Benchmarking Trends: Cyber-Attacks Drive Insurance Purchases For New and Existing Buyers

The number of US-based Marsh clients purchasing standalone cyber insurance increased 32% in the first half of 2015 compared to the first half of 2014 (see FIGURE 1). The all-industry cyber take-up rate — the percentage of existing Marsh financial and professional liability clients that purchased cyber insurance — increased 25% in the first half of 2015 compared to the same period in 2014. Many existing buyers looked to increase limits — at times doubling their expiring limits. Pricing generally increased, particularly for companies in industries that have been hard-hit by cyber losses.

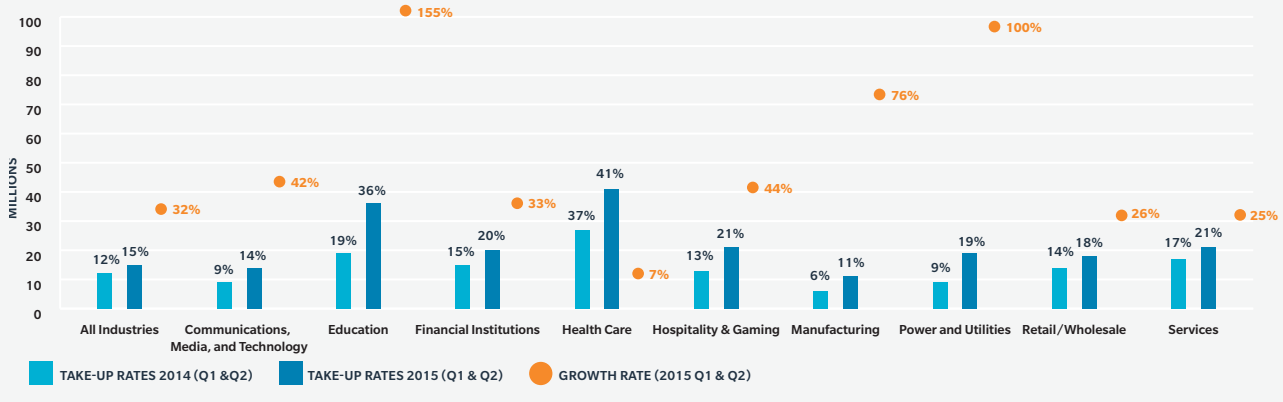
The reasons for purchasing cyber insurance varied, and included filling gaps in traditional coverage, lessening financial harm, mitigating reputational damage, and covering costs associated with class-action lawsuits.

EDUCATION, HEALTH CARE AND OTHER SECTORS INVEST IN CYBER INSURANCE

Universities, health care organizations, retailers, and financial institutions purchased cyber insurance due to their data breach exposures, though companies in other sectors also showed high growth and take-up rates for purchasing cyber insurance in the first half of 2015 compared to last year at this time. Power and utility companies, for example, more than doubled their take-up rates during this time period. The sector's growth rate increased 100%.

Universities and other organizations in the education sector saw almost a 90% change in cyber insurance

FIGURE 1: Cyber Insurance Take-Up and Growth Rates by Industry: First Half of 2014 vs First Half of 2015
Source: Marsh Global Analytics (Marsh Clients)



take-up rates in the first half of 2015 compared to the first half of 2014. The sector's cyber insurance growth rate surged to 155% during this time period. School settings are ripe for cyber-attacks due to the hefty amount of student and staff personal information that is stored in a variety of places.

Health care organizations had the highest take-up rates by sector in the first half of 2015, at 41%, which is up from 37% at the end of the first half of 2014. Given the amount of patient data and other physician, health plan, acute care system, and employee information that flows through health care organizations, this sector is highly targeted by cyber criminals. Shared system data exposures and the threat of false claim submissions are among the reasons this group has upped its cyber insurance purchases.

Companies in the hospitality and gaming and financial sectors all witnessed between a 5% to 8% increase in cyber insurance purchases in the first half of 2015 over last year in the same time, at 21% and 20%, respectively. The abundance of personal data collected by these industries – and the many avenues through which data can be accessed, including mobile phones, kiosks, and apps – escalated their risk profile.

Though financial institutions are already on guard against a barrage of cyber-attacks on their networks, rating agencies have also weighed in. Standard & Poor's, for one, provided an added warning to banks that they run the risk of a credit rating downgrade due to lack of preparation for cyber incidents. The agency is questioning, in particular, whether banks have cyber insurance policies.

