

How Do You Do? Cybersecurity Liability Insurance

Social security numbers, tax information, bank accounts, payment methods, health records...there's no shortage of sensitive information contained in state agency databases. The exposure of such data can prove costly for both agencies and residents, which is why cybersecurity remains a top priority for government IT professionals. However, there is another layer of protection employed, a "break glass in case of emergency" option: cybersecurity liability insurance. Whether purchasing coverage, developing supplier requirements for IT solicitations, or managing awarded IT contracts, a basic understanding of cybersecurity liability insurance is vital for risk management and the success of an IT procurement project.

Cybersecurity liability insurance, also known as cyber liability, cybersecurity insurance, or cyber insurance, typically refers to a class of insurance policies that cover the financial liabilities associated with the disclosure, theft, or loss of personal, sensitive, or proprietary data.

For the purposes of this publication, it will be referred to as **cyber insurance**. What follows will explain some fundamental components of cyber insurance, important issues to consider, common approaches used by states and government entities, and some practical examples for illustration.



Incidents and Breaches

Generally, this coverage is invoked in the wake of security incidents or data breaches. It is important to note that there are differences between what constitutes a security incident versus a data breach.



A **security incident** refers to a security event that compromises the integrity, confidentiality, or availability of an information asset.



A **data breach** is any incident that results in the confirmed disclosure (not just potential exposure) of data to an unauthorized party.

Think of a burglar breaking into a house. The burglar may be able to get in through the front door, but may have trouble locating and stealing valuables within the home due to locked rooms or safes. Such is the case when it comes to cybersecurity—sometimes the network or system (the “house”) can be accessed, but no valuable data is extracted. If it cannot be confirmed that data was extracted from the network or system, the matter is termed a “security incident” and not a “data breach.” The distinction is important when it comes to each state’s laws regarding notice requirements to those potentially affected by a security incident or data breach.

In a data breach, the nature of the data accessed without authorization is significant in determining the applicable notification and potential remediation requirements. It is important to remain diligent about protecting against both security incidents and data breaches.



Consider the distinction between security incidents and data breaches when reviewing terms and conditions.

What's in a Plan?

Cyber insurance can have many different coverage components, and needs may vary across different state agencies, even within one agency. One data set may not have the same sensitivity or confidentiality as another data set (e.g., basic information available on the web compared to Social Security numbers), so it is essential to identify the risk level. Generally, personal identifying information, or PII (e.g., social security or driver's license numbers) and other sensitive data (e.g., health records and bank accounts), as well as systems that carry out mission-critical functions, represent significant risks and are prioritized for protection and coverage.¹

It is important to recognize the risks associated with the data involved in your procurement projects to identify coverage needs and any coverage your state or office already has. This informs cyber insurance requirements for solicitations and identifies existing gaps. Familiarity with your office or state's current cyber insurance policies is necessary for:



Risk Management – Ensuring that suppliers/ service providers have the appropriate coverage required by their contracts so that the state is adequately covered in the case of security incidents or data breaches.



Evaluation – Understanding cyber insurance features is useful when reviewing proposals from potential suppliers/service providers to differentiate between coverage levels, conditions, and insurer ratings.



Incident Response – Knowing what remediation options are available and how to access them following a data breach is essential to developing a quick and effective response.

¹Government Finance Officers Association, "Cyber Risk Savvy: How To Be a Smart Customer of Cyber Insurance," GFOA, 2022, https://gfoaorg.cdn.prismic.io/gfoaorg/3d840f3b-4ce1-4a06-aa65-a29b2cec8216_Cyber+Risk+Savvy_R1.pdf.

