Benchmarking Trends: As Cyber Concerns Broaden, Insurance Purchases Rise

Cyber-attacks are escalating in their frequency and intensity, and pose a growing threat to the business community as well as the national security of countries. High-profile cyber incidents in 2014 reflected the expanding spectrum of cyber threats — from point-of-sale (POS) breaches against customer accounts to targeted denial-of-service (DoS) attacks meant to disable a company's network. Insureds in ever-larger numbers sought financial protection through insurance, buying coverage for losses from data breaches and due to business outages. In 2014, the number of US-based Marsh clients purchasing standalone cyber insurance increased 32% over 2013 (see **FIGURE 1**). The cyber take-up rate — the percentage of existing Marsh financial and professional liability clients that purchased cyber insurance — rose to 16%. Early evidence in 2015 shows a continued acceleration in the demand for cyber insurance.

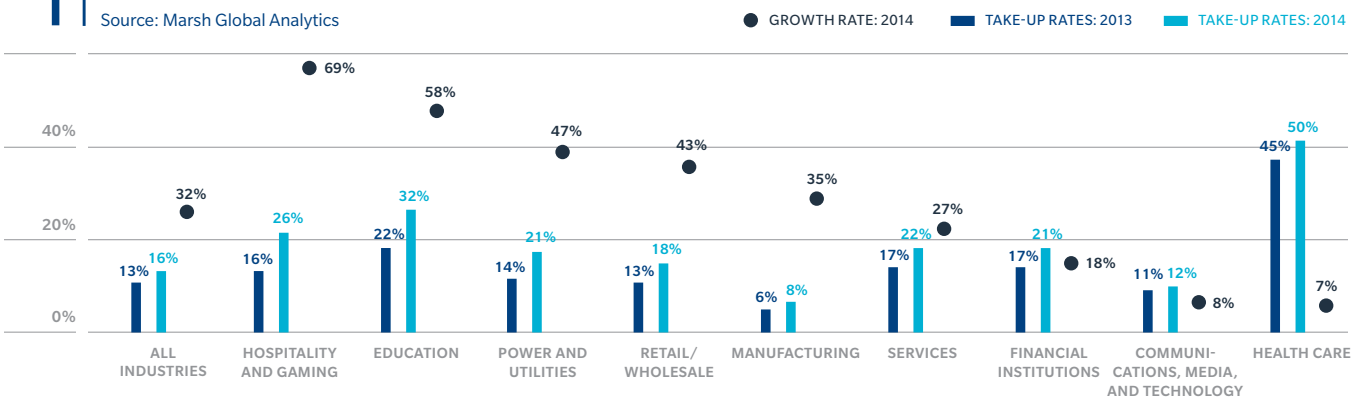
BOOST IN CYBER INSURANCE DEMAND DRIVES INSURERS' RESPONSE

Health care facilities, universities, and schools continue to be on cybercriminals' radar, but attacks in the hospitality and gaming, power and utilities, and other sectors, reveal that no organization is immune to a cyber-attack or failure of technology. Health care and education clients had the highest cyber insurance take-up rates in 2014 at 50% and 32%, respectively, followed by hospitality and gaming (26%) and services (22%). Universities and schools present attractive targets because they house a vast array of personal information of students, parents, employees, alumni, and others: Social Security numbers, health care information, financial data, and research papers can all be compromised.

The broader scope of hacktivists contributed to the increase in cyber insurance purchases in 2014. Sectors that again showed notable year-over-year increases in the number of clients purchasing cyber coverage included hospitality

FIGURE 1 | **CYBER INSURANCE TAKE-UP AND GROWTH RATES BY INDUSTRY**

Source: Marsh Global Analytics



In the above chart, "growth rate" refers to the percentage increase from 2013 to 2014 in the number of clients purchasing standalone cyber insurance. "Take-up rate" refers to the overall percentage of clients that purchased standalone cyber insurance.

and gaming (69%) and education (58%). Other areas that stood out in 2014 included the power and utilities sector, with 47% more clients buying standalone cyber coverage. Power and utilities companies frequently cite the risks and vulnerabilities associated with the use of supervisory control and data acquisition (SCADA) networks — which control remote equipment — and the cost of regulatory investigations as driving factors behind their cyber coverage purchases.

