TEAM8™

A CISO'S GUIDE

Legal Risks and Liabilities

A handbook on what CISOs need to know before a chat with the General Counsel

By the Team8 CISO Village
in collaboration with SINET.

November 2022

WRITTEN BY

Legal and Security Content:

Mark D. Rasch

Computer Security and Privacy Lawyer
Kohrman, Jackson & Krantz

Security Content:

Gadi Evron

CISO-in-Residence
Team8

Editing & Proofreading:

Niv Lilien

The writers would like to thank members of the community (listed alphabetically): **Adam Zoller, Amir Zilberstein, Ariel Litvin, Bob Blakley, Caleb Sima, Charles Blauner, Chenxi Wang, David B. Cross, David Fairman, Jason Witty, Jerry Perullo, Liran Grinberg, ADM Michael S. Rogers, USN (ret), Mike Johnson, Nadav Zafrir, Nicole Darden Ford, Robert Rodriguez, Sounil Yu, Tim Callahan.**

The Team8 CISO Village is an exclusive community of CISOs from the world's leading enterprises. The primary focus of the Village is to facilitate collaboration among the world's most prominent companies with the goal of sharing information and ideas, conducting intimate discussions on industry and technology trends and needs, and generating value and business opportunities for all parties. By helping Team8 to identify real pain points and understand the requirements of large organizations, members of the Village are first in line to leverage solutions that are purpose-built by Team8's portfolio companies to support their needs.

To contact the Team8 CISO Village, please email **cisovillage@team8.vc**

DISCLAIMER: **These materials are provided for convenience only and may not be relied upon for any purpose. The contents of this document are not to be construed as legal or business advice; please consult your own attorney or business advisor for any such legal and business advice.**

This document is released under the Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) license.

WHY THIS GUIDE?

The recent criminal prosecution of Uber's former CSO, Joe Sullivan, served as a trigger for growing interest by CISOs in how they can protect themselves from legal risks and liability, both civil and criminal. For example, activities from governments and class action lawsuits are starting to name CISOs, and at times. [1, 2, 3, 4, 5]

Being a CISO is a tough job.

Not only are CISOs held responsible for the cyber security of the entire enterprise, but are often not given all the appropriate tools and resources to do their job effectively. Progress is often measured by what does not happen, and failure can be disastrous for the company — and for the CISO personally.

This document is a short guide on what a CISO needs to know to navigate the changing legal and regulatory landscape, with the growing personal risk and liability CISOs operate under in mind. That, with the clear understanding that the document is far from exhaustive, is meant to educate, and doesn't replace a conversation with the General Counsel and/or private counsel.

Further, please take into consideration that in writing this guide we limited ourselves to United States law only. We write with three main themes in mind:

- The contract and the employer vetting processes.
- The CISO role and responsibilities and the internal processes for engagement with stakeholders.
- Creating an environment of shared responsibility and accountability.

Before you take on a new role, you'll have either an offer letter, an employment agreement, or a contract. (Most CISOs don't have a contract). Regardless of the paperwork established before you start Day 1, there are several things to look into, have agreed, and/or out in writing.

This is the purpose of this document, to help you consider and agree to the very broad nuances you are taking on with your role as a CISO, as well as to serve as a reference you can use internally with your General Counsel and the board, as well as be the basis for discussion in the wider community.

CISOs used to be mainly IT and risk practitioners. They are now executives, and are expected to make the adjustment.

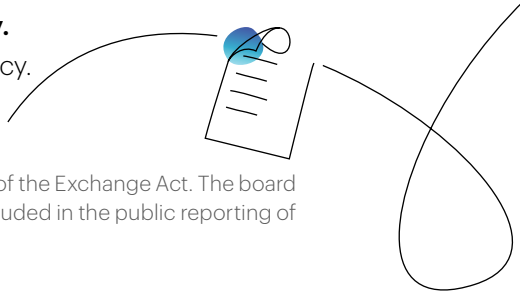
01

Contracts and Employment Agreements

What to look for?