An efficient and effective cyber insurance plan is tailored to meet the specific needs of the covered entity and will typically cover some or all of the following:

- **Data Loss or Corruption** – Provides funds for recovering and restoring compromised data, remediation, repairing systems and hardware, and other ancillary services related to recovering functionality.
- **Identity Theft** – Covers costs associated with notifying potential victims, providing credit and identity monitoring services, and financial and/or property losses resulting from identity theft.
- **Ransomware** – Provides funds to pay the ransom/extortion demand, the costs of a consultant or expert to negotiate, the costs of backing up or retrieving previously saved data in the event of loss, and/or the costs of an expert to help block the attempted intrusion and reinforce the security.
- **Business Interruption** – Covers expenses associated with calculating and compensating for losses resulting from the disruption of critical business operations experienced during and immediately following a security incident.
- **Fiduciary Liability** – Covers potential liability of the government entity for financial losses of individuals and organizations resulting from cyber incidents or other data privacy violations in which the government has fiduciary responsibility to manage assets or provide services in the interest of stakeholders (e.g., pensions, social security accounts, healthcare benefits, etc.).
- **Breach Response** – Provides legal consultation with breach response experts, forensic investigation expenses, data restoration or replacement expenses, and public relations consultant expenses, and can also include expenses involved with notifying affected parties and offering credit monitoring and repair.
- **Crisis Management** – Includes expenses for general management of an incident, specifically the investigation, remediation, data subject notification, call management, and credit checking/monitoring.

Beyond these events, policies may cover claims pertaining to regulatory violations, digital asset loss and restoration, and privacy liabilities, among others.

Ransomware Exceptions



One of the most costly incidents that motivates public sector entities to strengthen or increase their cyber insurance coverage is ransomware attacks. These attacks hold data and/or network access hostage for payment, interrupting operations and potentially releasing sensitive data. However, some providers and policies exclude such events from coverage, and policies with robust protection can be prohibitively expensive.²

² Jule Pattison-Gordon, "Self-Insurance, Grant Planning on States' Cyber Agendas," Government Technology, August, 26, 2022, <https://www.govtech.com/security/self-insurance-grant-planning-on-states-cyber-agendas>.

First-Party and Third-Party Coverage

At its core, cyber insurance consists of two primary coverage components: first-party and third-party coverage.

First-party coverage pertains to the direct costs to an entity for a data breach or cyberattack, such as investigations, response actions, and disruptions of business operations. It covers the organization.

Third-party coverage pertains to liability, providing indemnity to the entity for any potential damages claimed because of a breach or attack. It covers the organization's clients or stakeholders. This coverage typically provides for monetary compensation, credit monitoring services, and other remediations to persons potentially impacted by the event, e.g., victims of identity theft.

Requirements for comprehensive third-party coverage for victims of identity theft resulting from a cybersecurity incident or breach may include:³



An established minimum level of financial coverage for each participant.



Costs associated with re-filing applications, including but not limited to loan applications and grant applications that were denied because of the identity theft.



Costs for notarizing affidavits, communications expenses, and postage required to restore the individual's identity.



Costs for a specified number of credit reports within an established time frame following the theft (e.g., six reports in the following 12 months).



Lost wages resulting from the need to take time off from work to engage in identity restoration activities, including reimbursement of paid time off (e.g. vacation, annual leave, etc.) taken to engage in identity restoration activities.

³Amendment 2 - RFP # 928 - Cybersecurity and Information Security Services - Idaho, GovWin IQ, July, 29, 2025, <https://iq.govwin.com/neo/document/view/26575803>.



Legal fees incurred in the defense of a civil suit against the individual/entity for non-payment in which the suit resulted from the identity theft, or for removal of a judgment against that individual/entity that resulted from the identity theft.



Coverage that extends to any identity theft that occurs while the individual/entity is enrolled, even if the identity theft is not discovered until after the credit monitoring and identity theft monitoring services have expired.