The consequences of not heeding cybersecurity risks to organizations, their stakeholders, and customers have also grown larger. Marsh's proprietary Cyber IDEAL (identify damages, evaluate, and assess limits) model puts the cost of 1.7 million payment card industry (PCI) records at almost $30 million, according to Marsh Global Analytics.

CYBER LIMITS RISE

Communications, media, and technology (CMT) companies with revenue exceeding $1 billion purchased almost 50% more cyber insurance limits on average in the first half of 2015, at $55.8 million, compared to $38 million in the first half of 2014 (see FIGURE 2). CMT cyber insurance limits buying surpassed that of financial institutions in that same revenue band. Attacks on CMT networks have grown in intensity and sophistication, prompting renewed interest in purchasing cyber insurance.

Looking at all industries, cyber insurance limits purchasing averaged $30.4 million at the end of the second quarter 2015, just slightly higher than the first half of 2014.

Taking into account companies of all sizes, the CMT sector was also notable, coming in second among all industries in the second half of 2015 at an average of $18.1 million in cyber insurance limits purchased (see FIGURE 3). It was surpassed only by the financial institutions sector, which purchased an average of $21.6 million in cyber limits during this time and was closely followed by power and utilities at $17.2 million.

RESPONSE TO HIGH-PROFILE LOSSES

The insurance market's response to cyber losses in the first half of 2015 was reflected in the structure and pricing of cyber programs — those particularly hard hit by cyber criminals, such as the retail sector, saw average price increases on cyber insurance of 32%. This compares to an average price increase of 19% for all other industries. The health care sector has experienced similar

FIGURE 2: Cyber Liability Total Limits Purchased (Companies With Revenue of $1 Billion+)
Source: Marsh Global Analytics

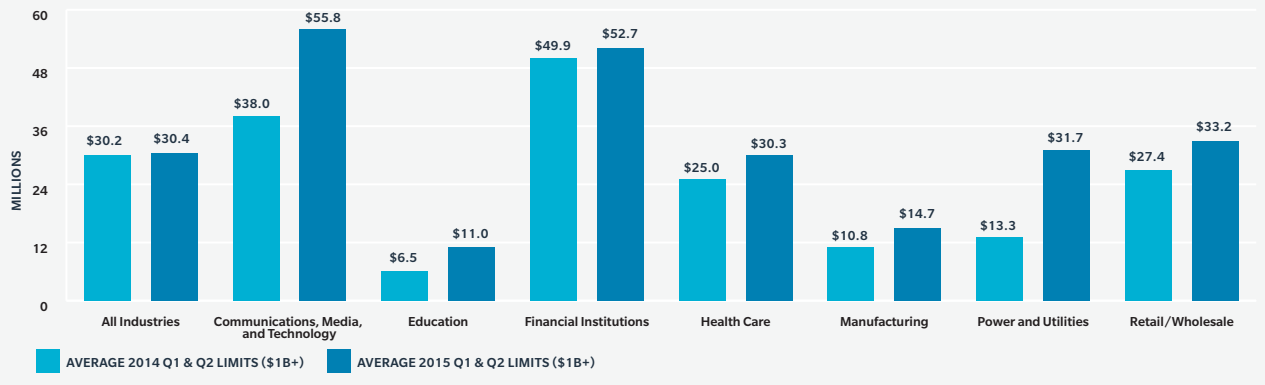
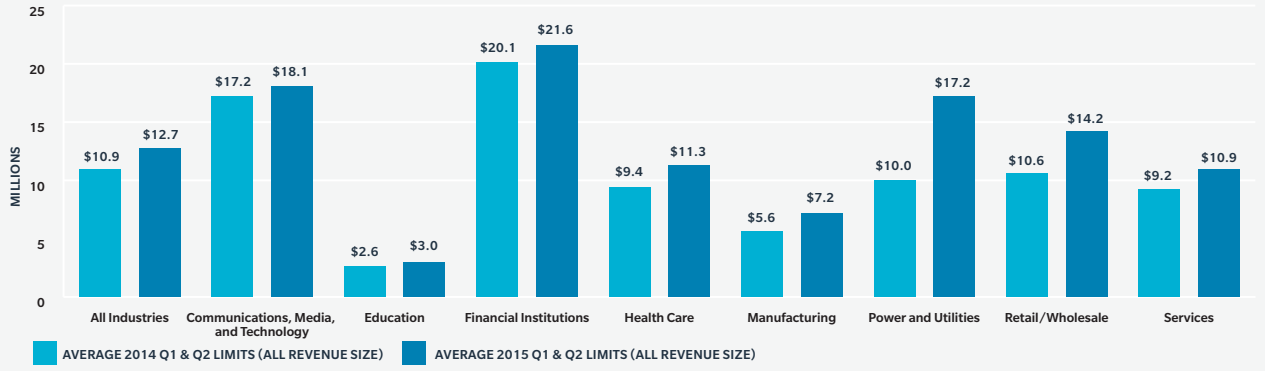


FIGURE 3: Cyber Liability Total Limits Purchased (All Companies)
Source: Marsh Global Analytics



changes to program structure and pricing related to cyber as in the retail space, particularly in the managed care area.