As far as liability is concerned, the following should be considered by the CISO (in addition to the ability to be successful at their job and therefore avoid liability, to begin with), and is becoming best practice:

- Inclusion in the company's Directors and Officers (D&O) liability insurance (and named therein). But remember, D&O insurance does not cover criminal liability but may cover advancement of legal costs in criminal cases (if agreed to in advance). For example, the company will pay for an attorney to represent you if you are named in a lawsuit.
- While this is not yet best practice, there needs to be a board resolution to hire you as a CISO, or to be elected or appointed by the board or a senior management committee as the CISO, so that you can be named an Officer of the company (check!). Otherwise, the D&O coverage may not apply. Some employers may be resistant to the idea of naming the CISO an officer, and in that case, the language of the D&O should reflect your coverage and indemnification.
- Reasonable deductibles and exclusions (e.g. high deductibles could effectively invalidate the usefulness of a policy).
- Being indemnified by the company and its insurer for personal liability to the company (first party) or others (third party), is an often overlooked and important aspect for CISOs to protect themselves, on par with, if not more so than the D&O.
- **In the event of a criminal investigation and other legal needs** — either of the company or the CISO, make sure that the company provides **advancement** of legal fees associated with a criminal investigation, and that the CISO can retain their independent counsel. D&O doesn't cover criminal cases.
- The ability to engage with an outside (private) counsel for support with decision-making where you are interested in a second opinion prioritizing you, or would be otherwise placed in an unfavorable position by the General Counsel should be mentioned, and not blocked by NDA.
- CISOs should consider obtaining (or insisting that their employer provide) professional liability insurance — typically in the form of an Errors and Omissions (E&O) policy.
- There are other expenses that should be considered as well beyond coverage of legal fees, such as fines, damages, etc.
- As the CISO is often laid off following a data breach, consider negotiating:
  - Advance pay for twelve months (often referred to as a "Golden Parachute")
  - Acceleration of your stock options
- Then, **CISOs should consider purchasing their private umbrella policy.** Work with your insurance company, this can be treated like any other policy.



[1] Certain positions are specifically deemed an "officer" of the company, as stipulated by Section 16 of the Exchange Act. The board can pass a resolution to acknowledge an individual as a Section 16 Officer. These officers are included in the public reporting of the company, and the board oversees their successions.

02

Building the Right Processes

Perhaps the best protection a CISO may have is a strong and well-developed reporting strategy and a mature and well-defined process for doing their job.

PRO TIP

Understanding corporate challenges that can be used against you in a court of law, will protect the CISO more than many measures we discuss in this guide, especially as the process matures over time.

Integration and joint responsibility

Many organizations, particularly large organizations (and more specifically bureaucratic ones) have individual silos which may be strictly protective of their own authority. A CISO, by definition, has authority over data security, but in a way that crosses multiple business and functional units.

The CISO **must** provide input into various organization activities and be included in their strategy sessions.

Reporting and resolution structures:

- Legal must be kept in the loop as well as approve any public statements being made.
- Similarly, risk management and compliance **must** see what the CISO is doing — and understand why.
- Cross-functional committees and organizational structures need to be established, maintained, and rewarded.
- These functions have to include:
  - A dispute resolution process in a safe environment
  - An escalation processes

Similarly, make sure you undergo communications training. Understanding the boundaries within which you can operate is important, and that starts with what words mean, and how context affects that meaning.

Most importantly, an incident response playbook needs to be built with a clear definition of roles in what order should they be informed, and responsibilities, including all stakeholders in and outside of the CISO organization in what order should they be informed, and with a clear agreement on who can declare an incident a breach (usually, the General Counsel and/or an appointed Chief Privacy Officer — never the CISO). Then, a clear prioritization path for incidents as the General Counsel may choose to not review all of them it must all be documented.