Buyer, Beware Be Aware

The market is limited. Compared to the traditional types of insurance coverage (home, business, auto, etc.), the cyber insurance market has fewer providers, less capital investment, and a significant lack of historical trend data for basing investment and business decisions. An already limited number of insurers are dependent upon an even more concentrated group of reinsurers (insurance providers for insurance providers). This means that the risk for insurers is also more concentrated, which can discourage capital investments and new providers from entering the market. Such conditions ultimately lead to expensive premiums.⁴

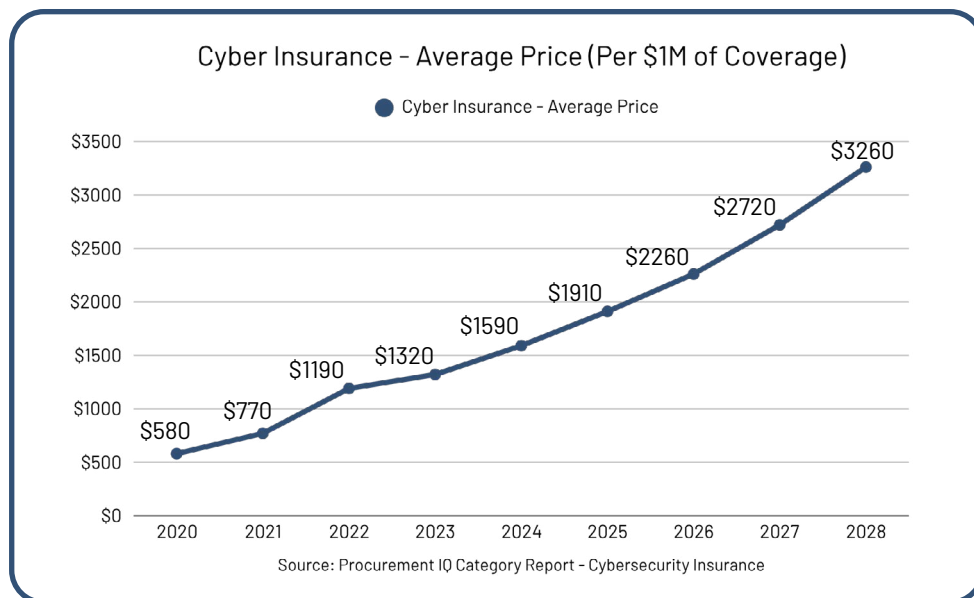
It's still young. A big factor in the market conditions for cyber insurance is its relative infancy. As both public and private organizations began exploring and acquiring coverage over the past decade, little information was available to guide decisions on coverage levels and premiums. Meanwhile, cyberattacks and their resulting financial consequences have continued to evolve in potency, increasing the risks to insurers and the insured. This has resulted in little consistency in premium levels industry-wide which makes benchmarking costs and coverage options difficult.⁵

Growing price trends. Both the limited market and its relative youth have contributed to a persistent rise in costs for coverage over the past several years, and current CAGR (compound annual growth rate)

