WHITE PAPER

CYBER COVERAGES

UNDERSTANDING POLICY TRENDS AND OPPORTUNITIES

IDT911

Protecting Identities. Enhancing Reputations.

IDT911 7580 N DOBSON RD, SUITE 201 · SCOTTSDALE, AZ 85256 | PHONE (480) 355 8500 · FAX (480) 355 8470 · WWW.IDT911.COM

1

DEFINITIONS

1. Cyber Coverage - Insurance coverage that focuses on services and systems related to technology and their use in business. Risks addressed include website and software design, network equipment, damage caused by service interruptions and computer viruses, and much of the work performed by technology vendors and consultants. Insureds are also commonly covered for damages if they inadvertently transfer a virus to a network owned or operated by someone else.

2. Data Breach Coverage - Often used interchangeably with Privacy Breach Coverage and/or Security Breach Coverage. Coverage that protects businesses in the event sensitive, protected data is compromised or exposed. Many policies also cover costs associated with first-party response and third-party liability exposures. ■

2

CARRIERS ARE CREATING AN ARRAY OF COVERAGE SOLUTIONS TO ADDRESS MOUNTING BUSINESS RISKS.

Misconceptions and myths about data breach, privacy, and cyber coverages abound. Insurers, brokers, and agents may be as confused as their clients, potentially putting businesses at risk if they believe they don't need crucial coverage, or if they think they have coverage when in reality they do not. By developing a more in-depth understanding of the latest insurance solutions, agents and clients alike will be in a better position to assess the options.

HISTORY OF CYBER AND PRIVACY BREACH COVERAGES

The first cyber coverage solutions appeared in the early 1990s, as technology began to play a larger role in daily life and the Internet was emerging as a viable business tool. Service interruption and website liability coverages were popular early options as businesses discovered the need for risk management and mitigation in a world that was increasingly reliant on technology. Websites evolved into active business platforms rather than just online placeholders, or the digital equivalent of billboards. With this evolution in the late '90s, the increase in the connections to consumers and other businesses grew exponentially. Coverages that spoke to network liability soon followed and became prominent, at least for larger companies and specialized online businesses.

In 2003, the first privacy breach notification legislation was passed in California, prompting a major leap into what we recognize today as privacy data breach coverage. More businesses recognized the need for first- and third-party coverages as they grappled with a wide range of new data protection issues and the risks associated with them. Breach notification obligations were being mandated at the state level. In addition, industry standards in the payment card sector and federal regulations in the form of HIPAA and HITECH brought more stringent compliance requirements as well.

The expanding scope of risks businesses face today has prompted carriers to create a broader array of coverage solutions. These new options are designed to more fully address not only the conventional issues of doing business online, but also the dangers surrounding consumer data breaches and cyber business interruption as well as emerging threats such as data ransom and cyber extortion.

Unfortunately, while there may be more variety in the coverage options available to businesses, less than half of carriers currently offer cyber policies, though a majority indicated they plan to offer some form of cyber coverage in 2015[1]. And in spite of the near-constant media attention to

1 Cyber Insurance Survey, ISO, Nov. 2014

3

THERE ARE SIGNIFICANT DIFFERENCES BETWEEN CYBER AND PRIVACY BREACH COVERAGES.

major data breaches, there continues to be a misperception–or perhaps it's apathy–among business owners that they don't need coverage for cyber or breach risks, or that their current umbrella policy already includes this type of coverage. Even among insurers surveyed by A.M. Best, more than half said they don't purchase cyber coverage for their own businesses [2]. The insurance industry has an opportunity here to lead by example in its drive to increase customer awareness of the very real need for cyber coverage. This must remain the number one priority for producers.

With big breaches dominating headlines, more business owners are looking for ways to move from fear to action. They are increasingly acknowledging the need for cyber coverage and want help determining their needs, but many don't know where to turn, especially if their broker isn't familiar with or doesn't offer cyber policies. The need is there. How can the industry better drive demand? The answer: Education. Today's environment has created a prime opportunity for insurance companies to market and sell cyber risk programs much more effectively by creating a solid foundation of knowledge for producers and clients.

Education and awareness of risks and mitigation best practices are key to proactive protection. Policyholders have the tools available to significantly improve their security posture and reduce their risk of a breach, but identifying and implementing effective measures requires they have a better understanding of today's cyber threat environment. Insurers also must have top-tier knowledge available to help guide clients toward the right solution.

The evolution from narrowly focused coverage to coverage that addresses multiple risks in interrelated areas is one reason behind the confusion felt by businesses and producers. Knowing which risks a particular company faces and how best to mitigate them isn't nearly as straightforward as it was even five years ago. Current thought leadership and insight into the evolving world of best practices from experts in the cyber coverage realm is crucial to marrying risks with appropriate mitigation strategies

UNDERSTANDING POLICY TYPES AND COVERAGES

The terms "cyber" and "privacy breach" are often used interchangeably when referring to the policies available, but there are significant differences between them.

