MARCH 2019

More Cyber Insurance Buyers as Awareness Grows

In the wake of several high-profile cyber-attacks and losses in recent years, and with their increasing reliance on technology, organizations are recognizing the need to view cyber as a critical enterprise risk and to understand the scope and value of their cyber risk exposures. No longer considered solely the domain of technology teams, cyber risk is now a regular area of focus in the boardroom.

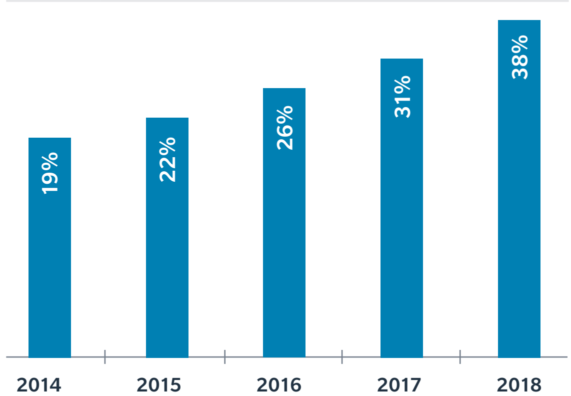
Companies Without Significant Privacy Risk Buying Coverage

Over the last five years, the number of Marsh US clients purchasing cyber insurance has doubled, from 19% in 2014 to 38% in 2018 (see Figure 1). As risk awareness has grown, cyber insurance products have evolved to address a variety of privacy and operational exposures, making coverage more attractive to buyers in a broader set of industries.

In 2018, the leading buyers of cyber insurance were organizations in industries that make significant use of personally identifiable information (PII) and protected health information (PHI), which have traditionally been viewed as the primary source of cyber risk for businesses. Education and health care led the way, with purchase rates of more than 60%, followed by hospitality and gaming (see Figure 2).

FIGURE 1 Cyber insurance take-up rates have doubled since 2014

SOURCE: MARSH PLACEMAP

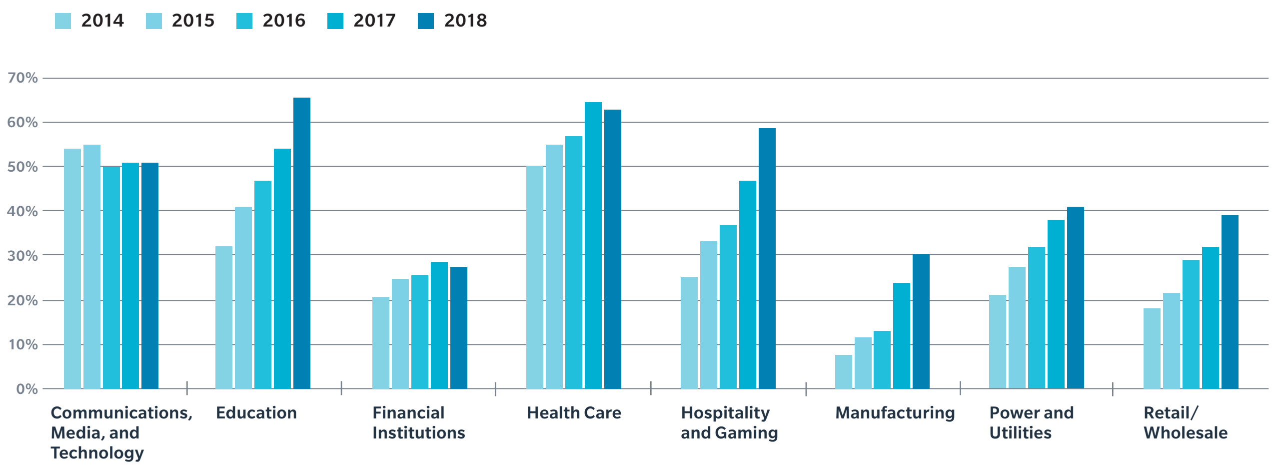


Hospitality and gaming purchase rates have, in fact, increased more than any other industry sector over the last three years. Recent events have demonstrated that the significant amount of PII held by these companies makes them attractive targets for cyber-attackers, and thus vulnerable to significant losses and liability costs.

