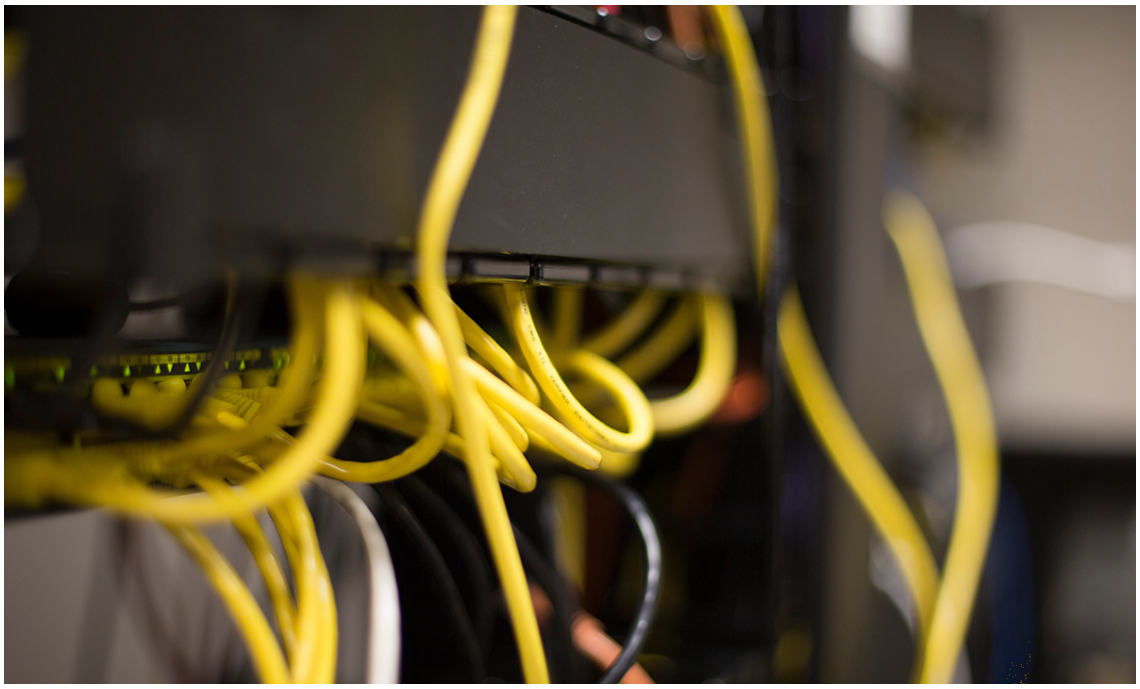
# Know Your Policy: Your Coverage and Responsibilities under the Cybersecurity Policy



**By Sherie Edwards, J.D.**

As a value-added benefit of your SVMIC professional liability policy, you and your practice are provided with $50,000 of cybersecurity coverage (with the option to purchase more coverage). This coverage, although provided by SVMIC, is written and administered by Tokio Marine Houston Casualty Company, referred to in this article as TM. As with any insurance policy, it is good to familiarize yourself with what is covered, what is excluded, and what your responsibilities are in terms of reporting an incident to be sure that you are doing all you can to maximize this benefit. This information will also be valuable in conforming your internal policies and procedures related to incident reporting to the requirements under the policy; it's better to know and be ready for an incident rather than to expend precious time scrambling to try to figure out what should be done while in the thick of a crisis.

**What is Covered?**

The protection provided under the Cybersecurity policy falls into two categories: First Party claim coverage and Third Party claim coverage. A First Party claim is an event that impacts your practice and/or your systems, such as a potential compromise resulting from a phishing email or ransomware attack. A Third Party claim is an event which has the potential to result in a lawsuit against your practice. An example of this would be a HIPAA breach. The nine types of coverages named in the policy are:

**Coverage A: Multimedia Liability**—the release or display of information on your website or in printed material for which you have sole responsibility and which results in a claim of defamation, libel, or product disparagement (list is not inclusive).

**Coverage B: Security and Privacy Liability**—this category includes HIPAA/HITECH breaches, data breaches that involve Personally Identifiable Information (PII), breach of government laws and regulations regarding privacy protections; a security breach that occurs due to the failure to have systems and protections in place; and unauthorized access or use of your computer systems.

**Coverage C: Privacy Regulatory Defense and Penalties**—covers the fines, penalties, and awards you are required to pay, by statute or regulation, that result from a security or privacy breach.

**Coverage D: Privacy Breach Response Costs; Patient Notification Expenses and Patient Support; Credit Monitoring Expense**—up to the limits of your coverage, pays the costs of notifying affected individuals when a privacy/security breach occurs.

**Coverage E: Network Asset Protection, which includes Loss of Digital Assets and Non-Physical Business Interruption and Extra Expense**—this coverage pays to restore data and computer programs to their same state and contents as they were prior to being damaged, destroyed, or stolen. This includes the time spent by your employees to recover or restore these digital assets. Non-physical business interruption includes income loss and expenses incurred while the use of your computer system is interrupted

due to a covered event (such as a phishing hack or ransomware).