2 A.M. Best Fall 2014 Insurance Industry Survey

4

BIG FIRMS ARE AT HIGHER RISK FOR CYBER EXPOSURE; SMBS FOR PRIVACY BREACH RISK.

Cyber coverage typically focuses on services and systems related to technology, and their use in business. Risks addressed include website and software design, network equipment, damage caused by service interruptions and computer viruses, and much of the work performed by technology vendors and consultants. Insureds are also commonly covered for damages if they inadvertently transfer a virus to a network owned or operated by someone else.

Privacy breach coverage protects businesses in the event customer, consumer or patient data is compromised or exposed. Also covered under many policies are costs associated with first-party response costs and third-party liability exposures.

First-party coverage provides for legal expenses associated with regulatory compliance, such as state breach notification regulations, federal healthcare mandates including HIPAA and HITECH, and financial industry regulations including contractual agreements surrounding PCI compliance. It also covers expenditures incurred as part of any forensic investigations into the duration and extent of exposures to determine specifically what data was compromised and who was impacted. The costs to respond to a breach, to notify affected parties and any applicable regulatory agencies, and to provide victims (and potential victims) with credit monitoring tools and identity theft remediation services are further benefits of first-party coverage.

Third-party coverage focuses on liability costs related to defending against consumer-based litigation or regulatory actions that arise as a result of a breach. The majority of these risks are significantly reduced–if not eliminated–by appropriate use of first-party coverage.

The way policies are currently being offered and written is also notable. Only 57 percent of companies that write cyber risk write dedicated policies. More often, cyber is bundled with existing policies, notably general liability, property and business interruption, and E&O. This general reluctance to participate in the cyber market is dominated by insurers' concerns about a lack of data surrounding cyber policies and claims[3]. Launching in 2015, ISO's data breach policy and claim data sharing program–part of the organization's cyber risk platform–will begin to address much of the existing data scarcity.

3 A.M. Best Fall 2014 Insurance Industry Survey

5

MARKET STRATEGIES VARY DEPENDING ON BUSINESS SIZE AND INDUSTRY.

MARKET PROFILE: LARGE COMPANIES

The nature of a big company and its way of doing business means that they commonly need strong privacy breach and cyber coverage. A vast number of them gather, process and store large amounts of information, and they also typically have complex technology and network infrastructures supporting their operations. These companies often deploy and manage much of the underpinnings that drive wider activities, such as the processing of financial transactions and the compilation and analysis of large databases.

Systems within the infrastructures of Fortune 1000 and similar companies usually have many connections to outside partners, such as suppliers and client organizations. Cloud computing is also heavily leveraged for core computing functions, and the extensive use of external vendors also leads many big businesses to allow network access to companies and people outside their own workforce.

These factors put the typical large company at risk for cyber exposure. Privacy breach risks, on the other hand, are often managed through the proactive policy making and robust security measures available to big firms that have sufficient funding and ample internal resources.

MARKET PROFILE: SMBS

In contrast to large organizations, the majority of small and midsized businesses don't often run the same levels of risk when it comes to cyber exposure. They may have their own internal systems while only occasionally providing services to other companies or using their networks for extensive connected activities. And they may rely on cloud technology regularly, but its use within the organization is typically limited.

SMBs do, however, often have higher privacy breach risk. Most don't employ data protection experts or large technology teams, making the information they collect and manage potentially more vulnerable to exposure. They're also less likely to implement strict data retention policies, they may not be familiar with the safest ways to store and dispose of information, and in some instances they may be unaware that they're subject to state, federal, or industry compliance regulations. In addition, non-digital breach causes remain a top-tier risk among small and midsize businesses (SMB). Mailing hard-copy invoices and patient statements to the wrong address, for example, or improperly disposing of obsolete paper files, may pose as great a breach risk as any electronic network intrusion.

Breach impacts in the SMB sector have the potential to inflict significant damage. Ongoing customer concerns about data privacy and exposure was

6

CYBER AND PRIVACY BREACH COVERAGES ARE ESSENTIAL FOR BUSINESSES OF ALL SIZES.

