# Top 10 CISO Tips

Conquer the challenges being faced by CISOs in today’s cybersecurity environment. Learn how to overcome them with mitigating strategies.

# Introduction

Chief Information Security Officers (CISOs) are a relatively new addition to the C-suite. When the role first came to prominence, CISOs' job duties were limited to the technical aspects of cybersecurity. Organizations subsequently grew to realize the importance of a CISO to ensure business continuity, a point that the COVID-19 pandemic hammered home. In the current version of this role, CISOs are now expected to possess business acumen along with security expertise.

As the CISO role continues to evolve, cyberattacks are increasing in frequency, intensity, and cost, and CISOs are feeling the pressure of being the organizations point to address these increasingly complex issues. A stunning 88% of CISOs report experiencing moderate to high stress levels[1].

This paper attempts to advise ways to relieve this stress by discussing the 10 most common challenges that today's CISOs face, along with mitigating strategies for overcoming them.

# Failure to Obtain Leadership Buy-In

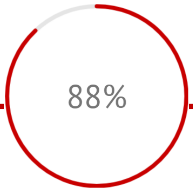
Executive buy-in is crucial to ensure the financial and human resources needed to keep your organization safe. You also need executive buy-in to cultivate a security culture of awareness throughout your organization. Without organizational awareness, buying the right technology is not a solution.

Two of the most common roadblocks to leadership buy-in are finances and a misplaced sense of invincibility, or "This can't happen to us." To overcome these obstacles, you must clearly define the organization's risk appetite and speak in terms that the C-suite understands.

It is helpful to translate risk into expenses and lost revenues. All organizations, regardless of size or industry, have sensitive digital assets that can be breached, and all organizations have business-critical systems that could be targeted for a ransomware attack. Explain how much a data breach or ransomware attack could potentially cost the organization, using real-life examples.

On the flip side, make sure you stress how security can help drive revenues and give the organization a competitive edge. An increasing number of businesses expect their vendors and partners to prove that they have adequate cybersecurity controls in place by meeting specific compliance standards, such as SOC 2.

It is  important to realize  that leadership buy-in is not a one-time event but an ongoing process that needs continuing reinforcement. After the initial project is approved and implemented, regular security assessments are highly recommended to understand and prioritize your organization's risks and vulnerabilities.



**Percent of CISOs report experiencing moderate to high stress levels.[1]**

[1] https://www.securitymagazine.com/articles/93710-mental-health-warning-in-cybersecurity-cisos-across-the-industry-reporting-high-levels-of-stress

## Balancing Operations with Cybersecurity & Compliance

To ensure leadership buy-in over the long term, cybersecurity must be a partner to the business, not an impediment. A CISO must balance organizational cybersecurity and compliance with industry and regulatory mandates, with external, and sometimes conflicting operational needs such as:

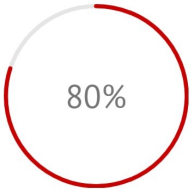
- **Dealing with requests for exceptions**
- **Identifying processes that may lead to regulatory compliance violations**
- **Minimizing Shadow IT**
- **Identifying rogue or malicious company insiders**
- **Preventing cybersecurity personnel from developing alert fatigue**
- **Facilitating workflows for employees who are not technologically savvy**

Regular security assessments and regulatory gap assessments are necessary to ensure that cybersecurity processes do not interfere with business operations and are effective, while a managed security information and event management (SIEM) system, paired with managed detection and response (MDR), will prevent internal security staff from developing alert fatigue.

## Not Having Insurance, or Relying on Insurance too Heavily

Cyber insurance policies, just like health, auto, and homeowners' policies, have coverage limitations and loopholes. For example, cyber policies generally do not cover breaches due to "employee negligence." This may sound reasonable, but some policies consider an employee clicking on a phishing link to be "negligence," and phishing attacks account for over 80% of security incidents.[2]

Additionally, no policy can cover all of an organization's losses after a cyberattack, especially indirect losses, such as the damage to the company's reputation. Nearly 40% of the average total cost of a data breach is due to lost business and includes customer turnover, lost revenue due to system downtime, and increased costs of acquiring new customers in the wake of a damaged company reputation.[3]



**Phishing attacks account for over 80% of security**

[2] https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html
[3] https://www.csoonline.com/article/3434601/what-is-the-cost-of-a-data-breach.html

That said, not having insurance at all is a high risk and potentially a very expensive approach. In 2020, the average cost of a data breach in the U.S. was $8.64 million[4]. Recovering some of that cost is far better than having no insurance to turn to. When shopping for a policy, hire a security consultant to closely review policy details, ensure that the coverage is adequate for your organization's threat profile and risk appetite, and avoid any "gotchas," such as excluding coverage for phishing attacks. Have the consultant review your policy annually, or whenever you make significant changes to your data environment, such as migrating from on-prem to the cloud or switching public cloud providers.

