



Worldwide Facilities, LLC

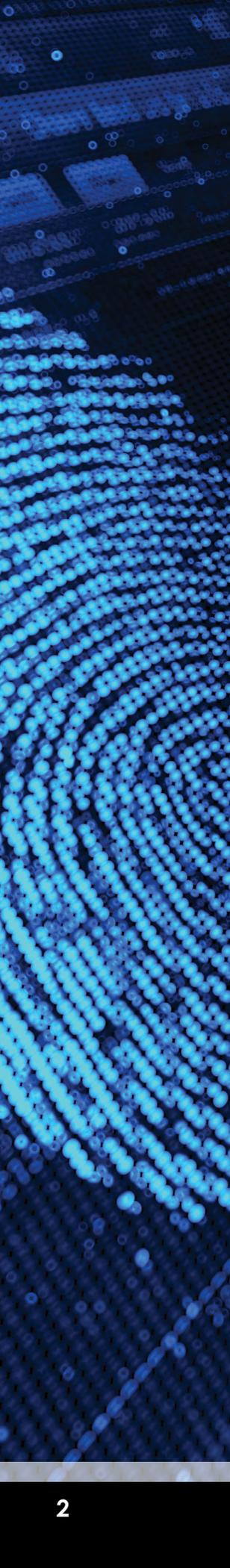
“Experience a World of Difference”

www.wwfi.com

Evaluating Cyber Scope of Coverage

**ARE YOU LEAVING
YOUR CLIENTS EXPOSED?**

WHITE PAPER



Evaluating Cyber Scope of Coverage: Are You Leaving Your Clients Exposed?

Hardly a day goes by without some high-profile cyber breach in the news. From the May 12 WannaCry ransomware attack that took down enterprise systems all over the world, to the malware that infected over 1,200 properties owned by InterContinental Hotels Group, the message is clear: All organizations need cyber insurance.

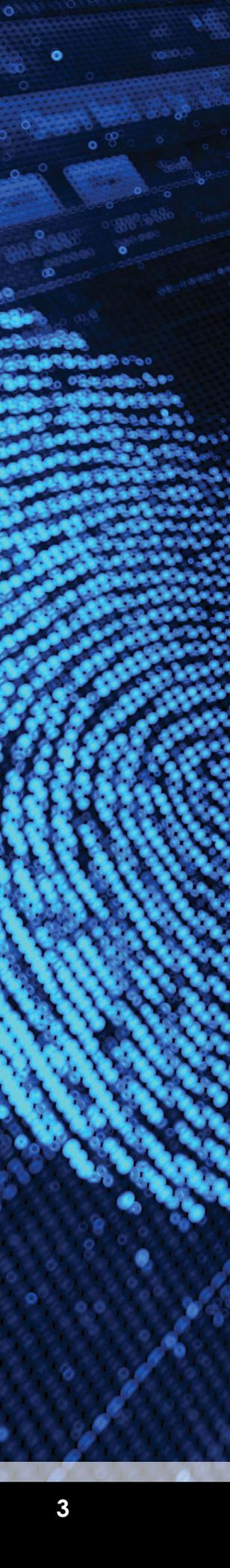
However, getting the right coverage isn't easy—and the stakes are high. Without proper coverage, a cyber breach can bring about financial ruin.

Certain aspects of cyber insurance policies are geared toward what many perceive to be traditional breach response obligations. However, other business dependencies must be carefully weighed—as exposures, coverage, and the language used to describe that coverage continually evolve.

We routinely say there is no “one-size-fits-all” approach to cyber coverage. Here are some considerations every agent needs to evaluate with their clients to make sure they aren't caught financially unprepared when a breach hits.