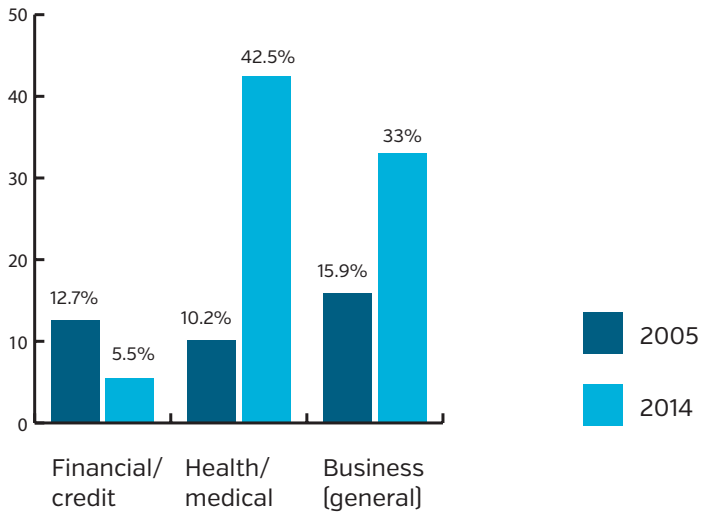
shown to have a measurable impact on the bottom line in the case of the Target breach. Couple that lost revenue with the costs necessary to respond to a security incident–from investigative services that determine the extent of an exposure to litigation brought by affected parties–and a breach has the very real potential to threaten a small company's financial health. In stark contrast to the big business sector, an SMB breach and resulting costs typically aren't as easily absorbed as they might be with companies like Target and Home Depot. Business continuity and long-term viability are of serious concern.

SPECIFIC NEEDS

A subset of firms both large and small have risk profiles shaped by more than just their size. Companies that operate in specific industries–healthcare, legal, and financial to name a few–often require more robust privacy breach coverage. These businesses are responsible for managing the most sensitive information types, and exposure of that data could lead those impacted to suffer significant harm. Whether it's a large hospital organization or an individual doctor's office, a nationwide law firm or a small-town attorney, these companies have valuable and highly confidential information that is actively sought by hackers and that the businesses must vigorously strive to protect.

A review of breach statistics over the past decade shows trends within several key industries:

Breaches by industry – 2005 – 2014



Source: ITRC Breach Statistics 2005-2014

7

GREATER AWARENESS FOR CYBER AND PRIVACY BREACH COVERAGE SOLUTIONS DRIVES DEMAND FOR POLICIES IN ALL BUSINESS SECTORS.

This data demonstrates that the financial and credit sectors may be preventing exposures more successfully now than in years past, but the healthcare and general business industries have experienced a worrying uptick in breach events.

MARKET STRATEGIES

The market needs for both cyber and privacy breach coverage solutions are specific to the size of the business being considered as well as industry or other risk factors that may be present.

Big companies generally have a number of other insurance products in their portfolios, and cyber risk coverage will often naturally dovetail with existing initiatives overseen by the organization's risk management group. It's likely that these internal teams already have identified where potential liabilities lurk and what can be done to mitigate them. And while large firms regularly absorb significant levels of risk internally for financial reasons, most have also accepted sizable insurance premiums as a normal cost of doing business.

Contrast that to the small company sector, which has been largely overlooked in the past as a segment of the marketplace that was either uninterested or unable to secure robust coverage. But many SMBs, and particularly those in the high-risk categories related to the healthcare, financial, and legal industries, often benefit from highly targeted and carefully underwritten policies. Keep in mind that, regardless of their risk profile, most SMBs are likely to be much more price-sensitive than larger firms, as they often have far less budget available to cover high premiums. However, small companies are often receptive to the concept of add-on coverages to the commercial package or business owners' policies they already have.

In all business sectors, increased awareness of the need for cyber and data breach coverage drives greater demand for these types of policies. However, there is still a significant lack of awareness among potential clients that cyber coverage is something they should have. In fact, companies that don't believe they need cyber insurance is cited as the greatest selling challenge by 40 percent of producers in a recent study conducted by Hanover Research[4]. Opportunities for increased revenue will follow when businesses understand the critical need for breach coverage and how accessible effective coverage options are to organizations of any size.

4 Cyber Insurance Survey, ISO, Nov. 2014

8

A SOLID UNDERSTANDING OF CYBER AND PRIVACY BREACH COVERAGES CAN HELP PRODUCERS BUILD PROFITABLE, RISK-AVERSE SOLUTIONS TO SUPPORT INSUREDS AND CREATE REVENUE POTENTIAL.

In addition, SMBs rarely have internal legal or risk management resources that can help them navigate through their firm's specific areas of risk. Small business operators may not be familiar with their existing insurance products or they may misunderstand what the various coverage solutions offers. Producers who present cyber- and privacy breach coverage options to smaller firms must have a thorough understanding of the coverages and be able to provide guidance on where liabilities exist or where their present policies may have gaps.

SUMMARY

Though technology touches nearly every aspect of business in today's environment, cyber and privacy breach coverage solutions extend far beyond hacking incidents. Even low-tech businesses and non-digital data face breach risks, such as when a small construction firm loses its personnel files in an office break-in. The need for breach coverage is becoming a far more crucial offering for clients as well as the producers and carriers who serve them.

Education has become a critical tool for agents and brokers, with a number of support options available to ensure that the advantages of the various coverage solutions are clear. With a good understanding of the coverages available, producers can build a profitable risk-averse breach coverage that properly supports their insureds and provides increased revenue opportunities. ■