FIGURE 2

Education, health care, and hospitality and gaming organizations were the leading buyers of cyber insurance

SOURCE: MARSH PLACEMAP (*CMT figures include cyber/blended deals.)



Two trends, however, are driving up purchase rates for standalone cyber insurance coverage among non-traditional industries. First, insurers have sought to more carefully define the boundaries of property, casualty, and cyber policies; property insurers, for example, are generally no longer willing to provide coverage for business interruption caused by network intrusions. Those losses are increasingly expected to be covered under cyber policies, which have expanded to respond to a wide variety of potential risks while still being competitively priced.

Second, the severe economic and operational disruptions caused by the 2017 WannaCry and notPetya malware attacks continue to haunt organizations with no heavy use or handling of PII, including manufacturers, logistics companies, and others. Those attacks, coupled with more recent, high-profile ransomware incidents, have made clear that cyber threats have evolved from data breach and theft to now include business interruption and supply chain disruption.

FIGURE 3

Hospitality and gaming, manufacturing growing quickly

SOURCE: MARSH PLACEMAP (*CMT figures include cyber/blended deals.)

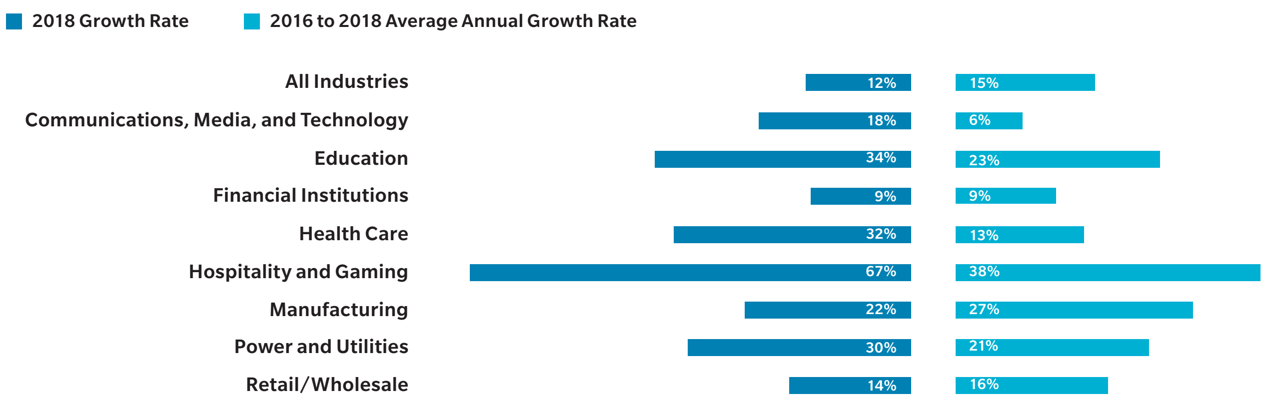
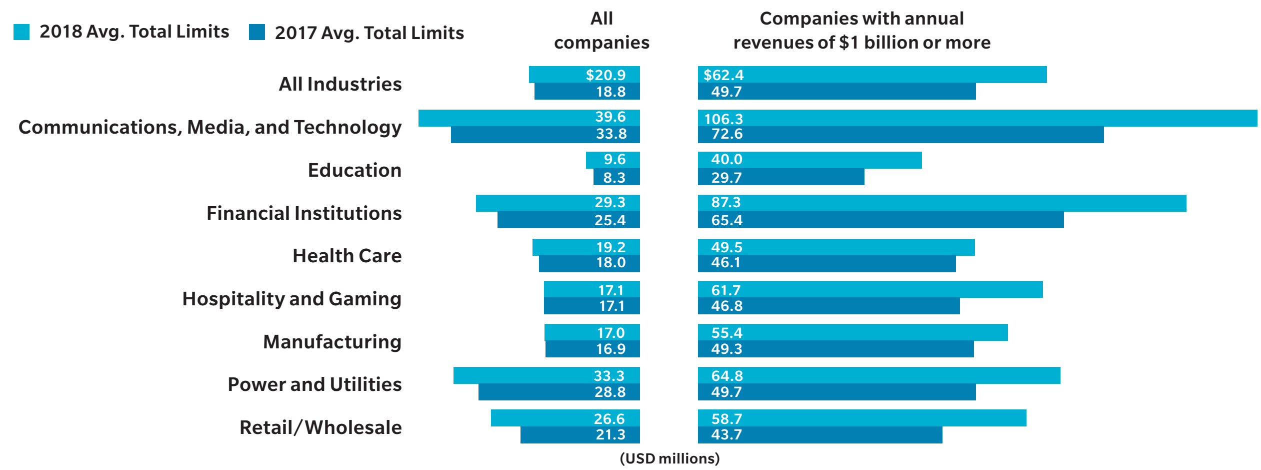


