MARSH

CYBER PRACTICE

Setting the Record Straight on Cyber Insurance

For almost 30 years, cyber insurance has covered losses and expenses associated with a growing range of cyber perils. So why is there continued skepticism about its responsiveness? It's time to correct the record: Cyber insurance is an essential component of a comprehensive cyber risk management program, and a worthwhile investment for businesses.

Data breaches. Notification costs. Third-party liability. Business interruption. Cyber extortion. Reputation damage.

The potential cyber and technology exposures that businesses face continue to expand — as do the potential economic losses they can cause. So it's no surprise that cyber risk now ranks among the top five concerns for companies. And as recognition of the risks increases, more companies are purchasing cyber insurance to take advantage of the expanding protections those policies offer.

Despite the growth in uptake, the value of cyber insurance has recently been the subject of considerable debate within the insurance industry, some of which has played out in the media. The discussion has, in many cases, not reflected fairly on the role of cyber insurance in reducing the economic impact of risk. The debate has often conflated cyber policies with property, casualty, and crime policies, particularly around how these policies do or do not respond to cyber claims.

But the facts are clear: Cyber insurance is a reliable, cost-effective way to transfer the risks companies face from the increasing use of data and technology in business operations. And standalone cyber policies will generally respond to those risks.

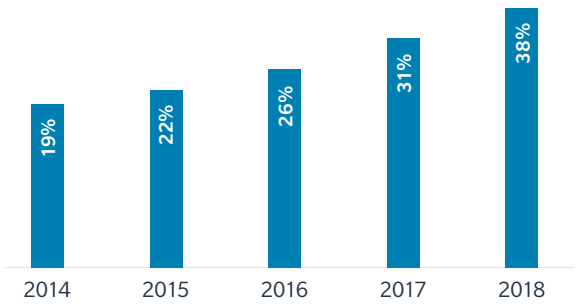
Increasing Appetite, Claims, and Payouts

As the range of cyber risks and coverages have expanded, so have purchase rates of standalone cyber insurance. The number of Marsh clients buying dedicated cyber insurance has doubled over the past five years, with nearly 40% now purchasing cyber policies (see Figure 1). And the development of broader coverage offerings is attracting a wider range of buyers; purchasing among Marsh clients has risen by an average of 15% annually since 2016, with highest growth among the hospitality, manufacturing, education, and power and utility sectors.

FIGURE 1

Cyber insurance take-up rates have doubled since 2014

SOURCE: MARSH PLACEMAP



MARSH & McLENNAN COMPANIES

Cyber insurance claims, and claim payouts, are rising in tandem with purchasing. According to CreditSights, US domiciled insurers paid cyber claims totaling $394 million in 2018, up from $226 million the previous year. And NetDiligence reports that the number of claims submitted for inclusion in its Cyber Claims Study, which analyses claims to cyber insurers, rose more than 40% in 2018 over the previous year.

Individual insurers have reported similar trends:

- AIG says it handled more than 2,000 cyber claims globally in 2018.
- Beazley handled more than 3,300 data incidents in 2018 (more than 10,000 since 2009).
- In 2018, specialty cyber insurer CFC paid more than 1,000 cyber claims and expects that number to increase by 50% in 2019.
- Hiscox dealt with more than 1,000 cyber-related insurance claims in 2017, a 1700% rise over 2013.

These figures point to an increasing recognition of cyber risk as a top corporate concern and of cyber insurance as an effective and responsive way to cover cyber event losses.

US domiciled insurers paid cyber claims totaling **$394 million** in 2018

Confusion and Conflation of Cyber, Property, and Crime Policies

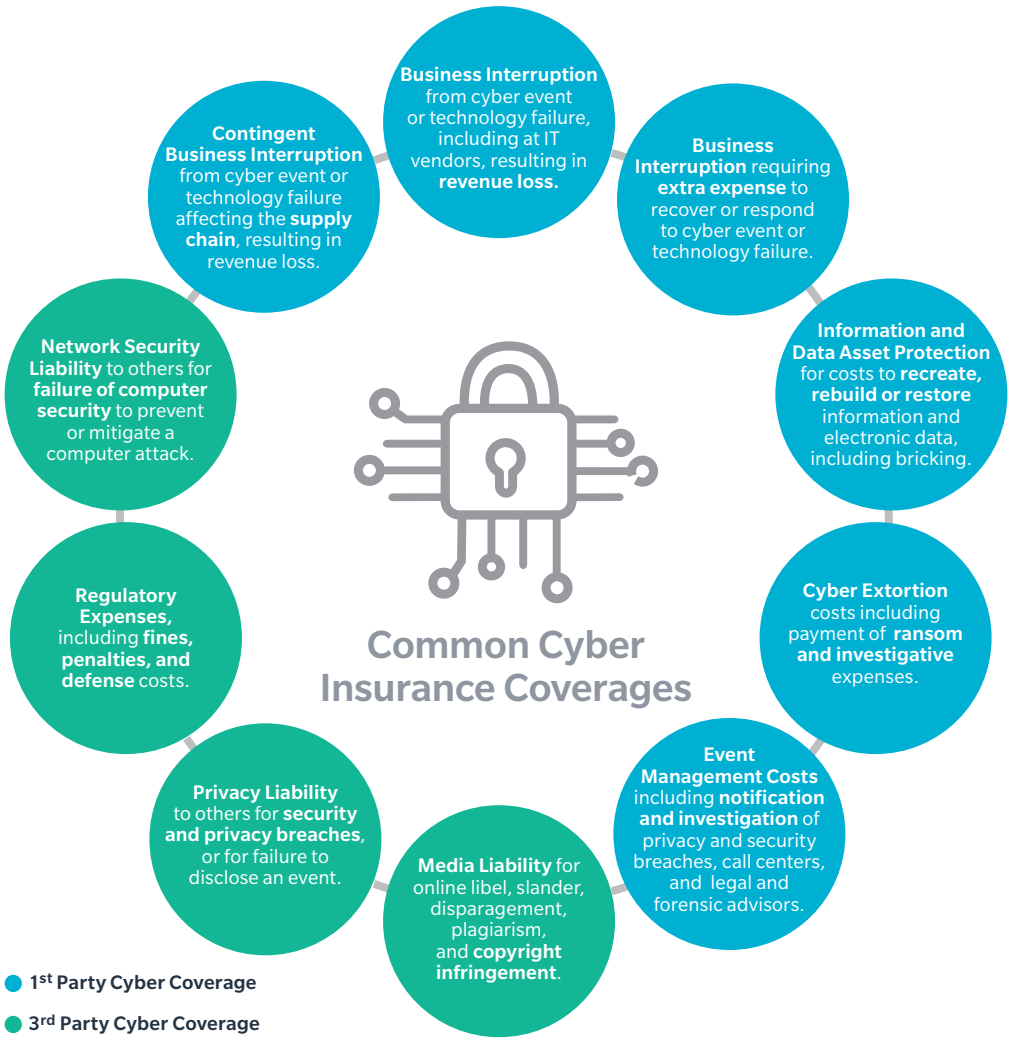
Despite increasing appreciation for cyber insurance, many organizations still expect — mistakenly — that cyber losses will be fully covered under non-cyber (property, casualty, or crime) policies. This confusion has been exacerbated by inaccurate or misleading commentary in, and by, the media.