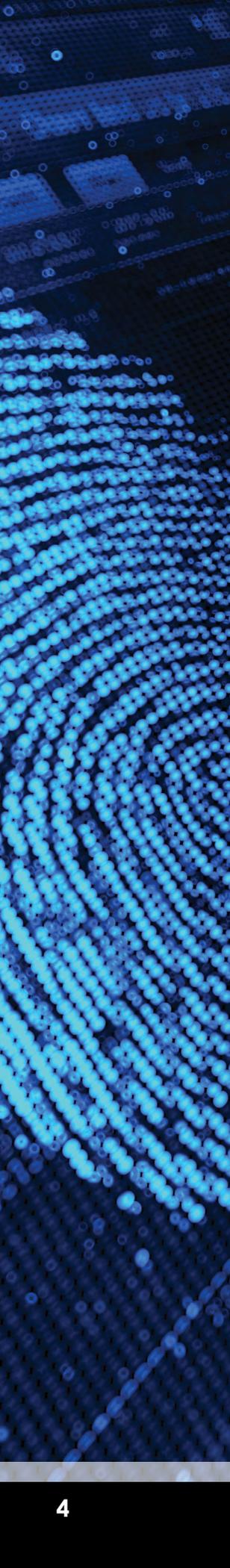
In the Event of a Data Breach

- ✓ How is “network” defined? Does the definition include outsourced providers? What about your outsourced provider's outsourced provider?

- 
- ✔ Is coverage written on a Full-Prior Acts basis? What happens if malware first starts to affect computers or systems during the policy period, but has been dormant for some time prior to the retroactive date?
 - ✔ Are there onerous “failure to patch” or “wear and tear” exclusions? “Failure to patch” refers to a company’s failure to install regular patches or system updates released by software and hardware manufacturers. Many policies exclude breaches if the insured hasn’t kept current with these updates, which are very easy to miss.
 - ✔ Are contractually-driven exposures considered? These may include non-disclosure agreements, Business Associate Agreements, PCI/Merchant Services Agreements, or other confidentiality agreements. Not all policy forms cover each type of data protection agreement completely and can be a severe shortfall in coverage.

When Dependent Revenue Is Affected

- ➔ Does the insured rely on a cloud or Software as a Service (SaaS) provider? Many businesses keep critical data on outside servers, paying monthly access fees to use software hosted in the cloud rather than developing an in-house system. For many companies, this is a more affordable way to get their enterprise software needs met, but it comes with



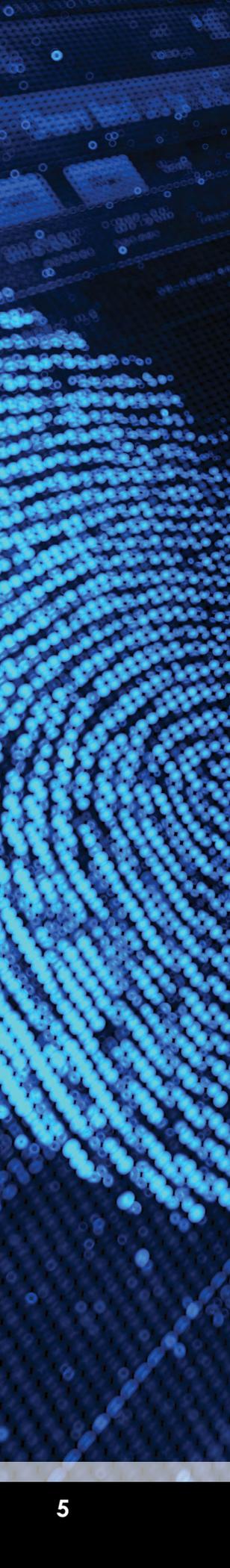
risks. For instance, if there is an outage in that provider's environment and your ability to generate revenue is affected, is this covered in the policy?

- ➔ When revenue is lost due to a system outage, how is coverage triggered? Is business income coverage exclusively triggered by a network security event, or will it kick in when a system glitch causes an outage?

There are a limited number of markets offering dependent business interruption and system failure coverage due to the aggregation issues it presents the carriers, but understanding the exposure and options for risk transfer is important for many types of businesses.

✓ **Cyber-Crime Coverage**

- ➔ Social engineering fraud: Is only funds-transfer coverage included, or is there coverage for funds lost to “social engineering” fraud? This type of fraud involves scammers sending what looks like a legitimate request for money or personal information, often using official-looking business logos and websites, manufactured email chains, and more to make their requests look authentic. Traditional funds transfer fraud may not cover situations where the insured has “voluntarily parted” with the funds because they were duped into doing so.
- ➔ Instances where clients fall susceptible to fraud: If your network is utilized to trick a client into sending funds to a hacker, are those funds covered? Does that coverage require the funds to be sent “to” a particular person, or are all transfers covered?



