Worldwide Facilities®, LLC

"Experience a World of Difference"

www.wwfi.com

Cyber Liability Insurance

NOT IF YOUR CUSTOMERS WILL NEED IT, **BUT WHEN**

WHITE PAPER

MAR 2016

Cyber Liability Insurance: Not If Your Customers Will Need It, But When

In February 2015, a data breach at Anthem put approximately 80 million customer and employee records in criminal hands.[1] In June, the records of as many as 22.1 million people were compromised in an attack on the US Office of Personnel Management—one of the largest hacks of a US government organization in history.[2] Just one month later, over 30 million accounts were exposed in a headline-grabbing attack on the infidelity dating site ashleymadison.com.[3]

And the hacks have continued. Throughout 2015 and into 2016, breaches at HSBC, Dow Jones, Hilton Hotels, and others further damaged public trust in companies' ability to protect their data. In early 2016, Wendy's began an investigation into fraudulent charges on customer credit cards after finding data-stealing malware on some of its systems.[4]

These events put millions of people at risk of identity theft, and incurred millions more in IT consulting, legal, and public relations costs to the targeted companies and organizations.

But data breaches don't just happen to global businesses. Any organization that stores its data digitally is a target, and as larger companies increasingly invest in cyber security, hackers are starting to focus their efforts on easier prey. Approximately 62% of cyber attack victims are small to mid-sized businesses.[5]

The costs of a data breach can be damaging to larger corporations—and ruinous to smaller ones. Cyber liability insurance is the only product that covers the financial fallout of these events. For insurance agents, this type of coverage represents a significant opportunity.

What Is Cyber Liability Insurance?

Cyber liability policies are specialty lines designed to provide the coverage most corporate policies don't offer when it comes to data breaches. These policies are usually tailored to the specific risks faced by individual insureds. Possible costs to be covered include:

- Emergency data breach response and crisis management.
- Legal expenses—including privacy legal consulting and defense.
- Regulatory fines and defense expenses.
- Network security and IT-related costs.
- Claims from 3rd-party vendors and suppliers.
- Class action claims by affected consumers.
- Customer notification, credit monitoring, and remediation costs.
- Website vandalization and defacement.
- Loss of business due to breach of public trust.
- Public relations expenses.
- Cyber extortion and ransom demands.
- Intellectual property infringement.
- Network downtime costs, including loss of business income due to downtime.

There is often overlap between cyber liability coverage and other corporate policies, such as crime coverage. But the damage caused by data breaches can be extremely broad, and no other type of corporate insurance covers all or even most of the cost. That's why this type of coverage is so essential to any organization with digital data and assets to protect.

Who Needs Cyber Liability Insurance?

When we think of data breaches, most of us think of high-profile events targeting large companies. And while it's true that big companies are obvious targets, small and mid-sized businesses are often even more vulnerable. Hackers are aware that smaller companies often don't have the resources to fully protect their data or investigate a breach.

This applies to companies and organizations across every industry. According to the Identity Theft Research Center's *2015 Data Breach Reports*,[6] the sectors that experienced the highest number of data breaches in 2015 were as follows:

- Business: 40%
- Health and medical: 35.5%
- Banking, credit and finance: 9.1%
- Government and military: 8.1%
- Education: 7.4%

These are not the only sectors at risk, however. There's a case to be made for this type of insurance in almost every organization and industry, both in the United States and abroad.

The law is also catching up. Currently 47 US states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have mandatory breach notification laws requiring companies to inform customers when their data has been compromised.[7] In Europe, the pending EU Data Protection Regulation[8] will impose a similar requirement.

No company subject to these laws can legally or ethically keep a data breach out of the public eye, which only compounds the damage to the company's bottom line and reputation. The expenses incurred—including legal, notification, public relations, IT forensics, loss of business, and erosion of public trust—can be

devastating. According to a 2015 report by Hewlett Packard and the Ponemon Institute of Cyber Crime[9], these events cost American companies an average of $15.4 million per year.

Overcoming Barriers to Cyber Liability Purchase

Demand is rising for cyber liability insurance. According to Hamburg-based statistical portal Statista, approximately 54% of global companies held cyber liability policies in 2014, and over 50% of companies without such coverage were considering making the purchase.[10]

However, there's still a lack of coverage, especially among smaller companies—approximately 97% of small businesses don't have cyber liability coverage.[11] Here are a few reasons why.

Cost of Coverage

Premiums are rising in the wake of high-profile attacks, but there's opportunity for insurance agents to guide their customers in reducing premium costs. Companies can reduce the cost of premiums by taking preemptive steps to mitigate risk, such as assessing their own specific risks and implementing a targeted IT security policy.

