Issues in Information Systems
Volume 27, Issue 4, pp. 624-632, 2026

DOI: https://doi.org/10.48009/4_iis_2026_150

Who supports director and officer insurance for chief information security officers?

Christopher Scalise, *Robert Morris University, cs.scalise13@gmail.com*

Abstract

This study compares cybersecurity professionals to non-cybersecurity leaders and their support to provide director and officer insurance to chief information security officers (CISOs). Director and officer (D&O) insurance is a type of personal liability insurance often offered to an organization's top executives. In this study, I analyzed whether there were similarities in support between the two groups. To accomplish this analysis, I developed a survey to examine each relationship through the lenses of cybersecurity professionals and non-cybersecurity leaders. The questions were carefully curated using the Likert scale to assess the extent to which they support the CISOs receiving D&O insurance. A Mann-Whitney U test was performed using two groups, cybersecurity professionals and non-cybersecurity professional leaders, to determine whether there was a significant difference between the two groups. This study helped identify if there is an alignment in support between cybersecurity professionals and non-cybersecurity professional leaders. The knowledge gained from this study helps set the stage for CISOs to have supporting documentation for organizations that don't offer D&O insurance to the CISO. Based on my search for scholarly articles for the literature review, there is a severe lack of scholarly studies on CISOs and how liability affects their job and the strength of cybersecurity programs. My hope is that this can begin to build scholarly research on an important title, the CISO, which is still considered fairly new in organizations.

Keywords: D&O Insurance, Director and Officer Insurance, executive personal liability, CISO liability, CISO retention, CISO recruitment

Introduction

I have over 28 years of experience in information technology and information security as of 2026. I observed that as they delved deeper into cybersecurity, the risks cybersecurity professionals were taking increased. If the cybersecurity leader does not have personal liability insurance, they may be personally sued. The lack of personal liability insurance could cause them to lose their home, their retirement, and even face jail time. To protect CISOs from personal liability lawsuits, I argue that CISOs should be included in their organizations' D&O insurance policies. A survey conducted at the RSA Conference (RSAC) found that many large companies are providing D&O insurance to their CISOs (Leyden, 2026). Still, as the size of the company shrinks, this rate drops drastically: at Fortune 1000 organizations, it's 88%; at organizations with 500+ employees, it's 53% (Leyden, 2025). This research may help give CISOs confidence to at least start the conversation within their organization if they are not offered D&O insurance. Although the research found a statistical difference between the two groups, the box plot and further analysis using Cohen’s guidelines show that non-cybersecurity leaders who help decide who gets D&O insurance are approaching the same level of support for D&O insurance as cybersecurity professionals.

Background

CISOs are risking their reputation, their career, and their livelihood every day. Even if a CISO believes they met all their requirements, they could still be accused, just as with any other wrongdoing or crime. The difference is that they could be held personally liable if they don't have D&O insurance, even if the wrongdoing is not true. As a cybersecurity professional, I have serious concerns here because it is up to a judge, or a judge and jury, to determine whether a CISO with years of experience and training is guilty or not guilty. There is also some incentive to accuse a CISO. Under the False Claims Act (Department of Justice (DOJ), 2025), a whistleblower is entitled to a portion of the settlement if a CISO is charged and found guilty of a regulatory failure. Again, even if they met their requirements, the claim they didn't can still be made, and it is up to the CISO's personal lawyer or their organization's lawyers to defend the CISO, creating undue stress and attention. The Securities and Exchange Commission (SEC) (2023) filed charges against Timothy G. Brown, the CISO of SolarWinds, for fraud and internal control failure. On November 20th, 2025, the SEC (2025) dismissed all charges with prejudice. Uber's Chief Security Officer (CSO), Joseph Sullivan, who covered up a security breach by paying a bounty hunter (DOJ, 2022; IANS Faculty, 2023), received three years' probation and 200 hours of community service (IANS Faculty, 2023). Sullivan was convicted of obstruction of the Federal Trade Commission (FTC) and misprision of a felony. These examples show how one case was dismissed, and another ended in a conviction.