## Lacking Visibility Across the Entire Data Environment

If you don't know it exists, how can you secure it? Frequent supply chain cyber attacks, zero-day exploits such as those plaguing Microsoft Exchange, and the explosion of remote work post-pandemic illustrate the importance of having an accurate and complete inventory of all devices, users, and applications in your network. This is a basic requirement to understanding your data environment and is the first step in understanding your organization's threat profile.

Regular security assessments in combination with timely log and event monitoring will help you keep tabs on the users, applications, and devices connecting to your network, while regulatory gap assessments will identify how closely your organization is following industry standards and regulations, such as ISO 27001. A managed and monitored SIEM and MDR solution will defend against cyberattacks in near real-time.

## Lacking Clearly Defined Security Policy

If your employees do not know what is expected of them, how are they supposed to adhere to security best practices? In addition to providing employees with regular security awareness training, including phishing simulations, all organizations must have a written security policy with clearly defined rules.

**At a minimum, a security policy should include password security rules:**

- an acceptable use policy for email, internet browsing, and social media
- rules regarding access and control of proprietary data and client data
- rules regarding access to company data from remote locations or on personal devices
- and what to do in the event of a suspected security breach or data loss.

Most security policies cover much more territory, and depending on an organization's industry and compliance regulations, a security policy can be quite a complex document. Security policies require routine review and updating to reflect changes in the company's data environment and the cybersecurity threat environment. We recommend hiring a security consultant to help you craft an appropriate policy.

[4] https://insights.dice.com/2021/02/11/data-breach-costs-calculating-the-losses-for-security-and-it-pros/

## Lack of Employee Cybersecurity Training

A clearly defined security policy and employee cybersecurity training are like the head and the neck; one cannot function without the other. Often, an organization's biggest cybersecurity risk is its own people. All of the technological security defenses in the world will be of no use if an employee clicks on a phishing link. Conversely, a properly trained employee can be the organization's first line of defense against a cyberattack.

**Often, an organization's biggest cybersecurity risk is its own people.**

Employee cybersecurity training must be ongoing and include real-world exercises and tests, such as phishing simulations, which are critical to helping your employees avoid falling for social engineering schemes.  An outside security consultant can help you devise and implement appropriate cybersecurity training.

## Lacking an Incident Response & Disaster Recovery Plan

Unfortunately, the reality is that all organizations will eventually fall victim to a cyberattack. The question is not if, only when and how much impact did it have. At its simplest, an incident response and disaster recovery (IR/DR) plan is a set of instructions to help organizations detect, respond to, and recover from network security incidents, with an eye on minimizing damage, protecting data, and ensuring business continuity.

**The reality is that all organizations will eventually fall victim to a cyberattack. The question is not if, only when and how much impact did it have.**

Organizations such as NIST and SANS provide templates for developing IR/DR plans, including guidelines on responding to an active security incident. These templates are helpful starting points, but a real-world IR/DR plan will be far more comprehensive and actionable, assigning specific tasks to specific people at specific times.

Additionally, an IR/DR plan is useless without regular training drills to keep security personnel's skills sharp, iron out any kinks in the procedures, and ensure that the procedures are up to date. The cybersecurity threat environment is continuously in flux, so your IR/DR plan will need to be updated regularly to ensure that your team is ready to defend against new and emerging threats. Consider hiring a professional security consultant to help you develop and maintain your IR/DR plan.

## Difficulty Establishing Priorities with Conflicting Demands

A If everything is top priority, then nothing is urgent -- and nothing ends up getting done. All cybersecurity vulnerabilities and threats are not created equal, and prioritization is key for risk mitigation. A successful CISO understands how to prioritize projects and technology based on the risks and rewards they provide to the organization. Because security does not directly generate revenue, quantifying "rewards" means looking at factors such as whether a solution addresses prioritized risk areas, provides indirect returns by mitigating those risks, simplifies the organization's existing security, or enables the organization to meet its business objectives.

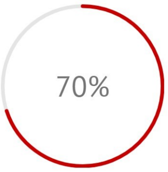
Regular security assessments and technology audits are necessary for CISOs to identify and prioritize areas of risk and propose security initiatives to mitigate these risks. A managed SIEM and log analysis provide additional information, including critical insights that might not show up during an assessment.