The Belief That Cyber Hacks Only Happen to Big Companies

The data has been clear in showing that small businesses are increasingly vulnerable. Three of the cyber threats facing small businesses include:

- Denial-of-service attacks. These involve overwhelming the victim's servers with data, crashing its website. A 2014 Incapsula survey[12] stated the average cost of such an attack can be as high as $500,000.

- Funds transfer fraud. Cyber criminals impersonate or hack into a CEO's email account and ask an employee to transfer funds. Banks will usually reimburse insureds with personal accounts, but not commercial accounts.[13]

- Ransomware. This malware locks up files and forces victims to pay a ransom for decryption. Small businesses are particularly vulnerable because they often don't have the security measures in place to defend against attacks or recover the files on their own.[14]

Lack of Familiarity Among Insurance Agents and Insureds

Understanding cyber liability insurance requires a combination of technical and specialized insurance expertise. Because of the relative newness of the product, insureds are often not fully aware of their options—and many insurance agents have not built up the expertise yet to proactively guide them.

Especially for agents and brokers who are new to the field, it's crucial to find a wholesale broker who can present to the insured, help them understand their options, consult with them to mitigate risk, and serve as a partner to new insurance agents in building credibility.

Choosing a Wholesale Insurance Broker for Cyber Liability Insurance

A wholesale insurance broker is essential in placing cyber liability risk, and can be an extremely valuable partner in presenting to insureds. But not every broker has the expertise to answer tough technical and financial questions from insureds. Here are some key deliverables to look for.

A Proposal That Identifies Your Insured's Pain Points

A good proposal will be able to pinpoint your insured's vulnerabilities right away, and identify appropriate coverage and limits based on evidence such as real-time data and examples of prior claims for similar businesses. It should take into account the following:

- Business plan
- E-commerce system
- Data collection practices
- Regulatory exposure
- Data security procedures
- Privacy policies
- PCI exposures
- Aggregate loss exposure

A Current Library of Claims

The wholesale broker should maintain a current library of claims examples for every industry—including that of your insured. This gives their team the ability to analyze risk exposure prior to an incident, provide expertise in marketing that risk to carriers, and get access to policies tailored to it.

Strong Relationships with Underwriters

The right broker should also maintain robust working relationships with underwriters who specialize in cyber liability, and have an in-depth understanding of which markets are best suited for insureds of specific classes. A broker who does a large volume of cyber submissions often gets priority with these underwriters.

Signs point to the likelihood that cyber liability insurance will become common corporate coverage for organizations of every size, in almost every industry. As cyber threats evolve, every sector will see the value in insurance agents who can help them navigate their coverage options and mitigate their risks.

Insurance agents who get into this market now will be perfectly placed to help their insureds protect themselves financially as cyber threats evolve.

Notes

[1] Abelson, Reed & Goldstein, Matthew. “Millions of Anthem Customers Targeted in Cyberattack.” *The New York Times*, February 5, 2015.

[2] Nakashima, Ellen. “Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say.” *The Washington Post,* July 9, 2015.

[3] Goodin, Dan. “Ashley Madison Hack is Not Only Real, It’s Worse Than We Thought.” *Ars Technica*, August 19, 2015.

[4] “Credit Unions Feeling Pinch in Wendy’s Breach.” KrebsonSecurity: http://krebsonsecurity.com/2016/03/credit-unions-feeling-pinch-in-wendys-breach/ (Accessed March 16, 2016).

[5] Donlon, Rosalie L. “Small, Mid-Sized Businesses Hit by 62% of All Cyberattacks.” *PropertyCasualy360*, May 27, 2015.

[6] “2015 Data Breaches.” Identity Theft Resource Center: http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html (Accessed March 7, 2016).

[7] “Security Breach Notification Laws.” National Conference of State Legislatures: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (Accessed March 7, 2016).

[8] “Reform of EU Data Protection Rules.” European Commission: http://ec.europa.eu/justice/data-protection/reform/index_en.htm (Accessed March 7, 2016).

[9] Griffiths, James. “Cybercrime Costs the Average US Firm $15.4 Million Per Year.” *CNN Money*, October 8, 2015.

[10] “Statistics and Facts on Cyber Insurance.” Statista.com: http://www.statista.com/topics/2445/cyber-insurance/ (accessed March 7, 2016).

[11] “Analysis Shows Less Than 3% of Small Businesses Have Cyber Liability Insurance.” Insureon: http://www.insureon.com/blog/post/2015/01/28/analysis-shows-less-than-3-percent-of-small-businesses-have-cyber-liability-insurance.aspx (accessed March 7, 2016).

[12] Incapsula Survey: “What DDoS Attacks Really Cost Businesses.” http://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20Impact%20Survey.pdf (accessed March 7, 2016).