Literature Review

Introduction

There is a shortage of cybersecurity professionals, and the need continues to grow; as this need increases, the CISO role becomes even more crucial than ever (Aspen Digital, 2023). Aligning cybersecurity with business functions is the CISO's key responsibility (Aspen Digital, 2023). This involves working with senior leadership to align strategy, decision-making, risk management, governance, and procurement (Aspen Digital, 2023). According to American International Group, Inc. (2025) and Gartner (2024), most CISOs are not covered by D&O insurance the same way other high-level executives are. CISOs without D&O insurance face no personal liability protection and could be ordered to pay restitution, face imprisonment, be fined, or all of the above.

This CISO is responsible for ensuring that cybersecurity and business functions align. Overseeing cybersecurity can be a significant source of anxiety due to stress and risky responsibility. As compliance and regulations increase and expand the role of CISOs, it was found that the retention of a CISO was 1 to 2 years, and that 88 out of every 100 CISOs were overly stressed (Nobles, 2022). Organizations use benefits to improve "retention and attraction, employee well-being, organizational citizenship behaviors, and task performance" (Werner & Balkin, 2021). However, you must have upper management's support to use this strategy to improve CISOs' working conditions. D&O insurance could be a benefit for organizations to support CISO retention, attraction, and work-life balance.

Why Firms Purchase D&O Insurance

The longevity of an organization can be affected by many factors (Jiang et al., 2022). Part of that longevity requires the board of directors and officers to remain for a significant period of time. D&O insurance is available to these senior executives because their decisions often entail risk, including litigation, compliance, and share price risks. If good-faith attempts fail, they should not be held personally responsible when significant economic policy uncertainty (EPU) is part of the decision-making process. EPUs are often beyond senior leadership's control and are not always specific to a single nation. President Trump's 2025 tariff policies, which included reciprocal tariffs on other countries, are a specific example of how EPUs

could affect an organization over which senior leadership had no control. An intangible issue that has surfaced in 2025 is the political landscape, which is causing tension between managers and investors. This tension is another driving force behind senior executives' purchase of D&O insurance. This effective risk mitigation tool is used not only in the United States but globally.

D&O insurance – Good or Bad?

A 2022 study found that organizations with D&O insurance took on higher-risk investments and invested more amid economic uncertainty than those without D&O insurance (Jiang et al., 2022). Often, with high risk come high rewards, so the question remains: Does this also protect investors by allowing senior leaders to take on higher risk without worrying about lawsuits that could cause even greater loss of revenue and time for an organization?

Donelson et al. (2022) conducted a study to determine whether D&O insurance affected settlement amounts, examining class action lawsuits with and without a lead plaintiff, and those involving accounting violations and those without. It was determined that settlements were consistent, and no determination was made regarding whether an organization had D&O insurance, leading to the conclusion that D&O insurance was not purchased to commit fraud or deceive investors.

Another study by Egger et al. (2015) examined the hypothesis that D&O insurance protected against mismanagement, enabling them to take risks without considering the consequences. 232 companies were analyzed from 1996 to 2008, and it was found that coverage increased or decreased with volatility; however, the null hypothesis was accepted. The study concluded that D&O insurance did not create a moral hazard requiring additional regulation and that other areas should be investigated to explain why markets collapse.

Breadth of a CISO

From the establishment of the CISO role to 2025, the CISO role has been viewed as a technical security advisement role to the C-suite (Aspen Digital, 2023). However, the CISO role has slowly evolved, and it is no longer just about reporting on vulnerabilities and patching assessments; it is now an expert on business risk, a role that in the past was left to the board and the C-suite. This was due to the significant increase in the number of threat actors, regulations, and new laws. However, many CISOs still lack the authority with their increased responsibilities. This is because many of the leaders on those boards and the executive team have a limited understanding of the CISO role, which creates barriers to the person in the role's success. According to Aspen Digital (2023), the way to break this trend is to include them in senior-level discussions on strategy, governance, and risk management. Another area where many organizations are not including CISOs, which is now considered best practice, is ensuring they are involved in product and procurement decisions and have access to senior leadership regardless of reporting structure. In summary, CISOs need to be woven into the fabric of leadership and leadership committees to ensure their guidance informs executive-level decisions on strategy, governance, and risk management.