The reasons for purchasing cyber coverage varied — from board-mandates protecting reputations to mitigating potential revenue loss from cyber-induced interruptions of operations. Insurers responded to this demand by offering broader cyber insurance coverage in 2014, including coverage for contingent business interruption (CBI) and cyber-induced bodily injury and property damages. They also expanded availability of loss-control services, including risk assessment tools, breach counseling, and event response assistance.

CYBER LIMITS RISE

Companies with revenue exceeding $1 billion purchased 22% higher cyber insurance limits on average in 2014 at $34.1 million compared to $27.8 million in 2013 (see **FIGURE 2**). Among these large firms, financial institutions again purchased the highest average limits, followed by power and utilities firms and communications, media, and technology companies.

Looking at firms of all sizes, power and utilities companies witnessed the sharpest percentage increase in average limits, at 59% (see **FIGURE 3**). All industries in this group purchased more cyber insurance limits on average in 2014 than in 2013.

FIGURE 2 | **CYBER LIABILITY TOTAL LIMITS PURCHASED (COMPANIES WITH REVENUE OF $1 BILLION+)**

Source: Marsh Global Analytics

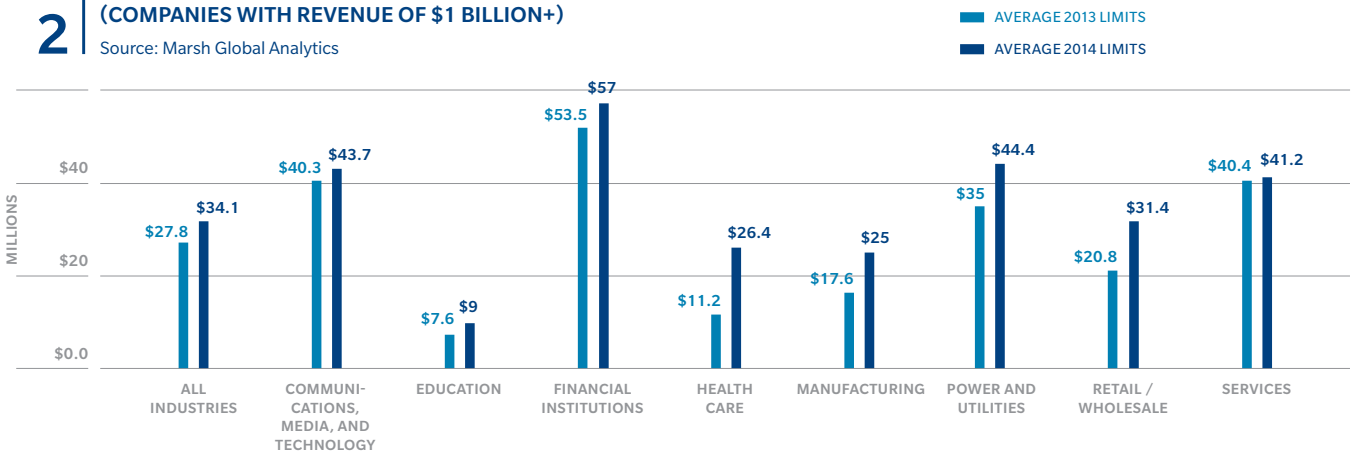
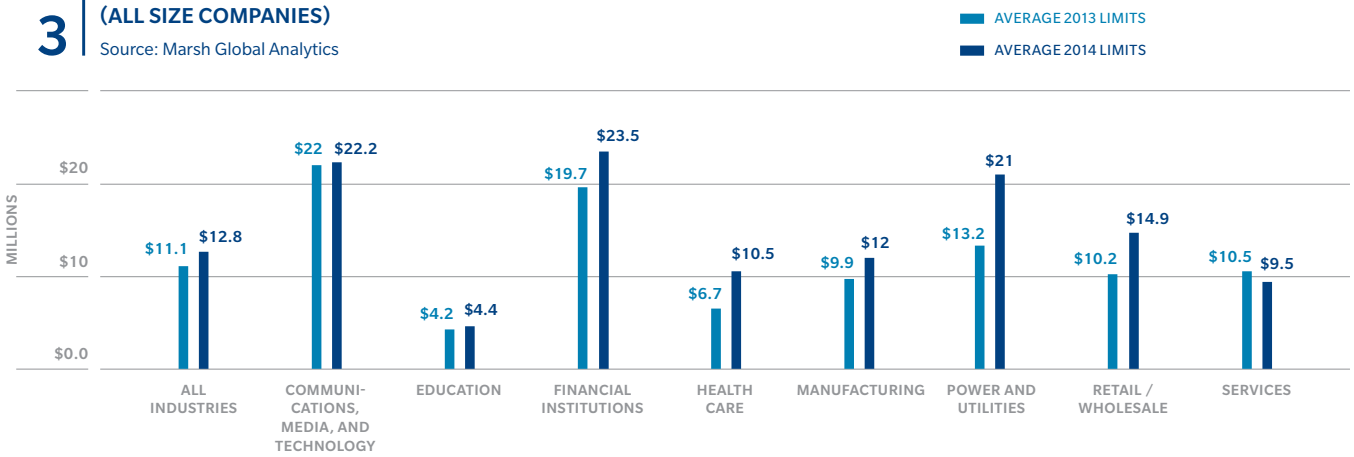