PRO TIP

Consider removing the word "Breach" from the organization's taxonomy, reserving it for General Counsel declaration. Instead, use a structured process for "incident" definition and escalation. For example: event, issue, incident, crisis, and only then Breach.

PRO TIP

Working with incident response firms is an evolving practice with every data breach, and you should strive to stay up-to-date. For example, in recent years it is a growing best practice to engage with incident response providers through law firms. Your insurer is a great source of information you should consider tapping.

Further, set up a process with your various stakeholders to study and then create a table-top exercise following incidents as they happen in the enterprise, as well as outside incidents and how you can learn from them. These exercises are meant to test the process and decision making, not the technical capabilities of the team.

Conflict Resolution

A mature process must include a conflict resolution process, mentioned earlier briefly. The following are some ideas you should consider when building such a process.

- What should the CISO do if management does not want to report an incident that the CISO thinks should be — or must be — reported?
- What if this decision impacts public health or safety?
- What if the impact is imminent or could be considered reasonably so?
- What if a contract or other legal obligation imposes a duty on the CISO to take or refrain from some action that the company as an entity insists on not doing?

It is these kinds of conflicts that most often result in liability to the CISO. Even if that wasn't the case, the company needs a reporting structure and resolution process that can effectively deal with these issues as they come up.

The one way CISOs have faced and will face legal issues in the future, is when they make warranties, representations, or decisions based on bad information provided to them that they failed to validate themselves.

Trust, verify, and document

The four worst words a CISO can hear are “Oh, by the way.”

CISOs need to recognize that individuals and organizations may not only be unwilling to share bad news but may actively lie about or conceal it. This is especially true where someone’s bottom line, job, or career is at stake.

One way CISOs faced and will face legal issues in the future, is when they make warranties, representations, or decisions based on bad information provided to them that they failed to validate themselves.

Most commonly, these take the form of a CISO being told that a device, a share, or some other asset need not be secured because it is “not connected” or that it “has no personal data” on it.

Patches are deprioritized because the data on the devices is “not critical.” A variant of this is when a CISO is informed that the security of a device or share is not the company’s responsibility — as in, it belongs to a partner, affiliate, or cloud provider.

However, if the data is not protected, and worse, if it is compromised, it will be the CISO who is blamed. The best advice for a CISO here is trust, but verify.

PRO TIP

Some CISOs find it useful to involve a third party in the process. This provides external verification, as well as in the case of errors being made, possible risk transfer to the third party.

As we cannot validate everything ourselves, just as much as our regulators or our customers cannot validate everything themselves, we instead ask for an attestation. Similarly, we would be asking for an attestation from the other business leaders that when they say, for example, "there's no personal data" on a device, they are being held accountable to that statement if not true.

Some things to get in writing (which may just be an email) include:

- To whom does the CISO report? This refers both to the direct manager, and periodically, such as when presenting to higher management or the board.
- **How** does the CISO report (formal reporting, written reporting, informal discussions)?
- Who within the organization will be responsible for each of the following functions:
  - Security software and hardware acquisition
  - Testing and assurance
  - Training and awareness
  - Privacy and access control
  - Monitoring and response

Then, ask yourself: how do you account for potential negligence that you are not responsible for? It is important to document your communication with other departments. For example, if you've been trying to get IT to install a control based on a defined policy or standard, and they have not been implementing, are you negligent, or are they? Paper trail demonstrating your consistency and the actual status would prove invaluable.

PRO TIP

CISOs should consider how much to voice, and how you should improve that process over time. Regardless, both you and your team need to be aware all your communication is discoverable.

A seat at the table: The “business enabler”; Be ready to say "NO"

Being a business enabler is more than just a buzzword on CISO strategies, it will help protect you from liabilities. We will shortly touch on the topic, to build up for the essence of the matter - your readiness to say no.