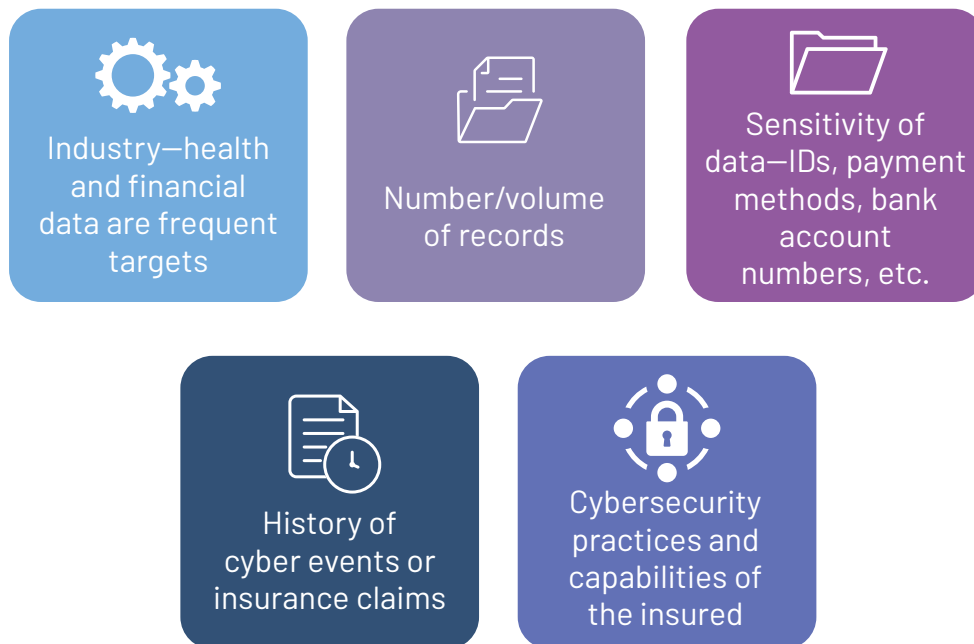
⁴Tom Johansmeyer, "Cybersecurity Insurance Has a Big Problem," Harvard Business Review, January 11, 2021, <https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem>.

⁵United States Government Accountability Office, "Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market," 2021, GAO-21-477, <https://www.gao.gov/assets/gao-21-477.pdf>.

projections predict these prices to continue to rise significantly year-on-year. For 2025, organizations can expect to pay an annual cost of approximately \$1,900 for each million dollars of coverage.⁶



Some key factors impacting cyber insurance premiums:



An environment of ever-evolving threats, lucrative targets for malicious actors, rising costs for coverage, and potentially grievous consequences for breaches presents tremendous risks for government entities. So, who is responsible for carrying cyber insurance coverage: the supplier or the state? More often now, the answer is both.

⁶ Ibis World, "Cybersecurity Insurance," Procurement IQ, 2025, accessed June 12, 2025, <https://client.procurementiq.com/procurement/reports/us/default.aspx?entid=1277>.

Coverage for the State

Some states have gone the route of obtaining their own insurance from a commercial provider for cyber and network liability, in addition to requiring their suppliers and service providers to have cyber liability coverage. A state's own cyber insurance policy, sometimes called an "enterprise-wide cybersecurity insurance policy," protects in the event of a data breach that originated within the state's own offices or agencies. As of 2023, over half of the states (53%) have acquired their own commercial cyber coverage.⁷

Planning and obtaining coverage for government entities should be done in partnership and consultation with Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and other risk management experts to assess potential solutions. The types of coverages acquired should align with the amount of risk involved in quantity and scope. Insurance specifications can be tailored to be agency, system, or project-specific. In the private sector, insurers commonly require documentation of, and some insight into, an organization's cybersecurity practices and defenses to inform the underwriting process. This may also apply to public sector entities. Such requirements reinforce the need for close collaboration with IT and security officials.

Some entities are stacking multiple insurance and risk management vehicles to provide comprehensive coverage and maximize available funds for responding to future events. This may include leveraging a self-insurance fund to mitigate gaps in commercial plans. Another approach includes pooling cyber risk together with other entities for a collective coverage plan, while acquiring secondary coverage to be used if the collective coverage limit is surpassed. Another available tool comes from IT suppliers, whose products and services may include a warranty that will provide some compensation for cyber events involving their products.⁹ Government entities can enhance their cyber liability coverage by strategically combining these tools for a multi-layered approach to protection and financial resilience.

State of Washington's Cyber Insurance Policies



Washington's Department of Enterprise Services has stacked cyber insurance coverages to fully cover the state's needs.⁹

Primary coverage is through a brokered service program that pools public entities nationwide. They also have an excess cyber insurance policy specifically for the state to cover gaps if the limits of the primary policy are exceeded. Together, they provide up to \$6 million per claim in cyber liability for extortion, data recovery, business interruption, and system failures.⁸

⁷National Association of State Chief Information Officers, "The 2023 State CIO Survey: The Force of Automation and the Reality of Modernization," NASCIO, 2023, <https://www.nascio.org/resource-center/2023-state-cio-survey/>.