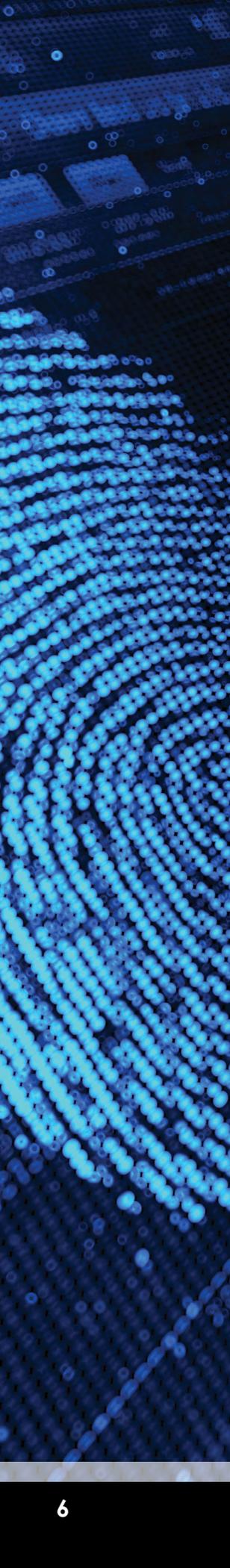
✓ E&O Considerations

- ➡ Ransomware: This type of fraud refers to malicious software that locks down a computer or system until a ransom is paid. The WannaCry attack was a recent, high-profile example. If the business suffers a ransomware or other network-interruption attack, can it still operate?
- ➡ Risk of third-party lawsuits for network interruptions: Would third parties be likely to sue if services were not performed due to the network outage?

The coverage afforded by the cyber marketplace is ever-evolving. Certain markets have pioneered unique solutions to address different network-based exposures that businesses face. The definitions and exclusions in a cyber insurance policy (or "cyber-light" coverage extension to another insurance policy) can greatly change the scope of coverage, and exposure to your client.

As a specialized wholesale broker, we strive to help you navigate these evolving risks and convey optional solutions to your clients.

The marketplace is rife with approaches to addressing these newer exposures, but the drastic variance in coverage language can easily leave pitfalls depending on the type of data breach, outage, malware attack or hack that a business experiences.



About Worldwide Facilities, LLC

Worldwide Facilities, LLC is a national wholesale broker and managing general agent providing services to insurance agents and brokers. In business since 1970, our seasoned team of brokers and underwriters offers specialized knowledge of cyber liability coverage, broad access to specialty markets, and extensive expertise in placing challenging insurance risks.

We offer unmatched tools, resources, and strategies to help insurance agents and brokers expand their corporate accounts to include cyber liability insurance—including training materials and marketing support.

Take advantage of our expertise in placing cyber risks today—contact Matt Donovan in our Dallas office at (615) 377-7687 or mdonovan@wwfi.com to schedule a conversation.

Disclaimer

This whitepaper is Copyright © 2017 by Worldwide Facilities, LLC. It may be freely redistributed in its entirety provided that this copyright notice is not removed. It may not be sold for profit or used in commercial documents without the written permission of the copyright holder. This whitepaper is provided “as is” without any express or implied warranty.

This whitepaper is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult with an attorney. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by Worldwide Facilities, LLC. The listing of an organization or website does not imply any sort of endorsement and Worldwide Facilities, LLC takes no responsibility for the products, tools, and Internet sites listed.

An aerial, top-down view of North America from space, showing the continent's topography and surrounding oceans. The image is set against a deep blue sky with a subtle light gradient.

HEADQUARTERS

725 S. Figueroa Street

19th Floor

Los Angeles, CA 90017

☎ (213) 236-4500

Visit wwfi.com for a full list of offices throughout the country.



Worldwide Facilities[®], LLC

“Experience a World of Difference”