"As a CISO, you will be most protected when you are aligned with the business objectives and needs of the business units." If you aren’t a business enabler, are perceived as an impediment to growth or the business strategy, or your answer to the various business units is often “No”, history has shown that the business units will find ways to circumvent your rules, and regulations, and to avoid the monitoring you have put in place.

PRO TIP

Try to say “how” instead of “no”.

When do you need to say “No”?

Be a business enabler, except for those times when you should say “No.” Have a pre-determined governance process to engage in conflict resolution, and that process should only be necessary where the business and the CISO disagree about the risk. Consider treating and documenting cases of consensus and agreement in a similar fashion.

When you explain that something the company is doing or plans to do is in violation of the law, a regulation, or puts the company, its employees (including the CISO), or its customers or partners outside of the company’s approved risk tolerance. Bank boards have to approve risk tolerance statements (a regulated requirement, and soon through this proposed SEC regulation draft may be required outside of banking as well).

A clear process on how to handle risk-based decisions should include who can accept or approve various levels of risk. An intern shouldn't be accepting potentially business-ending risks, on the other hand, it is perfectly reasonable for the head of engineering to accept risk in their world if the potential negative outcome is not company-ending. Having this documented in advance, before you need it, gives people a clear path when they want to proceed with something you think they should not.

This process provides risk transparency and does not leave you holding the proverbial bag. Elevate (informal) or escalate (formal) to your boss, to the GC, to Internal Audit, to the CEO, or to the board if needed. Be gracious, be humble, be bold, and be prepared for push back. This is the job, and this will protect you if you can show you brought transparency to the risk, the discussion around it, and the decision-making process.

PRO TIP

Be prepared for the eventuality that you will be uncomfortable with one or more risks that the business is taking. This is ok. It should be expected frequently. It's your responsibility to elevate the conversation to a higher level than just you.

Reporting Mechanisms

- Have a mechanism for anonymous reporting by employees or contractors to the CISO or compliance personnel, **and** by the CISO to management or the Board of Directors if necessary.
- Work with your legal team to understand applicable whistleblower laws and policies. And if someone "blows the whistle" — have an effective and documented process for addressing these in turn.
- The CISO needs to keep everyone in their reporting structure advised , to the level determined in the agreed-upon policies — typically in writing (in media backed up and monitored by the company) to document what has happened — even if this writing is cloaked in attorney-client privilege.
- If told, "you don't want to know..." something (e.g., "you don't want to know where we got this from...") that's when you do want to know. Inquire.
- Document the decision process and most importantly, who you contacted and when. This can be a note to yourself, and under some circumstances, to your personal lawyer.
- Even your physical notebook can be used as evidence in the legal discovery process.

A useful exercise

To begin, whether you are being hired as a CISO or are already the CISO, we'd recommend performing the following exercise.

Take a comprehensive information security standard such as the NIST Cybersecurity Framework (see the detailed spreadsheet, here), or the ISO 27001 series, and examine each requirement within the standard, and for each write:

- Who owns the governance of the control, and who owns the implementation of the control?
- Who is responsible for ensuring compliance with that requirement?
- Who has **input** into the methodology of compliance?
- Who has the authority to grant exceptions to the requirement, and how is the exception executed and documented?
- What organization/components are impacted by that requirement?
- What is the CISO's role in that requirement?

As a CISO, you will be most protected when you are aligned with the business objectives and needs of the business units.

Take, for example, the NIST Framework requirement ID.RA-4: "Potential business impacts and likelihoods are identified." While a CISO can determine what computer systems and networks are impacted by disruptions, malware, or failures, the BUSINESS impacts must be determined by the business units.

- What data is critical?
- What will be the impact on:
  - Availability?
  - Confidentiality?
  - Integrity?
  - Reputation?
  - Business operations?
  - Regulatory compliance?

This process helps point out where the accountabilities and responsibilities (which are not the same) for cyber security lie. While in the end, the CISO is responsible for the governance of cyber security, the execution is the responsibility of the entire enterprise, and to be effective, accountability and responsibility need to be shared.