Regulatory Recognition of the CISO Role

An article by Blosfield (2017) announced a significant milestone for the CISO role. The New York State Department of Financial Services passed a new regulation requiring all members of New York's insurance industry to appoint a CISO. This was the first time a regulatory requirement in an industry mandated the assignment of a CISO. This requirement was intended to ensure that the board of directors and senior officers are informed and that regulations are followed. It is expected that this new regulation will lead to a significant increase in cybersecurity-related questions when applying for D&O insurance, prompting more CISOs to be included in the policy.

CISOs Not a Priority for D&O Insurance

Uber experienced a breach in 2016 that leaked 57 million email addresses and phone numbers, as well as 600,000 driver's license numbers (Brumfield, 2022). John Doughs and Brandon Glover, the two threat actors who compromised Uber's internal system, requested $100,000 to delete the stolen data. Uber agreed to pay if the threat actors sign a non-disclosure agreement (NDA) (Brumfield, 2022). Joe Sullivan then classified the $100,000 as a bug bounty rather than disclose it to the public or regulators. In 2017, when a new CEO came on board, he discovered what Joe Sullivan had done, fired him, and reported the data loss (Brumfield, 2022). Joe Sullivan faced charges of obstruction of justice and failure to report a crime. Despite this, there was no uptick in D&O insurance due to Sullivan's charges, as the charges were seen as a clear moral violation, and companies were already dealing with a 74% increase in cyber insurance premiums (Brumfield, 2022). Joe Sullivan lost the case and, on May 4th, 2023, was fined $50,000 and was forced to serve three years of probation (Stupp, 2023). Rather than having anything to do with D&O insurance, this was more about ethics.

Liability Worries for CISOs

Effective in 2023, the Securities and Exchange Commission (SEC) adopted a new rule requiring organizations to report a cybersecurity incident to the SEC within 4 business days and include it in their public filings (Jones, 2023). Two studies led to the SEC's decision to adopt this new rule. One presented by Sen. Gary Peters in 2022 showed that 75% of ransomware attacks went unreported. Second, a 2022 Gartner Report found that 43% of organizations did not report a ransomware attack to the SEC. Jones stated that, due to this ruling, many CISOs were demanding D&O insurance if their names appeared in SEC financial reports. Jones also referenced a Proofpoint report stating that 60% of CISOs fear personal liability.

In 2020, another CISO the SEC sued was Tim Brown of SolarWinds (Nash, 2023). These charges differed from Joe Sullivan's because there wasn't clear, purposeful wrongdoing. The SEC claimed that SolarWinds did not disclose the full extent of the vulnerabilities. Since vulnerabilities occur all the time and a fix has to be developed and tested, the wrongdoing was less clear-cut than what happened with Joe Sullivan. Following the SEC's actions against Tim Brown and SolarWinds, there was a significant increase in requests for D&O insurance.

Another high-risk issue CISOs had to deal with, which raised concerns, was the all-remote workforce during the COVID-19 pandemic (Jackson, 2023). Jackson (2023) referenced a Proofpoint study that found that during the pandemic, the percentage of CISOs who felt they would experience an attack in the next 12 months was 64%, then fell to 48% in 2022. However, due to the number of ransomware attacks in 2022, this figure in the Proofpoint report jumped back up to 68% in 2023's report. Due to the teetering economy, many security budgets were strained, and the Proofpoint report Jackson referenced shows 60% of CISOs were experiencing burnout and 61% felt their jobs were unreasonable. D&O insurance could be a first step toward balancing some of the risks CISOs face.

Contribution

The literature review provided insight into how CISOs feel and what concerns them regarding personal liability. I compared cybersecurity professionals with non-cybersecurity decision-makers, such as executives and board members, and analyzed their support for D&O insurance for CISOs. Are cybersecurity professionals not being heard because they aren't talking it to the right people, or because they're holding it in and only complaining outside of work? My hopes are that this report would help CISOs feel more confident approaching their internal leadership for an open discussion about D&O insurance.

Research Question

The research question for this study was, "Is the support to provide D&O insurance to CISOs equivalent for the two groups, cybersecurity professionals, and non-cybersecurity executives?"