Average rate increases at renewal for both primary layers and total programs rose by double digits in the first half of 2015 at 16.1% and 20%, respectively (See FIGURE 4), with rates easing off somewhat in the second quarter compared to the first.

Overall capacity in the marketplace remains abundant at $500 million, although some industries continue to face challenges. Many clients are exploring renewal options with sublimits, and others are seeking specific policy requests related to cyber.

LOOKING AHEAD

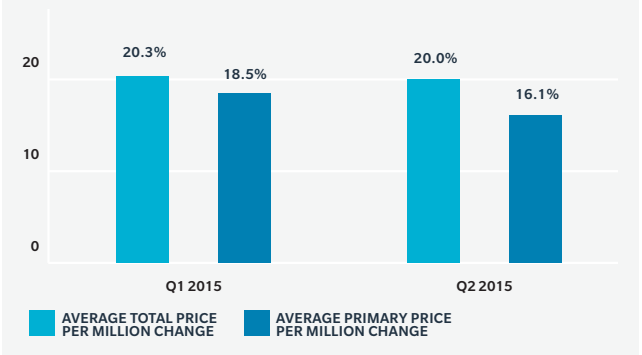
Recent high-profile cyber losses have proven to insureds that they need to alter their approach to cyber risk management from one that focuses primarily on prevention to a comprehensive strategy across the enterprise that involves assessing, managing, and responding to cyber risks. The more corporate leadership views cyber risk as an enterprise-wide concern and not just an IT problem, the more effective its risk management program will become.

Almost all companies have put in place some preventive strategies, such as incident response plans. Universities, for example, have instituted two-factor authentication processes, which help to secure login information. But organizations need to do more than simply patch holes they see in their cybersecurity; they need to assess their cyber risks, determine how they would respond to cyber threats, and evaluate how they would react in case of an actual cyber event.

How proactive organizations are against cyber incidents matters. Regulators continue to step up enforcement actions against companies that do not have cyber mitigation measures, such as cyber insurance, in place. A recent example is the Securities and Exchange Commission charging an investment adviser in September 2015 over failing to conduct periodic risk assessments, employ firewalls, and protect web servers that contain personally identifiable information (PII). Similarly, insurance regulators and federal officials met at the Treasury Department in April regarding best practices for cybersecurity.

According to network security firm FireEye, as soon as organizations' defenses evolve, attackers adapt and innovate. In its *M-Trends 2015: A View From The Front Lines* report, FireEye noted that organizations in 2014 learned of breaches sooner than they did in 2013, yet attackers still roamed undetected in breached environments far too long (a median of 205 days versus 229 days, respectively). In addition, FireEye observed new and emerging techniques at each stage of the attack lifecycle.

FIGURE 4: Historical Rate (Price Per Million) 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. The 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 MARSH'S CYBER RISK MANAGEMENT FRAMEWORK

Marsh's proprietary **Cyber Risk Management Framework** helps to identify and define risks based on organizations' assets and risk profile, better manage the threats, and respond in the event of a cyber event. We can help define risks, design an improved risk management program, and deliver a mix of services to better protect a company against cyber incidents.

ABOUT MARSH CYBER PRACTICE

Marsh's Cyber Practice, within the Financial and Professional liability division known as FINPRO, offers unparalleled resources in cyber advisory and risk transfer solutions. With industry know-how spanning decades, our Cyber Practice is able to help clients effectively assess, manage, and respond to cyber threats and events. We provide the full gamut of advisory services across diverse areas of cybersecurity ranging from risk analysis and threat intelligence to incident response. In collaborating with Marsh Global Analytics, Marsh has brought a suite of analytical solutions to market, including Cyber IDEAL, designed to identify damages, evaluate, and assess limits.

For more information on this report, contact your Marsh representative or:

THOMAS REAGAN

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

ROBERT PARISI

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