⁸Washington Department of Enterprise Services, "Cyber Liability Insurance Overview: Policy Year 2024-25," 2025, <https://des.wa.gov/sites/default/files/2025-02/APIP-Cyber-Liability-Insurance-Overview.pdf>.

⁹Jule Pattison-Gordon, "Facing Cyber Insurance Woes, Local Governments Find Other Options," Government Technology, May 11, 2022, <https://www.govtech.com/computing/facing-cyber-insurance-woes-local-governments-find-other-options>.

What is “Self-Insured?”

Self-insurance is an alternative or supplemental approach to cyber insurance coverage. To offset the expense of a potential cyber incident, a government entity regularly sets aside money for a self-insurance fund. Often, these funds are held in a low-risk investment account that can accrue interest. Following a cyber incident, these funds would be used to cover all necessary costs, recovery expenses, and liabilities. As of 2023, 33% of states reported being self-insured for cyber incidents.¹⁰

Commonly described benefits of self-insurance models include:



As previously mentioned, some public entities have elected to self-insure up to a specified liability limit while purchasing a commercial plan to cover any exceptional costs. In theory, assuming more risk on the part of the public entity will lower their insurance premiums.¹¹ **It is important for self-insured entities to conduct an internal risk assessment prior to any relevant contract agreement** to ensure their self-coverage is adequate and inform any corresponding insurance requirements for suppliers.

Arkansas's Self-Funded Cyber Response Program



Arkansas's Self-Funded Cyber Response Program was established via statute ([AR Code § 21-2-804](#)) and includes a trust fund to provide financial support in lieu of commercial cyber insurance for its political subdivisions. Legislative findings concluded that the cost of comprehensive cyber insurance coverage is "too burdensome for a city, county, or school district" and that "considerable savings might be effected by the establishment of a self-funded cyber response program" to provide coverage to those entities or as secondary coverage for those with commercial policies.¹²

¹⁰ National Association of State Chief Information Officers, "The 2023 State CIO Survey: The Force of Automation and the Reality of Modernization," NASCIO, 2023, <https://www.nascio.org/resource-center/2023-state-cio-survey/>.

¹¹ Jule Pattison-Gordon, "Facing Cyber Insurance Woes, Local Governments Find Other Options," Government Technology, May 11, 2022, <https://www.govtech.com/computing/facing-cyber-insurance-woes-local-governments-find-other-options>.

¹² AR Code § 21-2-802 (2023), accessed June 12, 2025, <https://law.justia.com/codes/arkansas/2023/title-21/chapter-2/subchapter-8/section-21-2-802/>.

Captive Insurance is a type of self-insurance where an entity legally creates another entity for the sole purpose of providing and administering insurance to itself and other designated entities. Justification for this approach is based on a captive provider's ability to more accurately evaluate, control, and mitigate risks due to their unique access and insight into government operations and assets. Captive insurance entities can set premiums with more precision and efficiently manage claims. Other benefits include tailored coverage for special or difficult risks, access to reinsurance markets, and reduced volatility in coverage costs.¹³



Tennessee's Captive Insurance



In May of 2021, Tennessee established the Tennessee Captive Insurance Company which provides property, general liability, and cyber insurance.¹⁴ The cyber policy covers data and security breach liability and response costs for all state government entities and public higher education institutions. It is governed by the Tennessee Captive Insurance Board which is comprised of several state department executives.¹⁵

¹³ Boards and Commissions, "Tennessee Captive Insurance Company Board of Directors," Tennessee Department of Treasury, accessed June 12, 2025, <https://treasury.tn.gov/Explore-Your-TN-Treasury/About-the-Treasury/Boards-and-Commissions/Tennessee-Captive-Insurance-Board>.