PRO TIP

When speaking with CISOs who kept their job following a breach, they often presented on risks in advance, as part of a wider security program plan approved by the board. Sometimes, with the the help of a third party, and at times, audited after the fact.

Consider a personal lawyer

There may be times when the advice given by corporate counsel, or direction offered by management makes you uncomfortable or queasy. If the CISO believes that these decisions are wrong — or more significantly, unlawful, they can and should appropriately consult with knowledgeable outside counsel (typically at their own expense) to guide their personal actions. Further, you should consider engaging with a private attorney on daily decisions. Following data breaches, it is becoming a best practice for the company to cover the associated costs.

PRO TIP

A proposed SEC regulation draft suggests corporate boards develop expertise in the cyber security space, and many companies are adding a security expert to the board. It is recommended that boards develop cyber expertise across their Board through education and the identification or appointment of a Director with experience managing cyber risk

---

NDAs or other agreements may limit what can be said to outside counsel — but the CISO should look at outside (personal) counsel as an extension of themselves, and as mentioned earlier consider this point in contract negotiations.

Data protection and the role of the CISO

One way that CISO's face legal challenges — or the companies for which they work do — is a failure to adequately protect the personal data they collect. While we typically think of data breaches, the CISO must consider all misuse of information.

For example, credit reporting agency Experian recently used the data it collects commercially to learn whether or not any of its remote employees were working more than one job in violation of policy — and fired them. Effectively, they were spying on their employees.

- The CISO must seek accurate advice (based on accurate information) about whether these data uses are appropriate. Even simple acts like recording conversations (including digital conversations) may give rise to civil or criminal exposure to the company and the CISO.
- The CISO needs to know what data are collecting and should work hand in glove with the privacy and legal departments.

Dealing with Fraud

While most CISOs do not have a responsibility for fraud, electronic processes which are secured by the CISO are responsible for financial management, reporting, payroll, invoices, etc. Often, those committing internal or external fraud must alter permissions or processes to facilitate the fraud. This fraud may be committed by insiders – up to and including senior management.

While the Sarbanes-Oxley (SOX) law does not apply directly to CISOs, it does require effective controls on financial reporting which may come into the domain of the CISO. In many such cases, the "fraudster" is actively attempting to circumvent these controls. In some cases, the persons seeking to circumvent the controls are senior management. Again, documentation, communication, and diligence are key – as are alternative reporting structures.

Implementing alternative reporting structures

Continuing our discussion of effective reporting structure to legal, compliance, and the CEO, a CISO should consider what happens when a conflict of interest arises in the reporting channel. In such a case, the CISO should be able to take advantage of an alternative reporting structure. They should have a protected channel (both technically and legally) to report their concerns (and the data upon which it is based) to the Board of Directors, to outside advisors.

If their concerns are not addressed or are ignored (or, frankly, if they are wrong) then the CISO's tenure is likely limited. But having the ability to escalate concerns like this is critical. Ultimately, the company (including the CISO) must comply with law or regulation, and the CISO must be prepared to resign if they firmly believe that the company is not doing so.

03

Employer Vetting and the Hiring Process

The first step for a prospective CISO is to determine whether the new proposed employer is a good fit for the personality, traits, experience, and skills of the CISO, followed closely by how seriously the organization treats the topic and prioritizes cyber security.

Know thyself

- Are you a strong detail-oriented person with a rigid adherence to process, or more of a freewheeling "people person" who makes connections with the heads of other departments?
- Do you wait for problems to come to you or do you actively seek them out?
- Do you operate in your own fiefdom, or are you a or do you prefer a more collaborative culture?
- Do you prefer to work alone or collaboratively?
- Do you adapt well to new circumstances and can act under the limitations of ambiguity, or do you prefer a more settled and conservative environment?
- Are you more inspired by deep technical innovations or by policy changes?
- Do you thrive within high-risk environments, or do you prefer a more risk averse environment?
- Are you highly technical or policy-oriented?
- Do you communicate better with engineers, lawyers, or business units?
- Are you internally facing or externally facing?
- Are you used to managing a staff of three? Thirty? Three Hundred?
- Do you delegate or do you take personal responsibility?