**Security Information and Event Management (SIEM)** centralizes data by collecting logs and events generated by host systems, security devices and applications on a single platform. These logs and events are then translated into actionable reports and alerts.

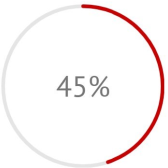
In addition to greatly simplifying an organization's security stack, a managed SIEM and MDR solution benefits the organization by freeing up internal IT and security personnel to work on projects that contribute directly to the organization's business goals.

## Difficulty Recruiting & Retaining Skilled Cybersecurity Staff

If your organization is having difficulty recruiting and retaining skilled cybersecurity personnel, you are not alone. Nearly three-quarters (70%) of cybersecurity professionals report that their organization is being impacted by the cybersecurity skills shortage, and 45% say that the situation is becoming worse.[5] Most organizations are unable to hire sufficient cybersecurity resources to devote to round-the-clock SIEM monitoring and threat management so an outsourced managed SIEM and MDR solution is a compelling necessity.



**Percent of cybersecurity professionals impacted by the cybersecurity skills shortage.**



**Cybersecurity Professions say that the situation is becoming worse.[5]**

Even if a CISO is fortunate enough to hire adequate staff, it is a best practice to periodically obtain the perspective of a third-party cybersecurity consultant. The consultant's analysis will support the CISO in internal discussions with management and budgetary decision-makers.

[5] https://www.csoonline.com/article/3571734/the-cybersecurity-skills-shortage-is-getting-worse.html

# Not Monitoring Security Alerts 24/7

It is generally not realized that SIEMs generate a large number of security alerts. According to Gartner:

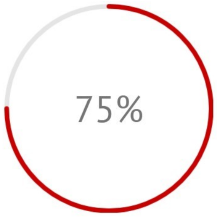
**A small SIEM deployment has up to 300 event sources, generates up to 1,500 events per second (EPS), and can store up to 800GB of data.**

**A mid-sized deployment has up to 800 event sources, generates up to 7,000 EPS, and can store up to 8 TB of data.**

**A very large deployment has thousands of event sources and may generate more than 25,000 EPS, with over 50 TB of data storage.**

SIEMs need to be monitored by skilled human security analysts 24/7 so that identified high-risk threats can be responded to immediately. Not surprisingly, the Ponemon Institute found that 75% of an organization's SIEM costs are spent on installation, maintenance, and staffing.[6]

Most organizations lack sufficient staff to devote to round-the-clock SIEM monitoring and threat management, In this case,  the SIEM is rendered all but useless other than for forensic historical data review after a network is breached. The majority of organizations need a managed SIEM and MDR solution backed up by a SOC staffed to provide immediate detection and response that can block cyberthreats in near real-time.



**Percent of SIEM costs spent on installation, maintenance, and staffing.[6]**

In the wake of the COVID-19 pandemic, organizational digital transformation efforts rapidly accelerated. Most business leaders now realize that cybersecurity is essential to the bottom line, but they are still unclear on what organizational cybersecurity looks like in practice. In addition to securing the organization's digital assets, CISOs are now expected to help leverage security technologies to further the organization's business goals. With the right technologies, processes, and partners, CISOs can overcome their most pressing challenges and implement a cybersecurity program that both protects the organization and aids in its growth.

[6] https://www.esecurityplanet.com/network-security/security-information-event-management-siem.html

SECNAP
NETWORK SECURITY

**Get a complimentary and customized consultation regarding your organization’s cybersecurity strategy.**

## About SECNAP Network Security

Since 2001, SECNAP Network Security has been combining human intelligence with innovative technology to protect organizations of all sizes against cyber threats, including data breaches, ransomware, phishing, and advanced persistent threats (APTs). Our proprietary, patented and patent pending CloudJacketX managed security-as-a-service platform addresses common pain points faced by IT teams, such as alert fatigue, challenges with meeting regulatory compliance requirements, lack of resources, and hidden vulnerabilities.

SECNAP’s proactive cybersecurity approach combines ongoing network security assessments with managed detection and response (MDR) services, an advanced SIEM solution, and a patented intrusion detection and prevention system (IDS/IPS) to provide multiple layers of detection and protection, which are monitored 24/7 by our U.S.-based security operations centers (SOCs). SECNAP utilizes proprietary security technologies that were developed in-house.

AICPA SOC aicpa.org/soc4so

GSA Advantage!

**844.638.7328 | SALES@SECNAP.COM | SECNAP.COM**