States Confront the Cyber Challenge

Cyber Liability Insurance for States

Perfect cybersecurity is impossible, and even the most sophisticated defenders fall prey to cyber attacks. This residual risk can potentially impose massive costs on an organization. Even mundane security breaches—a misplaced laptop storing confidential data—can trigger costly response procedures. States can offset the cost of a breach by purchasing *cyber liability insurance*.

Cyber liability insurance has existed in some form for many years, but not until recently have most major insurance providers begun to promote it. However, it remains a nascent field, and many policies are highly individualized to each policy holder. This document provides a broad overview of cyber liability insurance, highlights key questions that states should consider, and suggests authoritative resources.

What is Cyber Liability Insurance?

Purchasers of cyber insurance pay a regular fee—a premium—in exchange for a commitment by the insurer to absorb the reasonable costs of security incidents. Cyber insurance agreements have three components:

- *First-party coverage* for direct costs, such as customer notification; credit and identity theft monitoring; crisis communications consulting; forensic investigation; and database recovery.
- *Third-party coverage* for indirect costs, such as those arising from litigation or regulatory fines.
- *Exclusions* that allow the insurer to avoid payment in predefined scenarios, such as nation-state cyber attacks, breaches where the policy holder is an unintended victim, and disruption to computing resources that do not belong to the policy holder.

An applicant for cyber liability insurance must undergo an underwriting process by which insurers assess the maturity of the applicant's risk posture. If the insurer agrees to award a policy to the applicant, the insurance agreement will require the policy holder to adhere to certain cybersecurity practices. Deviance from these standards will void coverage. As such, whatever cybersecurity controls exist as part of the insurance agreement should be integrated into technical, administrative, and organizational security controls throughout all state offices subject to the insurance policy.

Cyber liability insurance is one component of a holistic risk management strategy; it is not a substitute for a robust information security program. Although it may offset first- and third-party costs incurred following a breach, but recovering expenses does not fulfill the state's obligation to *prevent* harm to the public welfare.

What Are Key Questions to Consider When Purchasing Cyber Liability Insurance?

Am I coordinating with state risk managers? Insurance providers offer policies covering a wide range of costs. Before states embark on the underwriting process, state managers should achieve consensus on the objective. One state might want to insure against catastrophic loss alone, while another might focus on addressing everyday security breaches. Existing risk management divisions are well-equipped to answer these questions. They can also assist in working with current insurers to review whether existing agreements already cover cyber-related losses. Particularly in cases where a state is seeking narrow coverage, modifying an existing policy can save significant staff time and resources.

How can I get a sense of the typical policies that exist? The SERFF Filing Access System is an online portal allowing insurance providers to submit products for review by state insurance regulators. Forty-nine states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands participate.

Exploring a sampling of policy submissions in the relevant jurisdictions should help state officials establish expectations for cyber insurance products. It is also a cost-effective manner for determining if standard insurance products are missing coverage provisions that are important to a given state applicant.

What if the provider rejects the application? States should not be discouraged if their initial foray into cyber insurance meets with apparent failure. The underwriting process can resemble a "black box": the insurance provider intakes an application for review, assigns a risk label, and issues an approval or denial, without a deeper analysis. A paper process deprives applicants of the ability to address the concerns of underwriters, for example by exempting from coverage individual agencies. States should attempt to secure in-person or video-conference meetings with underwriters to build rapport, encourage frank exchanges, and allow states to demonstrate flexibility.

Will the policy require constant updating? Cyber threats are dynamic, and states should negotiate for agreements that account for constant changes in techniques, tactics, and procedures.

What are some common exclusions to be aware of? Many security incidents are accidental. States should negotiate for policies that cover insider scenarios, including those wherein an attacker uses fraudulent information to trick an employee into committing a security breach. In addition, the disruption of some government services—such as emergency response—can result in bodily harm or even death, but many cyber insurance products exclude costs associated with the physical effects of security incidents. Most available policies also exclude *all* costs from breaches that are perpetrated by geopolitical actors.

What is an unexpected consequence of purchasing cyber liability insurance? Some insurance policies stipulate that policy holders must choose from a limited list of vendors for certain response services, such as forensic investigation or identity monitoring. In some cases, these requirements could conflict with existing agreements with other state prime contractors or subcontractors. States that cannot deconflict these provisions should be prepared to negotiate new terms or seek insurance from other providers.

How can states negotiate for a less expensive policy? Some insurance policies break down coverage into subcategories, such as data theft remediation, extortion payments, or identity theft mitigation. In negotiating with insurers, state should consider whether some of these subcategories are necessary. For example, if a state refuses to pay ransoms, or believes it will not require assistance in crisis communications, then it may be able to reduce premiums by working with insurers to eliminate those sub-limits.

Where can I find additional resources?

Cybersecurity, NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS (2017), http://www.naic.org/cipr_topics/topic_cyber_risk.htm.

Purchasers' Guide to Cyber Insurance Products, FINANCIAL SERVICES SECTOR COORDINATING COUNCIL (2016), https://www.fsscc.org/files/galleries/FSSCC_Cyber_Insurance_Purchasers_Guide_FINAL-TLP_White.pdf.

Cyber Liability Insurance: Overview, STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENT COORDINATING COUNCIL (SLTTGCC), (2016), https://ioem.idaho.gov/Resources/PDF/Cyber%20Liability%20Insurance%202016%2006%2017%20(final).pdf.

Cyber/Information Security Insurance: Pros/Cons and Facts to Consider, NATIONAL ASSOCIATION OF CHIEF INFORMATION OFFICERS (2015), https://www.nascio.org/dnn/portals/17/2015MY/Cybersecurity%20Insurance.pdf.

Frequently Asked Questions: Cyber Liability Insurance, WASHINGTON STATE DEPARTMENT OF ENTERPRISE SERVICES (2015), http://des.wa.gov/sites/default/files/public/documents/RiskManagement/APIP%20CL%20FAQ%20-%20V7.pdf.

Please e-mail David Forscey, Policy Analyst, Homeland Security and Public Safety Division, NGA at: dforscey@nga.org *with any questions.*