FIGURE 3 | **CYBER LIABILITY TOTAL LIMITS PURCHASED (ALL SIZE COMPANIES)**

Source: Marsh Global Analytics



CYBER RATES AND COVERAGE

Increases in the frequency and severity of losses and near-constant headlines about attacks and outages kept cyber insurance premiums generally volatile in 2014. Average rate increases at renewal for both primary layers and total programs were lower in the fourth quarter than in the first (see **FIGURE 4**). The increased loss activity prompted pricing challenges for some insureds, particularly retailers, where renewal rates rose on average 5% and as much as 10% for some clients.

Market capacity also varied according to industry. Most industries were able to secure cyber coverage with aggregate limits in excess of $200 million, while the most targeted industries, like retailers and financial institutions, faced a challenging market.

Insureds also face heightened due diligence from underwriters seeking to drill down beyond simple reviews of the company's general information security policies. For example, insureds in the retail sector are being asked about their deployment of encryption and EMV (credit card) technology. And all insureds are now routinely asked whether they have formal incident response plans in place that outline procedures for protecting data and vendor networks and, more importantly, if such plans have been tested.

A GROWING CONCERN

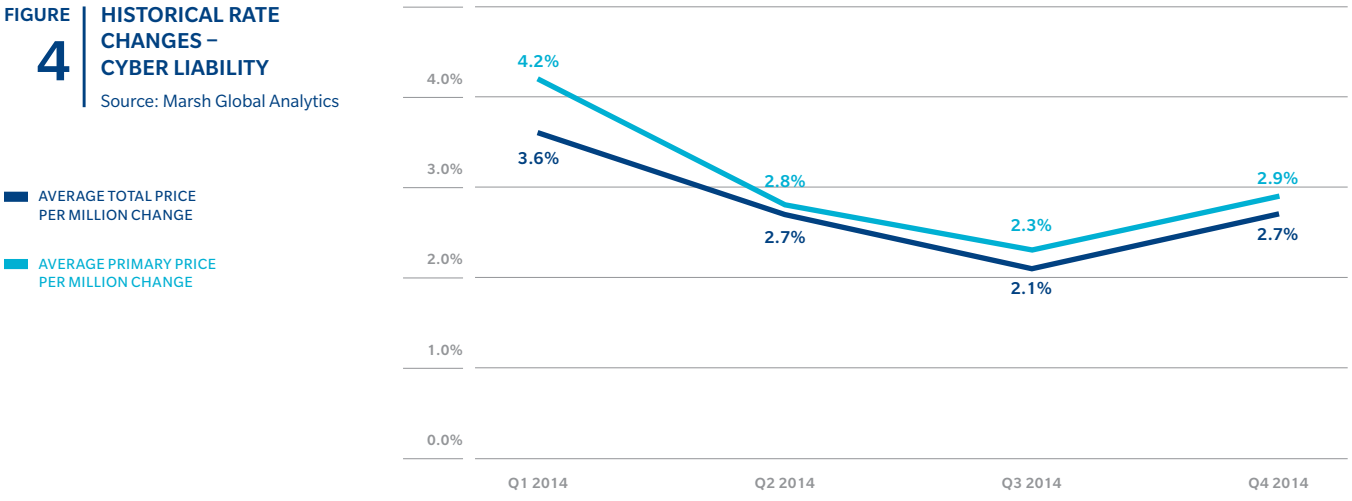
In 2015, managing cyber risk is clearly a top priority for organizations. For example, business interruption (BI) drew a lot of attention in 2014, a trend likely to continue throughout 2015. While BI has historically been thought of as the aftereffect of a critical system going down for an extended period of time, technology failures and cyber-attacks can create far-reaching outages affecting secondary systems, clients, and even vendors. Such events can also lead to higher recovery costs, which are becoming a concern for boards of directors and senior management.