Methodology

A quantitative research design was used to determine whether cybersecurity professionals and non-cybersecurity decision-makers provide the same level of support for CISOs in obtaining D&O Insurance. First, the participants were split into two independent groups based on their answers: one group of cybersecurity professionals and another of non-cybersecurity decision-makers. Second, they were asked how strongly they support CISOs receiving D&O insurance, on a scale of 1 to 100. I then converted these to a 1-to-10 scale, allowing for more granular responses and yielding stronger data not constrained by a simple 1-to-10 scale. For example, if a user selected 97, it would have been converted to 9.7 prior to the analysis. I then ran a Mann-Whitney U Test to determine whether there was a significant difference between the two groups. I ran a nonparametric test using Mann-Whitney U because the results were ordinal, the non-cybersecurity professional results were highly skewed, and there were influential outliers. Second, I created a box plot to assess how close the means of cybersecurity and non-cybersecurity professionals are and to represent outliers through the whiskers.

Population and Sample

The study population comprised executives, board members, cybersecurity professionals, CISOs, and aspiring CISOs with 2025 or earlier experience. The data was initially collected from LinkedIn and conferences; however, the number of respondents was low. I then shifted direction due to a lack of responses, and additional data were collected using SurveyMonkey and Cloud Research, targeting cybersecurity professionals, executives, and business owners. A survey was chosen to reach a larger pool of respondents.

Results

As shown in Table 1, I collected 143 Non-cyber professional respondents and 277 cyber professional respondents. I ran a Mann-Whitney U test, and the results are shown in Table 2. The *p*-value for the test was <0.001, indicating that the null hypothesis was rejected, and I conclude that there is a significant difference between the two groups in their support for CISOs having D&O insurance.

Table 1. Descriptives of Survey

	N	Mean Rank	Sum of Ranks
Non-Cyber Professional	143	179.64	25688.5
Cyber Professional	277	226.43	62721.5
Total	420		

Table 2. Mann-Whitney U Test

	D&O Support for CISOs
Mann-Whitney U	15392.5
Wilcoxon W	25688.5

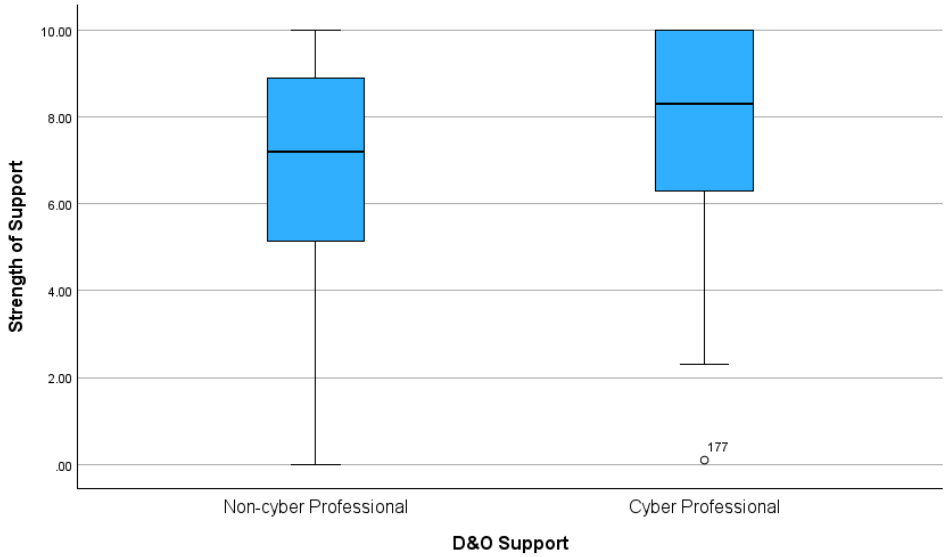
Z	-3.769
Asymp. Sig. (2-tailed)	<0.001

Discussion of Findings

Interpreting the detailed results provides further insight into why the *test's p*-value was <0.001. First, the sum of ranks for cyber professionals was more than twice that of non-cyber professionals, indicating that cyber professionals scored higher on support for CISOs receiving D&O insurance. The mean rank for non-cyber professionals was 179.64, while that for cyber professionals was 226.43. Both findings suggested a significant difference between the two groups. Lastly, the absolute value of Z exceeds 1.96, which corresponded to a statistically significant result ($p < .001$).

