge that existing computers simply aren't powerful enough to break them. Quantum computing, however, will solve in minutes what would take traditional computing thousands of years. This monumental shift means that the adoption of quantum-resistant algorithms will become an essential cybersecurity task for CISOs and their teams in the next few years.

- **New views of identity management.** Where firewalls and physical locations were once viewed as the barriers between what was safe and what wasn't, identity is now considered the new perimeter. Many applications now run in the cloud, and workers are dispersed more than ever. Security teams will need to continue to adapt to this shift. Implementation of security features, such as single sign-on and privileged access management, gives organizations a firmer grip on who has access to specific applications, systems and data.
- **Continued improvements in response capabilities.** Organizations must be prepared to respond to large-scale incidents, such as ransomware attacks, so that there's a clear plan of action in place.
- **Recognizing supply chain security risks.** Discovered in 2020, the vast SolarWinds backdoor attack prompted the U.S. Securities and Exchange Commission (SEC) to pursue fraud and internal control failure charges against the software vendor and its CISO in 2023, although a federal judge dismissed some of the SEC's claims in 2024. The attack against government and enterprise networks illustrated the potential cybersecurity risks that supply chains pose. Given the increasing connectedness of businesses and their vendors and partners, these sorts of third-party risks are going to be a growing concern for enterprise security teams.

Increased adoption of secure access service edge technology -- better known by its acronym, SASE -- and a cybersecurity mesh architecture are emerging measures to help organizations further defend themselves against possible attacks.

In this guide:

Cybersecurity leaders should be aware that the next big cyberthreat might come not from a gang of cybercriminals but instead from nation-state threat actors. Whether motivated by espionage, economic disruption or ideology, these sorts of attackers have considerable resources behind them. Stopping these well-funded and well-equipped hackers is a significant challenge for the enterprise. Grappling with geopolitical risk factors might not fit neatly on a CISO's daily to-do list, but it is a threat worth watching.

Phil Sweeney is an industry editor and writer focused on information security topics.

Craig Stedman is an industry editor focused on analytics, data management and other technology areas.

CONTINUE READING

- **Top in-demand cybersecurity jobs**
- **Top enterprise cybersecurity challenges**
- **How to develop a cybersecurity strategy: Step-by-step guide**