It's not that one style is better or worse than another, but challenges that could lead to legal issues often stem from style clashes with either the culture of the enterprise, or your skill set, or what is expected of you. And, indeed, what is expected of you by whom, who you report to any degree, and the various stakeholders you work with.

In many respects, the first thing to do is to look into the corporate culture and personality and make sure the fit is there!

The reporting structure and commitment to success

There is no one perfect reporting structure, and none of these should be a dealbreaker unless the reporting structure is inimical to your goals and expectations. In that case, you are setting yourself and your company up for failure. Depending on the sector, the CISO is increasingly moving out from under the CIO/CTO or IT. This is to protect the tech executive from having to give up security for the sake of production as much as giving the CISO the authority needed to manage risk outside of just technology risk.

Questions to ask here include:

Are you a strong detail-oriented person with a rigid adherence to process, or more of a freewheeling "people person" who makes connections with the heads of other departments?

- Is the CISO, in fact, an employee, Officer, or Director of the Company?
- What function does the CISO report to? Two examples are the CIO and the CEO. There is not always a perfect fit that is the same in all global companies, as every organization is different.

Consider:

› As a person, do you prefer technical solutions? Do you find yourself most comfortable designing how technical solutions will work? IT may be for you.

› If business metrics rather than technical ones will be your department's measure of success, i.e. rather than "mean time to patch", "decrease in phishing success" or degree of deployment of cloud solutions, you may be, at the most extreme, measured by profits obtained. Reporting to the CEO would then make a lot of sense.

› There are many other reporting structures, such as to the CFO, CLO, and CRO, but having the right hierarchy to support your role, which is a good fit for you, should help build good relationships and processes for success, especially during a crisis.

How the CISO is seen:

- Is the CISO seen as a "loss prevention" measure? Then you may only get the minimum resources needed to prevent breaches.
- As part of the "compliance team"? Then you may only get what's strictly necessary to comply with some regulation and no more.
- As a business enabler not limited to technical input? You will likely have the influence needed to manage risk.

Alternative reporting structures considerations:

CISOs may alternatively report to the risk, legal, IT, security, compliance, finance, or privacy departments, or vice versa, they may be reporting to the CISO. In addition to mere reporting, know who has authority, veto power, budgeting and staffing, and the ear of those in power. An optimal reporting structure is one where the CISO has adequate independence to make binding decisions and escalate concerns to the most senior governance structure in the company (i.e. board, executive committee, etc.).

PRO TIP

Actively query and request attestation of the support level the organization would lend you if, for example, if you cannot get D&O insurance, you could communicate with the CEO if the company will be responsible, for example, if you are named in a class action lawsuit, fined by the SEC, etc.

CONCLUSION

The best way to avoid personal legal risk is, of course, to conform to the law and regulations. But that is easier said than done when some laws mandate what other laws prohibit. Employing best practices and establishing clear and agreed-upon processes, engaging with multiple stakeholders, can also minimize the risk of a civil action suit, and can protect you if you or your organization are being sued, and even help if you face criminal charges.

A smart CISO should seek counsel (both advice and legal counsel) from many stakeholders within the framework of a documented process. A trail of documentation will prove immensely useful if conflicts arise and should be considered best practice regardless. Documenting the assertions and assumptions that lead to an exception in policy is paramount.

To leave you with a final thought, do remember the relationship between the CISO and the company is reciprocal, and the CISO also has a responsibility to their employer to build their own experience and provide value in multiple areas.

And don't forget, you have a tribe - a community of CISOs who have likely been through what you're experiencing. Reach out.