I next created a simple boxplot to visually assess how close the two groups were in their support, despite the significant difference. The boxplot under Chart 1 shows a couple of key points. One, the non-cybersecurity professional plot has a wide range of support responses that are significant enough to be more than outliers. Two, the means of the two independent groups are within two points of each other. Three, Chart 1 shows that cybersecurity professionals don't show low support as often as non-cybersecurity professionals. Despite Chart 1 emphasizing a significant difference between the groups, it also clearly shows that the trend among non-cybersecurity leaders is shifting toward supporting D&O insurance for CISOs.

Chart 1. Simple Boxplot



The simple boxplot interpretations help explain why the groups were different when running the Mann–Whitney U test. This can be explained by looking at the whiskers of the simple boxplots. As you can see in Chart 1 above, the whiskers for the non-cyber professional extend to zero, whereas those for the cyber professional do not. This skews the mean for the non-cyber professionals, and without these low whisker values, the mean would have moved up, possibly leading to an inability to reject the null hypothesis. The most likely reason for this is that some non-cybersecurity leaders still maintain a strong stance that CISOs should not be provided with D&O insurance, which has a significant effect on the mean, as evidenced by

the p-value <0.001. This issue is discussed in the next two sections: implications of the research and limitations.

Implications of Research

If one were to focus only on the Mann-Whitney U test, it is clear that a significant difference remains between the two groups, and one might conclude the research here. However, after comparing the groups with a box plot, it became evident that the difference between the two groups may be less significant when viewed through a different lens. This research would benefit from being a much larger study that incorporates industry and organizational size. For example, if a large number of small businesses responded to the survey, it could negatively affect the results, as small businesses are unlikely to have a CISO. Manufacturing is an industry that also often won't have a CISO. This is often because they are small, but even a medium-sized manufacturer may not have a CISO. These comments are based on my experience; the expanded study could either prove or disprove my hypothesis, which is exactly why it should be done. The CISO, as noted in the literature review, is a relatively new role in businesses and could benefit from further research to guide job hunters and organizations in planning CISO compensation packages.

Limitations

This study had multiple limitations. Because I didn't use the pre-screened services offered by Cloud Research, some respondents' results may not be suitable for inclusion. For example, if a hair salon's business owner answered the questions, technically, they are a business owner, but would they ever have a CISO? More than likely, no. If startups were answering the questions because they are doing anything they can to make extra money, would they have a CISO? Probably not. There would also be bias between groups. In other words, a cybersecurity professional will see this as a benefit and have a bias toward D&O insurance, whereas a non-cybersecurity leader will see it as an expense and have a bias against providing it without significant evidence of its benefit to the business as a whole. This study would benefit from a mixed-methods approach, allowing interviews to capture nuances that cannot be captured by a survey study such as this. This would allow for the identification of biases or additional data points that constitute legitimate business concerns and should be considered when determining whether D&O insurance should be offered. As previously mentioned, this research could benefit from a much larger project to examine where D&O support is and isn't, by industry and organization size.

Future Studies

There are a few recommendations for future studies. First and foremost, it would be helpful for someone to secure a grant to fund a pool of surveyors that Cloud Research could vet using key indicators determined in advance. Based on my observations, core components affected surveyors' responses. For example, the differences among public, private, and non-profit organizations appeared significant, and it would be beneficial to examine how the results differ across these three groups. Another study that would be beneficial to conduct with two independent groups is one examining differences between non-technical and technical organizations. The last recommendation would be the company size relative to the IT security team and the maturity of cybersecurity. The hypothesis is that results follow an S-curve: results slowly build up, then a fairly sharp upward trend until growth levels off, and that this relates to the organization's maturity.

Conclusion

In conclusion, there remains a significant difference between the two groups: support for D&O for a CISO persists among cybersecurity professionals, but it still struggles among non-cybersecurity leaders. However, looking at the simple boxplot, the visual exposed that we may need to look deeper to truly understand where the support lies and where it doesn't. Significant understanding was gained from this research. The key insight was that this research provided direction for future, expanded research.