There is also concern stemming from the expansion of regulation and litigation. Regulators were active in policing cyber risks in 2014, and oversight is likely to expand significantly in coming years. With cyber risk seen as a critical issue on both sides of the aisle in Washington, D.C., companies will face regulatory challenges in 2015 and beyond. Sectors that have already seen significant regulatory activity — for example, health care, financial services, and education — will likely face more stringent regulations and larger fines. All industries should pay attention to existing and impending regulations, tighten controls, and prepare to present and defend their compliance regime. Civil litigation in the wake of a breach or disclosure of a cyber event also escalated in 2014, with class-actions at times following the disclosure of a breach by mere hours.

As demand for cyber insurance grows, it's important to remember that risk transfer is only part of the solution. Enhanced information sharing between industry and government is another step toward having a comprehensive risk mitigation strategy. Insurers and brokers are expanding the availability of loss-prevention and risk mitigation services such as risk assessment tools, breach preparation counseling, and breach response assistance. The expanded roster of services and enhanced coverage can provide additional value from policies, usually without a specific added premium.

FIGURE 4 | **HISTORICAL RATE CHANGES – CYBER LIABILITY**

Source: Marsh Global Analytics



ABOUT THIS BRIEFING

This report was prepared by Marsh's Cyber Practice within Marsh's US FINPRO division, which specializes in financial and professional risk solutions. Companies should consult with their Marsh risk advisors to identify their most prevalent cyber risks and to explore the services that can best align insurance solutions with their exposures. This report was prepared in conjunction with Marsh Global Analytics — Placement Data Analytics, which provides purchasing patterns and pricing behavior analytics to Marsh clients and the insurance industry.

ABOUT CYBER IDEAL

Marsh's Cyber IDEAL Model, which stands for Identify Damages, Evaluate, and Assess Limits, quantifies the potential for an unauthorized cyber disclosure. Using US historical breach information dating back to 2005, the model determines the frequency and severity of cyber incidents using a one-year probability of a data-breach event.

ABOUT MARSH

Marsh is a global leader in insurance broking and risk management. Marsh helps clients succeed by defining, designing, and delivering innovative industry-specific solutions that help them effectively manage risk. Marsh's approximately 27,000 colleagues work together to serve clients in more than 130 countries. Marsh is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), a global professional services firm offering clients advice and solutions in the areas of risk, strategy, and people. With 57,000 colleagues worldwide and annual revenue exceeding US$13 billion, Marsh & McLennan Companies is also the parent company of Guy Carpenter, a global leader in providing risk and reinsurance intermediary services; Mercer, a global leader in talent, health, retirement, and investment consulting; and Oliver Wyman, a global leader in management consulting. Follow Marsh on Twitter @MarshGlobal, or on LinkedIn, Facebook, and YouTube.

For more information, contact:

THOMAS REAGAN
Cyber Practice Leader
thomas.reagan@marsh.com
+ 1 212 345 9452

ROBERT PARISI
Cyber Product Leader
robert.parisi@marsh.com
+1 212 345 5924