INSIGHTS | MARCH 2020

Underinvestment in Cyber Insurance Can Leave Organizations Vulnerable

Welcome to the 2020s, where every sector and company, regardless of size, is heavily reliant on technology to facilitate its operations, communications, and engagement with its supply chain. In this digital climate, cyber-attacks pose an increasingly significant business risk, which has resulted in cybersecurity steadily climbing up the C-suite's priorities agenda.

Recently, in a global study of cyber risk perceptions conducted by Marsh and Microsoft, more than half of companies rated cyber risk in their top five risks.

Yet many companies are still struggling to grasp the extent of their cyber risk exposure, and this misunderstanding creates an unnecessary roadblock for every organization that could benefit from cyber risk transfer but is reluctant to purchase it.

Prior to 2015, the cyber incidents that made headlines were predominantly data breaches which, although still a problem in their own right, are no longer always the worst case scenario. Via crippling ransomware and malware attacks, criminals now have the ability to completely paralyze businesses by bringing their technology-dependent operations to a halt, which in some circumstances can also result in physical damage and bodily injury. Worse still, companies are increasingly becoming collateral damage in attacks on other targets, so a threat assessment based on the likelihood of a direct attack is not the reliable barometer it once was.

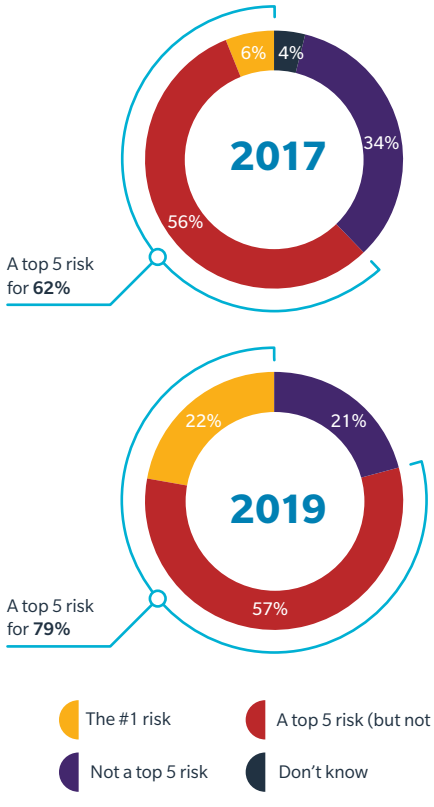
Underinsurance Versus Risk

In this risk landscape, it would be reasonable to assume that companies are shifting their risk perception from the physical to the digital and in turn adjusting the way they insure against risk. However, firms remain chronically underinsured against cyber risk.

FIGURE 1

Cyber risk has climbed sharply among organizations' risk priorities.

Q. Of the following business threats, please rank the top 5 that are the biggest concerns to your organization (cyber-attacks/cyber threats shown).



Base: All answering; n=1312 (2017); n=1512 (2019)

MARSH

Compare the property and cyber insurance markets. Many estimates put the annual economic impact of cybercrime at or above $500 billion, yet companies spend .008% of that figure on cyber insurance. Compare that to the estimated $300 billion annual impact of natural disasters and the spend jumps to 60%. To understand why this is the case, we must first examine the widespread misconceptions about the effectiveness of cyber insurance.

Myths and Misconceptions About Cyber Insurance

Myth: 'Cyber insurers just deny claims'. Insurance policies are legal contracts, interpreted on the basis of defined terms contained within such policies, which can be complex at times. This is why large companies employ insurance brokers to create an insurance portfolio adapted to their risk appetite. When a large cyber incident occurs at a company that chose not to purchase cyber insurance, its understandable reaction is to file the claim under any policy that might offer some coverage unintentionally or through ambiguous language. In the past few years, this dynamic has created several factually incorrect headlines about 'cyber insurance claims' being denied, when in fact there have been cyber incident claims denied under non-cyber policies that were never designed to cover them in the first place.