References

American International Group, Inc. (AIG). (2025). Directors & Officers (D&O) Liability Insurance: AIG US. Aig. https://www.aig.com/home/risk-solutions/business/management-and-professional-liability/directors-and-officers-liability

Aspen Digital. (2023, October 12). The evolving role of the CISO. The Aspen Institute. https://www.aspeninstitute.org/publications/the-evolving-role-of-the-ciso/

Brumfield, C. (2022). D&O insurance is not yet a priority despite the criminal trial of Uber's former CISO. CSO (Online), https://reddog.rmu.edu/login?url=https://www.proquest.com/trade-journals/d-amp-o-insurance-not-yet-priority-despite/docview/2716529469/se-2

Donelson, D. C., Glenn, J. L., & Yust, C. G. (2022). Is tax aggressiveness associated with tax litigation risk? Evidence from D&O insurance. Review of Accounting Studies, 27(2), 519–569.

Egger, P., Radulescu, D., & Rees, R. (2015). Heterogeneous beliefs and the demand for D&O insurance by listed companies. Journal of Risk and Insurance, 82(4), 823–852.

Gartner. (2024). Are United States organizations insuring against Ciso Liability Risk?. Gartner Peer Community. https://www.gartner.com/peer-community/oneminuteinsights/u-s-organizations-insuring-against-ciso-liability-risk-rgw

IANS Faculty. (2023, September 21). Why CISOs need D&O liability insurance coverage now. IANS. https://www.iansresearch.com/resources/all-blogs/post/security-blog/2023/09/21/why-cisos-need-d-o-liability-insurance-coverage-now

Jackson, D. (2023). CISOs find 'business as usual' shows the harsh realities of cyber-risk. Urgent Communications, https://reddog.rmu.edu/login?url=https://www.proquest.com/trade-journals/cisos-find-business-as-usual-shows-harsh/docview/3126314612/se-2

Jiang, H., Jia, J., & Hu, Y. (2022). Why do firms purchase directors' and officers' liability insurance?–Perspective from economic policy uncertainty. China Accounting and Finance Review, 24(1), 25-52.

Jones, D. (2023). SEC cyber rules ignite tension between reputation and security risk. Cybersecurity Dive, https://reddog.rmu.edu/login?url=https://www.proquest.com/trade-journals/sec-cyber-rules-ignite-tension-between-reputation/docview/2854690337/se-2

Likert, R. (1932). A technique for the measurement of attitudes. Columbia Univ.

Leyden, J. (2025, December 18). D&O liability protection rising for security leaders — unless you're a midtier ciso | CSO online. D&O liability protection rising for security leaders — unless you're a midtier CISO. https://www.csoonline.com/article/4107332/do-liability-protection-rising-for-security-leaders-unless-youre-a-midtier-ciso.html

Nash, K. S. (2023). Cyber Chiefs Worry About Personal Liability as SEC Sues SolarWinds, Executive; Tim Brown, the company's top security executive, is named in SEC suit. WSJ Pro.Cyber Security, https://reddog.rmu.edu/login?url=https://www.proquest.com/trade-journals/cyber-chiefs-worry-about-personal-liability-as/docview/2883908158/se-2

SEC. (2023). SEC charges SolarWinds and chief information security officer with fraud, internal control failures. United States Securities and Exchange Commission. https://www.sec.gov/newsroom/press-releases/2023-227

SEC. (2025). SolarWinds Corp. and Timothy G. Brown. United States Securities and Exchange Commission. https://www.sec.gov/enforcement-litigation/litigation-releases/lr-26423

Stupp, C. (2023). Cybersecurity Leaders Suffer Burnout as Pressures of the Job Intensify; Fallout from resource constraints is more stressful for cyber executives even if similar limitations affect every department, one CISO says. WSJ Pro.Cyber Security, https://reddog.rmu.edu/login?url=https://www.proquest.com/trade-journals/cybersecurity-leaders-suffer-burnout-as-pressures/docview/2814278294/se-2

United States Department of Justice (DOJ). (2022, October 6). Former chief security officer of Uber convicted of federal charges for covering up data breach involving millions of Uber user records. Northern District of California | Former Chief Security Officer Of Uber Convicted Of Federal Charges For Covering Up Data Breach Involving Millions Of Uber User Records | United States Department of Justice. https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-convicted-federal-charges-covering-data-breach#:~:text=SAN%20FRANCISCO%20%E2%80%93%20A%20federal%20jury,a%202016%20hack%20of%20Uber

United States Department of Justice (DOJ). (2025, January 15). The False Claims Act. Civil Division. https://www.justice.gov/civil/false-claims-act