**Coverage F: Cyber Extortion (ransomware)**—this article from our June 2021 Sentinel provides a comprehensive overview of ransomware attacks.

**Coverage G: Cyber Terrorism**—an act of cyber terrorism is an attack by a person or a group against computer systems, the Internet, or networks in order to cause disruption, intimidation, or otherwise cause harm. This is usually done to further a political, religious, or ideological cause. Many insurance policies, including this one, exclude damages caused by war, invasions, or insurrections; however, acts of cyber terrorism are not included in this usual exclusion.

**Coverage H: PCI DSS Assessment**—if you accept credit cards for payment, then you are familiar with Payment Card Industry standards, or PCI. This coverage provides protection if you are fined by a bank or credit card company in the event of a security or privacy breach that violates a PCI standard.

**Coverage I: BrandGuard®**—BrandGuard is the name TM gives to their coverage that protects you against decreased business income due to negative media coverage. As with all losses, there is a specific way this loss is determined, which is outlined in your Endorsement.

In some instances, the coverages listed above will extend to damages or loss caused by a third party Business Processing Outsourcing (BPO) provider or an outsourced IT service provider.

**How Much Coverage Do I Receive?**

The Cybersecurity policy that SVMIC provides as a benefit includes $50,000 of coverage per claim for each coverage shown above. The aggregate amount depends on the number of physicians in your group practice:

| | |
|---|---|
| 1 physician | $50,000 aggregate |
| 2-10 physicians | $100,000 aggregate |
| 11-20 physicians | $150,000 aggregate |
| 21+ physicians | $250,000 aggregate |

Unlike your professional liability policy, defense costs are included toward the total amount of your coverage. Also, depending on the type of coverage (D, E, F, G, and I above), claims arising from “the same, related on continuing incident(s)” will be considered as one claim. Likewise, claims made under Coverages A, B, C, and H, if considered to be

causally or logically related, will be viewed as a single claim.

**What is Excluded?**

Your Cybersecurity policy lists several Exclusions, and you are encouraged to read those in the Cybersecurity endorsement to your professional liability policy. A few examples of exclusions are a deliberate act or willful violation of a law; obligations under other insurance policies such as worker's compensation or any other employment matter; a liability you assume under a contract or agreement (unless you would have been liable even if a contract or agreement didn't exist); or a violation of sanctions imposed by the Federal government, including sanctions under the Office of Foreign Assets Control (OFAC).

The last exclusion mentioned above is critical as it relates to cyber extortion claims (ransomware). If a ransom payment is made to a terrorist group or another party on the OFAC sanctions list, that payment may be excluded from coverage. It may also result in criminal penalties from the Federal government. This underscores the importance of calling SVMIC to report an incident before taking **any** action on your own.

As noted earlier, this list is not all inclusive, and you should review your policy for the full list.

**What are my responsibilities under the policy?**

As with your professional liability policy, you have a duty to notify SVMIC of a claim or incident as soon as you are aware, whether by receiving a notice of claim from a third party or through your own discovery. The policy requires the following notices:

- For Coverages A, B, C, or H you are required to provide written notice of the claim during the policy period.
- For Coverages D, E, F, G, or I, you are required to provide written notice within 60 days of discovering (or within 60 days of when you should have reasonably discovered) a media report that is adverse, a security or privacy breach, a covered cause of loss, a cyber extortion threat, or a cyber terrorism act.

However, we strongly encourage you to contact SVMIC as soon as you know or suspect an incident has occurred, or that the potential for a claim exists. With your notice, we can place you in contact with TM who will provide the assistance (legal and technical) needed to address the issue.

It is also important to note that any payments you make or settlements you enter into before notifying SVMIC of an actual or potential incident may be excluded from coverage.

**Additional Coverage**

If, after reading this article you believe that $50,000 of coverage would not be adequate to protect your practice from a cybersecurity incident, please call SVMIC and ask to speak to

one of our Underwriting Specialists. They can help you obtain additional coverage.

**Prevention is always the best policy**

Just as the risk management education programs SVMIC provides help you decrease your professional liability risk, the cybersecurity resources you can access through Vantage® can help your practice protect itself against cybersecurity losses. These resources, offered by CyberNet and accessible via the Vantage policyholder portal, include educational materials, sample policies, information about incident response plans and business continuity plans, and news about the latest cyber threats. Just like your Cybersecurity policy, these resources are a value-added benefit of your professional liability policy with SVMIC.

If you have questions about cybersecurity or access to the resources available exclusively to SVMICmembers, call 800-342-2239 or email ContactSVMIC@svmic.com.

Individuals in your organization such as your administrator, privacy or security officer, or information technology professional may benefit from this article and the other resources available to SVMIC policyholders and staff through their Vantage account. If someone in your organization needs a Vantage account, they can sign up here.

**If you experience a potential cybersecurity incident**, contact SVMIC as soon as possible by calling 800-342-2239 and asking to speak to the Claims department.

---