¹⁴ TN Code § 9-8-103 (2024), accessed June 12, 2025, <https://law.justia.com/codes/tennessee/title-9/chapter-8/part-1/section-9-8-103/>.

¹⁵ Boards and Commissions, "Tennessee Captive Insurance Company Board of Directors," Tennessee Department of Treasury, accessed June 12, 2025, <https://treasury.tn.gov/Explore-Your-TN-Treasury/About-the-Treasury/Boards-and-Commissions/Tennessee-Captive-Insurance-Board>.

Requirements for Suppliers

Suppliers and service providers are often required to have certain minimum levels of coverage in order to do business with the states. Coverage held by those with whom the state does business protects the state if a security incident or data breach occurs due to the business activities and/or access of those suppliers or providers within the state's network. It also covers when providers' networks handle or store sensitive or protected data used to deliver on public contracts. This way, the state has some level of protection regardless of the event's location.



Insurance requirements for suppliers should:



Meet all statutory and regulatory obligations



Be appropriately matched to the level of risk associated with the services to be provided and the nature of the data involved

Insurance requirements for suppliers should not:



Be onerous or overly burdensome such that it significantly limits the number or ability of suppliers to compete



Be used as a supplement or substitute for sub-standard cybersecurity protections

Cyber insurance coverage requirements should be outlined in the solicitation, typically in a general conditions or general requirements section, using the same or similar language that will be used in the eventual contract. The type and value of the coverage required should be informed by the scope of services to be provided, the amount and nature of the data involved, and all applicable rules and policies. Before entering into a contract, there should be established procedures for suppliers to provide, and officials to record, proof of adequate insurance coverage throughout the contract's life.



Sample Language Requiring Specific Types of Coverage

Coverage. Coverage must be written on an occurrence basis. The minimum acceptable limits will be as indicated below:¹⁶

13.3.5 Information Security/Cyber Liability Insurance: The Contractor must maintain Cyber Liability and Security Insurance covering personally identifiable information transmitted to, accessed, created, or stored within the Contractor's computer system or within any associated third-party's computer system with minimum liability limits of \$5,000,000 per occurrence and provide coverage for the following risks (collectively, "cyber-security liabilities"):

13.3.5.1 Liability arising from theft, dissemination, and/ or use of personally identifiable information transmitted to, accessed, created, or stored on the Contractor's computer system or within any associated third-party's computer system;

13.3.5.2 Information or identity theft, misuse of, or unauthorized disclosure of personally identifiable information;

13.3.5.3 Spread of viruses, loss of, denial of access to, attacks on, damage to, alteration of or destruction of personally identifiable information;

13.3.5.4 Infringement of intellectual property, including but not limited to, copyright, trademark, multimedia/media, or trade dress infringement or violations;

13.3.5.6 Extortion or threats of extortion.

¹⁶ Amendment 2 - RFP # 928 - Cybersecurity and Information Security Services - Idaho, GovWin IQ, 29 July, 2025, <https://iq.govwin.com/neo/document/view/26575803>.

Beyond setting standards for coverage, there are other key terms and conditions that need to be addressed within the solicitation and subsequent contracts. Some common essential clauses include:¹⁷



Term requirements mandate that the supplier maintain in full force and effect the prescribed insurance for the duration of the contract and/or for as long as they possess the protected data.



Class requirements set business standards for the insurance carriers that suppliers can use. Typically, they must be licensed to conduct business in the contracting state and carry a minimum threshold rating score from a recognized independent evaluator such as A.M. Best or Moody's.



A waiver of subrogation clause protects the government (or its insurance provider) and officials from litigation and redress from a supplier's insurer in the event that negligence results in the payment of insurance claims. These clauses may also dictate the process and venue for resolving any disputes that arise.



Termination clauses allow the contracting state or government entity to terminate its agreement with a supplier who fails to acquire or maintain the required insurance coverage. Likewise, failure to produce certificates of insurance within the designated time prior to contract performance or following any necessary policy renewals can be grounds for termination.