Myth: 'Cyber insurance does not cover human error'. Although cyber insurance was initially created to address malicious cyber incidents, it has evolved to cover a wide range of operational and human risks. These risks include social engineering, accidental disclosure, loss of a laptop or device, rogue employees, failed updates, and system migration. Typically, exclusions of coverage are not made in cyber policies for accidental errors or omissions, and many programs affirmatively cover such losses through system failure or administrative error coverage grants.

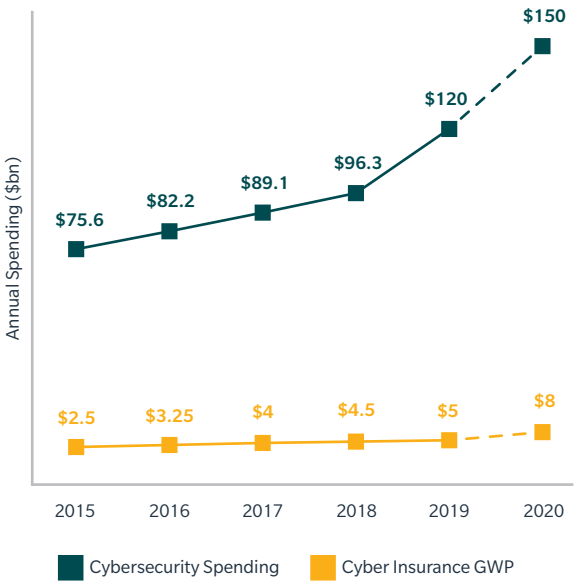
Myth: 'Data breach costs focus on legal liability'. Data breach insurance is actually the most established aspect of cyber liability programs and coverage is broad. This is especially true for first-party breach response costs, which can include legal, crisis management, call center, forensics, credit monitoring, and notification expenses. Cyber insurance will normally also cover the financial burden associated with business interruption and data loss events.

Myth: 'Insurers dictate the incident response providers and advisors selected for use'. While most cyber insurers have a recommended panel of service providers, which includes legal counsel and other 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.

FIGURE 2

Cybersecurity spending far outpaces cyber insurance spending.

SOURCE: Gartner, Munich Re



Myth: 'Business interruption cover is limited'. This aspect of cover has evolved considerably to reflect the nature of how companies function today. Business interruption insurance will typically extend to covering the overall financial impact of a cyber incident to the business, beyond just the duration of the cyber event. Many cyber policies will also cover losses resulting from a system failure or technology disruption at the place of work of an insured's IT vendor or within its supply chain.

Myth: 'Cyber insurance excludes recent technology or system upgrades'. On the contrary, legacy technology is more difficult to insure when software manufacturers stop implementing a regular patching system, as that technology is at greater risk of exploitation. This is a consideration that more traditional industries need to be aware of. A robust cyber liability insurance policy will consider the best practice standards of dealing with new system upgrades that will produce the most cost-effective solution. Cyber insurers embrace insureds that view security as a journey, not a destination.

Degree of Paralysis

Next, there is a perception gap and a degree of paralysis when it comes to treating cyber risk. There is a clear difference between how businesses perceive traditional risks, such as physical damage, compared to how they think of cyber risk. Tangible damage, like a fire in a warehouse, is much easier to visualize and the valuation of the affected physical asset valuation is relatively straightforward and predictable. The financial impact of a cyber-attack can be further reaching and more nuanced in terms of quantification.

Interestingly, we found that companies that engaged in a structured process to value cyber risk were more likely to invest in adequate cyber insurance. These companies are also better able to evaluate the best return on cyber security investments, achieving a harmonious blend of prevention and residual risk transfer.