The issue stems from the fact that cyber risk as a peril can result in multiple forms of loss that have not traditionally been explicitly excluded under property, casualty, and crime policies. This has created what is known as "silent cyber" — the unknown exposure in an insurer's portfolio created by a cyber peril that has not been explicitly excluded. As insurers have seen a rise in unexpected claims under non-cyber policies, "silent cyber" is now being more closely monitored and cyber risk increasingly excluded from traditional insurance lines.

Along those lines, several insurers have issued clarification of their intent to only cover cyber perils in cyber policies. In early July 2019, Lloyd's issued a new mandate requiring its market underwriters to ensure that all policies either explicitly affirm or exclude cyber cover, in an effort to eliminate non-affirmative or "silent cyber" risks from property policies as of January 2020, and from liability coverages a year later.

We have recently seen a few high-profile disputes where insureds have sought to recover cyber event-related losses from their property policies, and insurers have denied coverage. Regardless of the merits of those cases, such disputes point to the importance of obtaining cover under an affirmative cyber policy that is tailored to a company's specific cyber exposures and thus offers the best chance for insurance to respond.

In addition to this much-needed clarity of intent, standalone cyber policies offer other valuable benefits, such as reimbursement for costs to engage experts to assist with post-event forensics and response management, and even pre-loss prevention and risk management tools.



An Adaptive, Responsive Market

As cyber threats evolve and become more economically damaging to businesses, the cyber insurance market remains adaptive in responding to buyers' needs. As traditional insurance lines retreat from covering cyber events, cyber insurance is becoming an increasingly vital tool.

Organisations should look past the erroneous myths about cyber insurance and look to gain a more objective and accurate view of the broad and expansive protections that cyber coverage can offer. By working with a knowledgeable broker or advisor, organisations can design a standalone cyber insurance program that is tailored to their unique risk profile and risk tolerance.

Critical Truths about Cyber Insurance

The pervasive use of technology to power business and connect supply chains creates ever-greater cyber exposures and vulnerabilities for companies of all sizes and in all industries. Inaccuracies and misunderstandings around cyber insurance do a disservice to every organisation that could benefit from cyber coverage but may be dissuaded from purchasing it. Some of these myths include:

Myth: "Cyber insurance does not cover human error."

- **Truth:** While cyber insurance was primarily designed to address malicious cyber incidents, it has evolved to cover a wide range of operational and human risk, including social engineering, accidental disclosure, loss of a laptop or device, rogue employees, and failed updates or system migration. Generally, cyber policies do not exclude coverage for accidental errors or omissions, and many affirmatively cover such losses through system failure or administrative error coverage grants.

Myth: "Data breach costs focus on legal liability."

- **Truth:** Data breach insurance is the most established aspect of cyber insurance and coverage is broad, particularly for first-party breach response costs, which can include legal, crisis management, call center, forensics, credit monitoring, and notification expenses. Cyber insurance will generally also cover the expenses associated with business interruption and data loss events.

Myth: "Insurers dictate which incident response providers and advisors are used."

- **Truth:** While most cyber insurers have a recommended panel of service providers (legal counsel and vendors), many are willing to accommodate an insured's existing or preferred providers. Some insurers will even allow policyholders to have absolute discretion in their choice of vendors.

Myth: "Business Interruption cover is limited."

- **Truth:** Business interruption cover has evolved considerably to reflect the nature of how companies function today. Cover will typically extend to the overall financial impact to the business, beyond just the duration of the cyber event. Many policies will also cover losses resulting from a system failure or technology disruption at an insured's IT vendors or within its supply chain.

Myth: "Cyber insurance excludes recent technology or system upgrades."

- **Truth:** A robust cyber insurance policy can contemplate system upgrades where such best practice is the most cost-effective solution. Cyber insurers embrace insureds that view security as a journey, not a destination.

For more information, send an email to cyber.risk@marsh.com, visit marsh.com, or contact:

KELLY BUTLER
Cyber Leader – Pacific
+61 3 9603 2194
kelly.butler@marsh.com