CSDSIP Cyber Coverage

Explaining Your Policy

CSDSIP offers our Members the opportunity to add Cyber Enterprise Risk Management Coverage (Cyber) to complement our core policy. Cyber coverage is a supplementary coverage and is issued as stand-alone insurance policies, each with their own Declarations Page, Conditions, Insuring Agreements, and Endorsements. It is offered in alliance with Chubb & ACE American Insurance Company (collectively "Chubb").

Members may be granted coverage based upon the underwriting information they provide during the Renewal Application process. Members who successfully submit the application and are approved by Chubb receive Cyber coverage as part of their CSDSIP annual contribution.

This coverage summary is a basic overview of the policy and is in no way a substitute for the complete policy. This summary is a high-level overview of where coverage may be triggered. At the time of this article's publication, Chubb was still working on issuing the 2021-2022 Cyber Policy and our Member Certificates. As soon as we receive and review the policy, we will notify Members who have Cyber coverage that the policy is ready to be downloaded. As always, claims are subject to the terms and conditions of the policy. Claims are also reviewed on a case-by-case basis and ***need to be reported to us and to Chubb as soon as possible. Delay in reporting or failure to report may result in reduction of your limits.***

Also keep in mind that each of our Members who participate in this coverage have their own individual limits. These limits though are subject to a $5M Maximum Pool Policy Aggregate Limit of Insurance which applies regardless of how many Members or how many claims happen during the policy period. All claim expenses including attorney's fees, mediation costs, expert witness fees, forensic investigation fees and other fees and costs incurred in the defense and investigation of Cyber claims will erode your limit.

Your Cyber Policy

Chubb's Cyber Enterprise Risk Management policy has two basic categories for their Insuring Agreements: First Party and Third Party Liability.
First Party Insuring Agreements triggers coverage for your claims for damage as the owner of the property (including data) that you may incur as a result of a cyber incident including:

- Cyber Incident Response Fund – Provides coverage for **cyber incident response expenses** incurred by you in response to a **cyber incident** first discovered and reported during the **policy period**. For this particular coverage, coverage limits are reduced if you use a Non-Panel Response Provider.

- Business Interruption & Extra Expenses – Provides coverage for **business interruption loss** and **extra expenses** incurred by you during the **period of restoration** resulting directly from a **cyber incident during the policy period**.
- Digital Data Recovery – Pays for the **digital data recovery costs** incurred by you resulting from a **cyber incident** first discovered and reported during the **policy period**.
- Network Extortion – Reimburses **extortion expenses** incurred by you in response to a **cyber incident** which occurs during the **policy period**.

Third Party Liability Insuring Agreements trigger coverage for third-party claims that allege that you were liable for causing damage to them and includes:

- Cyber, Privacy & Network Security Liability – Pays for **damages** and **claims expenses** by reason of a **claim** first made against you during the **policy period** for a **cyber incident** which occurs during the **policy period**.
- Electronic, Social & Printed Media Liability – Pays for **damages** and **claims expenses** by reason of a **claim** first made against you during the **policy period** for a **media incident** which occurs during the **policy period**.

Coverage for third-party liability claims is written on a claims-made coverage form, escalating the importance of timely claims reporting. Please report claims to us as soon as you receive notice of the claim. The coverage in place at the time that the claim is reported (not at the time the occurrence happened) is the coverage that would apply to the claim.

As always, coverage is subject to the terms, provisions, limitations, exclusions and definitions of the policy. You'll notice there are several items that are highlighted above in bold. They are highlighted because they are defined terms in the Cyber policy. As such, when you are reviewing the policy, it's important that you carefully read all of the defined terms before you apply coverage.

Coverage Exclusions

This year Chubb added the following new exclusions to our policy which include:

- Specified Incident Exclusion for Government Shutdown.
- Specified Incident Exclusion for any Microsoft Exchange server which runs any version of software exposed to vulnerabilities documented with the National Institute of Standards & Technology's National Vulnerabilities Database.
- Specified Incident Exclusion for the presence or vulnerability of any SolarWinds Orion Platform software with any version prior v2020.2.1 HF 2.
- Loss of Technical Support Exclusion – Any Network Security Failure due to a loss of technical support.
- Protective Safeguards Exclusion – Applied to a Member's policy whose website has known vulnerabilities if the vulnerability is not corrected.

Current Market Factors

The exclusions above offer insight to the current Cyber insurance market, which is in great turmoil. In the last couple of years Cyber carriers have sustained frequent and severe cyber incidents in concert with a significant uptick in ransom claims. Because most Cyber insurance policies includes coverage for hackers ransoms, the industry cannot rule out the possibility that hackers may be intentionally targeting those with Cyber coverage. Expensive follow-up costs associated with forensic investigations and systems clean-up are also rising with demand, multiplying carriers' concerns.