FIGURE 4

Communications, media, and technology, financial institutions, and power and utilities companies are purchasing higher cyber insurance limits

SOURCE: MARSH PLACEMAP (*CMT figures include cyber/blended deals.)



As a result, more organizations that have not traditionally viewed themselves as at risk from cyber-attacks — such as manufacturers, power and utilities companies, and those heavily reliant on technology for operations, production, or systems control — are now purchasing cyber insurance (see Figure 3).

Larger Companies Purchasing Higher Cyber Insurance Limits

As cyber risk is now a regular item on the boardroom agenda, businesses are recognizing that their cyber risk management programs must include more than technology. Corporate cybersecurity budgets are soaring, but C-suite, financial, and risk executives are using risk quantification — calculating the potential financial impact of cyber events on an organization — as a basis for their capital allocation strategies. They're also seeking to invest more in response planning, recovery, and risk transfer, including purchasing higher cyber insurance limits (see Figure 4).

In 2018, the average cyber policy limits purchased by companies with more than $1 billion in annual revenue increased by more than 25%, from $49.7 million in 2017 to $62.4 million. Average cyber limits for all companies increased 11% to $20.9 million in 2018, up from $18.8 million in 2017. The sharpest rises were seen in communications, media, and technology, financial institutions, power and utilities, and retail/wholesale.

