Gartner
Peer Community

How are U.S. CISOs Addressing Liability Risk?

New regulations taking effect in the U.S. mean that cybersecurity leaders could face legal liability in the event of an incident. What strategies are they using to protect themselves?

Most have completed training on legal liability related to cybersecurity incidents, with some doing so on a regular basis

Clear incident response documentation is the most common strategy used by respondents to mitigate liability risk

Leaders consider available liability protections to be an important factor when deciding on new roles

Data collection: Oct 13 - Dec 4, 2023

Respondents: 100 U.S. information security leaders and IT leaders who own responsibility for their organization's cybersecurity program

About Gartner Peer Community One-Minute Insights:

Gartner Peer Community is for technology and business leaders to engage in discussions with peers and share knowledge in real time.

Surveys are designed by Gartner Peer Community editors and appear on the Gartner Peer Community platform. Once the respondent threshold is met, survey results are summarized in a One-Minute Insight.

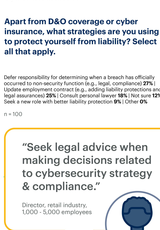
The results of this summary are representative of the respondents that participated in the survey. It is not market representative.

1 Minute Insights

The majority of leaders have completed legal training on liability

Over half (**58%**) of all respondents (n = 100) have **completed training on legal liability for cybersecurity incidents**, but one-fifth (20%) say such training is unavailable in their current role.

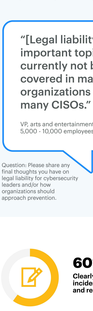
In your current role, have you completed any legal training that addresses liability related to cybersecurity incidents?



Other **0%**

n = 42

Note: May not add up to 100% due to rounding



n = 100

"Personal liability is something [our] Info Security team is very conscientious about."

VP, construction industry, 10,000+ employees

Among surveyed leaders who have not yet completed legal training on liability (n = 42), **58%** intend to seek it out over the next 12 months.

Do you plan to pursue legal training that addresses liability related to cybersecurity incidents in the next 12 months (either independently or through your employer)?[1]

"[Legal liability is a] very important topic that [is] currently not being covered in many organizations and for many CISOs."

VP, arts and entertainment industry, 5,000 - 10,000 employees

Question: Please share any final thoughts you have on legal liability for cybersecurity leaders and/or how organizations should approach prevention.

Most leaders use incident response documentation to mitigate liability risk

60% of all respondents (n = 100) are **clearly documenting incident response roles and responsibilities** to protect themselves from liability risk. 40% are updating their existing cyber insurance.

Apart from D&O coverage or cyber insurance, what strategies are you using to protect yourself from liability? Select all that apply.

Defer responsibility for determining when a breach has officially occurred to non-security function (e.g., legal, compliance) **27%** | Update employment contract (e.g., adding liability protections and/or legal assurances) **25%** | Consult personal lawyer **18%** | Not sure **12%** | Seek a new role with better liability protection **9%** | Other **0%**

n = 100

"Seek legal advice when making decisions related to cybersecurity strategy & compliance."

Director, retail industry, 1,000 - 5,000 employees

"I wish there was a guidance doc on what CISOs need to have in place as well as contracts to protect from personal liability."

C-suite, construction industry, 1,000 - 5,000 employees

Question: Please share any final thoughts you have on legal liability for cybersecurity leaders and/or how organizations should approach prevention.

Liability protection a key factor when considering new cyber leadership roles

Nearly all (97%) consider available liability protections when deciding whether to take on a cybersecurity leadership role, with over one-third (36%) citing it as a very important factor in their decision.

When seeking a new role in cybersecurity leadership, do you consider available liability protections to be an important factor in your decision?

"The legal landscape on this seems to be evolving and the liability risk to CISOs is increasing, [so] going forward, I will require liability coverage from any new employer rather than ask for it later."

C-suite, manufacturing industry, 1,000 - 5,000 employees

Question: Please share any final thoughts you have on legal liability for cybersecurity leaders and/or how organizations should approach prevention.

In their own words...

"This is an emerging area of concern for CISOs and I'm certainly going to look into this."

- C-suite, finance industry, 1,000 - 5,000 employees

"Far too often the CISO is protected but the downstream [senior] management is not. This results in a lot of verifying next steps with the CISO that should be automatic but leave you holding the ball if you don't."

- C-suite, professional services industry, 1,000 - 5,000 employees

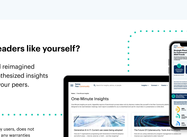
"I think most organizations will have to carry liability insurance in order to recruit future leaders."

- Director, healthcare industry, 10,000+ employees

"The legal risk exposure continues to expand."

- C-suite, professional services industry, 5,000 - 10,000 employees

Question: Please share any final thoughts you have on legal liability for cybersecurity leaders and/or how organizations should approach prevention.



Respondent Breakdown

Region

Job Level

Company Size

Respondents: 100 U.S. information security leaders and IT leaders who own responsibility for their organization's cybersecurity program

Want more insights like this from leaders like yourself?

Click here to explore the revamped, retooled and reimagined Gartner Peer Community. You'll get access to synthesized insights and engaging discussions from a community of your peers.

Gartner

Source: Gartner Peer Community, Cybersecurity liability risks: Protecting the CISO survey

[1] Question shown only to respondents who answered "No, but training is available to me", "No, training is not available to me" or "No, and I'm not sure if training is available" to "In your current role, have you completed any legal training that addresses liability related to cybersecurity incidents?"