303.722.2600
www.csdsip.org
: @CSDSIP

This cost inflation continues to provoke protective measures from Cyber insurance carriers, and we are seeing reduced limits, reduced coverage offered and/or sublimited coverage, and significant premium rise across the board from carriers who choose to stay in the market, not to mention those who simply no longer offer the coverage at all.

What Can Members Do?

While this article focuses on Cyber coverage, good Cyber risk management is the best way to prepare your school, district, or schooling entity for the uncertain future ahead. We don't yet know what Cyber coverage will look like next year including whether we will be able to secure Cyber coverage, but no matter what happens, CSDSIP will be here with trustworthy advice, guidance, and resources. This edition of InSight delves into the specifics of cyber safety, but the checklist below is a great place to start assessing what resources you may need.

- Ask your IT Team about their top-level concerns. What keeps them up at night?
- Review your electronics monitoring procedures. How do you ensure hackers aren't coming in?
- Check up on your protected data (data that has personally identifying information). Do you encrypt this data?
- Ensure routine hardware and software monitoring. Are there any security patches out there that need to be applied? How often do you apply those security patches?
- Inspect "end of life" (hardware and software that they are no longer providing security patches for) hardware and software securing procedures. Are all of your devices still receiving proper updates? Can they be updated?
- Analyze your data backup procedures. Are critical and sensitive systems and data backed up daily and stored securely offline?
- Focus on employee empowerment. Are you training your employees annually on cyber security such as being on alert for phishing and social engineering schemes?
- Employ cyber security best practices such as Multi Factor Authentication (MFA). Do you require MFA for remote access to your network? You may have to. We are hearing that some Cyber carriers that are requiring MFA in order to even consider coverage.
- Review your anti-virus and anti-malware programs and ensure the presence of Endpoint Detection and Response (EDR), which runs in the background of your system to constantly look for and fight viruses and malware.

Are you prepared to respond to a cybersecurity threat? Take steps to help reduce your exposures and mitigate potential losses. Chubb's expertise and specialized solutions can help you do just that. All Chubb policyholders are eligible for cyber services. Get the most value from your Chubb policy and request access by going to https://www.chubb.com/us-en/business-insurance/getcyberservices.html. You'll need to refer to your Chubb policy number which for our Members who have Cyber Coverage which is EON G25676683 006.

303.722.2600
www.csdsip.org
: @CSDSIP

CSDSIP Cyber Coverage

You'll find access to get to Chubb's Mitigation Tools including the following. We'd like to highlight the services that are in blue and asterisked because they are ***provided at no additional cost.***

	Solution/Service	Short Description	Provider
Incident Response	***Chubb Cyber Alert****	Mobile app for reporting incidents to the hotline	Chubb
	Online Response Plan Manager	Breach Plan Connect® helps you build and maintain a customized response plan that can be accessed via the web or mobile device	NetDiligence
	Response Readiness Assessment	A personalized assessment of your current incident response plan or get help creating one to get a fundamental plan in-place quickly	Security Risk Advisors
	Virtual Tabletop Exercise	A virtual simulation of a cyber scenario to test the organization's ability to appropriately comply with their incident response plan.	Mullen Coughlin
Vulnerability Management	***Chubb Vulnerability Alerts****	Get periodic updates that highlight the most critical and recent vulnerabilities	Secalerts
	External Vulnerability Monitoring*	BitSight Core, an online platform that helps identify vulnerabilities on your network – especially unknowns one that emerge or persist overtime.	BitSight
	Network Vulnerability Scan	An automated vulnerability scan of up to eight external network addresses	NetDiligence
Endpoint Security	Endpoint Protection & Response	CrowdStrike's Falcon Prevent, an EDR solution that can be deployed quickly across a network to transparently protect your personal computers against ransomware	CrowdStrike
User Security & Awareness	Multifactor Authentication Assessment	A review and test of an organization's MFA implementation and provide guidance on mitigating any exposures discovered.	Security Risk Advisors
	Secure Password Manager*	Dashlane, a secure password manager, that makes it easier to create and use stronger passwords	Dashline
	Phishing Simulation	Test a sample of your employees to see how well they respond to two unique simulated phishing attacks	Cofense
	Security Awareness Training*	Two courses to educate all your employees (Security Awareness Basics + Security Awareness for Information Technology)	Skillbridge
	Cyber Risk Resource Library*	eRiskHub®, an online resource to help prevent network, cyber, and privacy losses along with sample templates that you can use	NetDiligence
**** Included with Chubb's Cyber Coverage at no cost***			

If you have any Cyber coverage questions or would like to find out if you have Cyber coverage offered through CSDSIP, please contact our Risk Programs Team.

If you have any questions as to how you can better manage your risk of cyber-attack, please contact our Risk Control Team.

303.722.2600
www.csdsip.org
: @CSDSIP