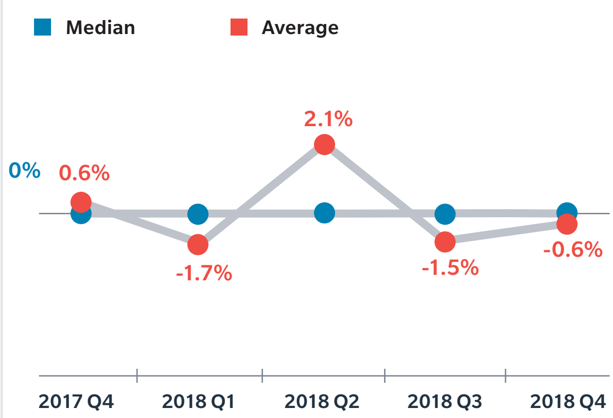
Market Remains Competitive

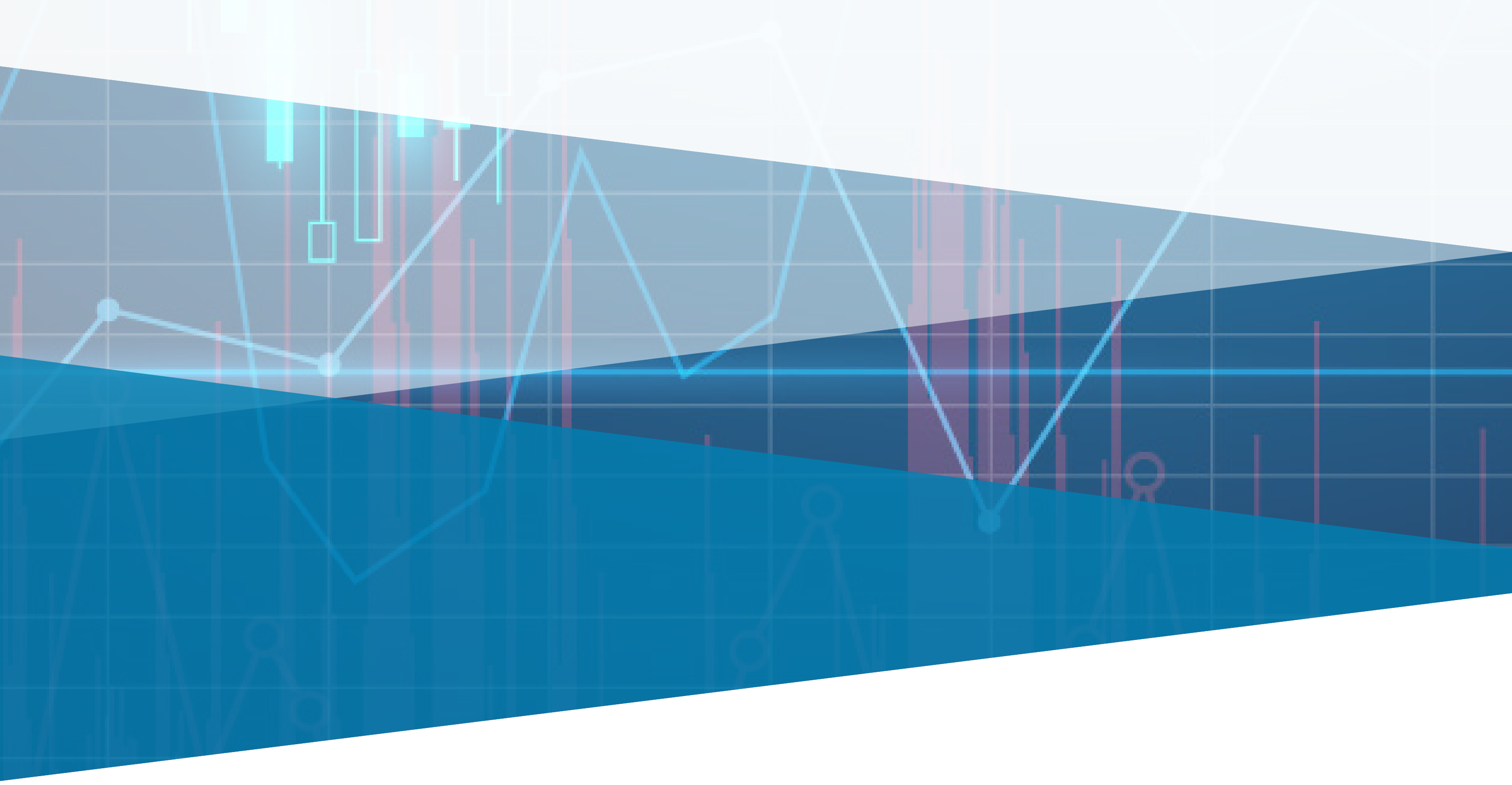
Growing awareness of cyber risk and expanded coverage offerings have driven demand for cyber insurance up significantly. Pricing, however, remains competitive thanks to a commensurate increase in supply. In the fourth quarter of 2018, average pricing for cyber insurance coverage fell by 0.6% (see Figure 5).

FIGURE 5

Cyber insurance pricing stays close to flat

SOURCE: MARSH PLACEMAP.





The market should remain stable for the remainder of 2019, barring a market-changing event.

Theoretical aggregate capacity in the cyber insurance market increased to $1.8 billion in 2018, a threefold increase from 2015. Insurers also continue to provide more coverage in exchange for premium, although this trend may not continue indefinitely.

Despite being able to purchase coverage at favorable rates, buyers — especially large ones — are seeing insurers scrutinize their approach to cyber risk management. Insurers are demanding more information about technology firewalls and system redundancies, system upgrades and critical software patching, training programs, and other activities. Organizations renewing their cyber insurance programs in 2019 should be prepared for detailed questions on these topics.

About This Briefing

This report was prepared by the Cyber Practice within Marsh's US FINPRO Practice, in conjunction with Marsh Digital, Data & Analytics. 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.

For more information, email cyber.risk@marsh.com, contact your Marsh representative, or:

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

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