[13] Ydstie, John. “When Cyberfraud Hits Businesses, Banks May Not Offer Protection.” NPR, September 15, 2015.

[14] Smith, Mark. “Huge Rise in Cyber Hacks as Cyber Criminals Target Small Businesses.” *The Guardian*, February 8, 2016.

About Worldwide Facilities, LLC

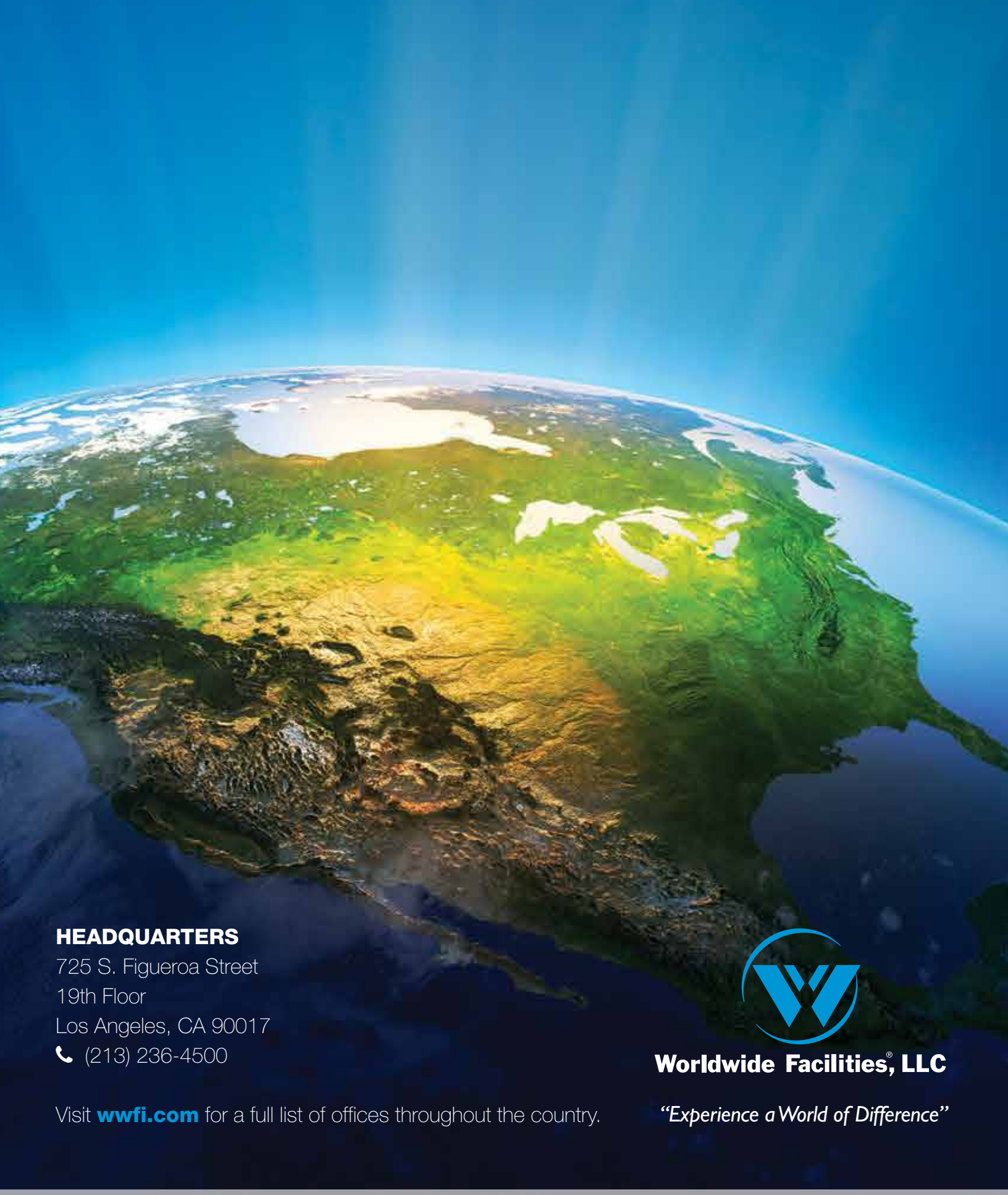
Worldwide Facilities, LLC is a national wholesale broker and managing general agent providing services to insurance agents and brokers. In business since 1970, our seasoned team of brokers and underwriters offers specialized knowledge of cyber liability coverage, broad access to specialty markets, and 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 Steve Vallone in our San Francisco office at svallone@wwfi.com or (415) 625-1277 to schedule a conversation.

Disclaimer

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.



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"