¹⁷ Rhode Island Department of Administration, Division of Purchases, "General Conditions – Addendum A: General Insurance Requirements," accessed June 12, 2025, <https://ridop.ri.gov/sites/g/files/xkgbur616/files/documents/general-conditions-addendum-a.pdf>.

What About Subcontractors?

If a contract allows for subcontracting any portion of the work, then consideration must be given to any associated risks. **Solicitation documents and contract agreements should outline the authorization to use subcontractors, the minimum requirements to qualify subcontractors, and any division of liability between the contractor and subcontractors.** For example, when addressing subcontracting, a government entity could include clauses stating that:

- *Contractors must request approval for the use of subcontractors*
- *Subcontractors must meet all minimum requirements provided in the solicitation*
- *Subcontractors must carry the same type and level of insurance as the contractor or otherwise present proof that the contractor's insurance covers them*
- *The contractor shall remain liable for all damages due to a subcontractor's negligence or non-performance*
- *Neither approval of the subcontractor nor the provision of payment for subcontracted work relieves the contractor of any responsibility or liability*



Have a Response Plan

Knowing what to do in the event of a data breach can save time and limit the damage as much as possible. Staff should know to immediately document any breaches they become aware of, noting the date, time, and duration (if known) of the alleged breach. Educate everyone on whom to contact in the event of a data breach, and establish a method for reporting questionable activity or suspected breaches. The federal Cybersecurity & Infrastructure Security Agency offers [reporting guidelines](https://www.cisa.gov/sites/default/files/publications/Shar ing_Cyber_Event_Information_Fact_Sheet_FINAL_v4_0.pdf).¹⁸ Training should be conducted regularly within the state procurement office to emphasize the importance of the state's cyber breach response plan..

¹⁸ "Sharing Cyber Event Information: Observe, Act, Report," United States Cybersecurity & Infrastructure Security Agency, 2022, https://www.cisa.gov/sites/default/files/publications/Shar ing_Cyber_Event_Information_Fact_Sheet_FINAL_v4_0.pdf.

Conclusion

Most data breaches are the result of either malicious or criminal attacks, system glitches, or human error. No location, industry, or organization is invincible when it comes to the potential for a compromise of data, and government servers are no exception. When obtaining coverage, public entities should consult their CIOs and thoroughly explore current market conditions and potential coverage options, including self-insurance. Specifications should be informed by the nature of the data involved, the scope or volume of coverage needed, and any statutory or regulatory requirements. When setting coverage standards for suppliers, requirements should match the level of associated risk and meet all legal obligations but not be burdensome to the point of limiting competition.

Ultimately, cyber insurance is a necessary stopgap measure. It shouldn't be an emergency plan or relied upon to save public entities from catastrophe. It is another tool in the toolkit to help entities recover from unexpected breaches and compromising events. Like most other forms of insurance, when it is needed, something has gone wrong. And once it is used, it will become more expensive. It is an important component of a comprehensive approach to security, but it does not lessen the critical need for investments in effective cybersecurity mechanisms and diligent cyber hygiene practices.



CHADWICK STEPHENS, Research Manager

September 2025

For any questions or requests, contact us at research@naspo.org

Resources for Further Learning

The National Association of State Chief Information Officers (NASCIO) conducts an [annual survey](#) focused on key cybersecurity and IT issues.

The Government Finance Officers Association (GFOA) and the Center for Digital Government offer a [highly detailed guide](#) for identifying the appropriate cyber insurance coverage options for government entities based on risk.

The United States Government Accountability Office (GAO) provided [this report to Congress](#) detailing the challenges emerging from the cyber insurance marketplace.

NASPO Procurement U Courses on Risk Management: [Identifying and Analyzing Risk and Responding to and Monitoring Risk.](#)