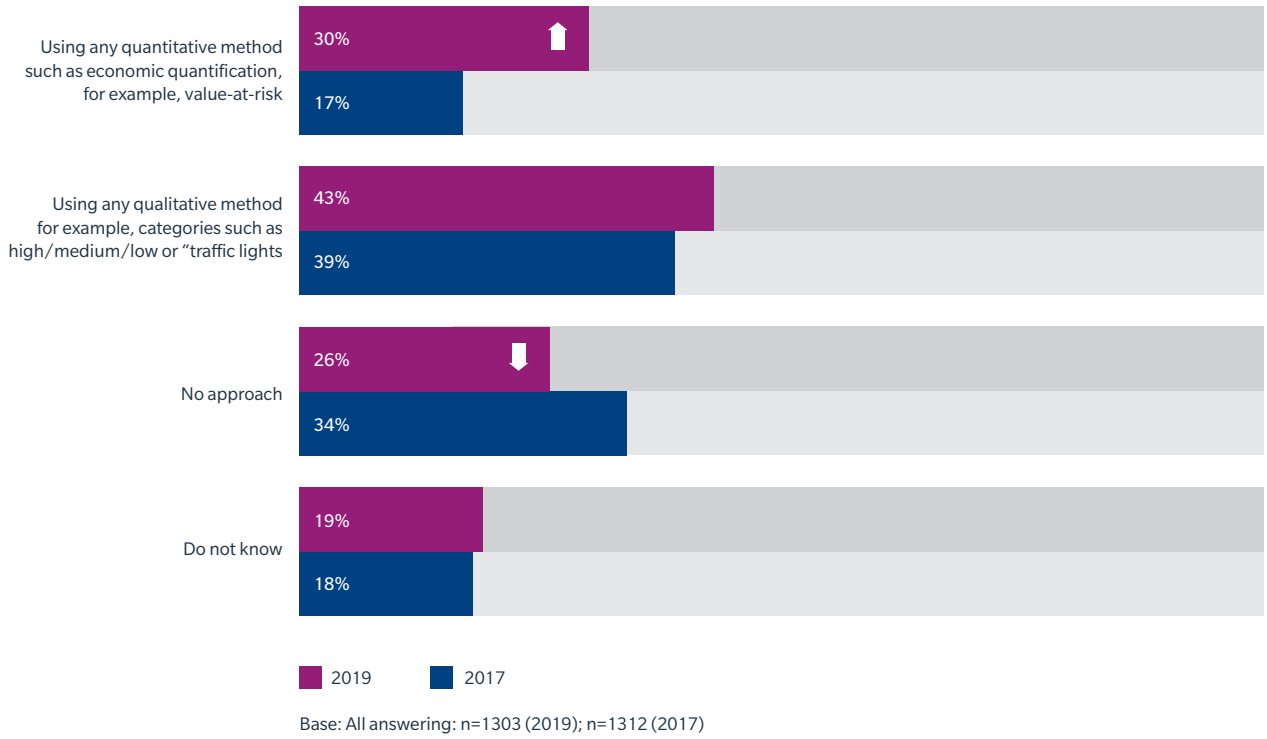
A further but related reason that some companies don't yet purchase cyber insurance is that there are fewer contractual imperatives to do so. It's well understood that proof of insurance is a key requirement for stakeholders with a vested interest in the company, whether those are lenders, investors, partners or customers. Often the list of required insurances has not been risk adjusted and more heavily emphasizes physical damage coverage or statutory forms of liability. In the US, it is now very common to see that insurance requirements do include cyber insurance, but this prudent measure has been slow at traversing the globe.

Finally, cyber insurance does come with a cost, and companies frequently budget for insurance on an annual cycle measured in small aggregate increases and decreases, rather than major risk-based reallocation of capital. Firms may also feel that they can somehow spend their way out of the risk altogether through relentless investment in more cyber security tools. According to Gartner, spending on cyber security jumped 24% from 2018 to 2019, yet the *Marsh Microsoft Cyber Risk Perception Survey* found that firms felt less confident about cyber risk in 2019.

FIGURE 3

Quantitative measurement of cyber risk exposure has increased substantially since 2017, but remains low overall.

Q: IN GENERAL, HOW DOES YOUR ORGANIZATION MEASURE OR EXPRESS ITS CYBER RISK EXPOSURE?



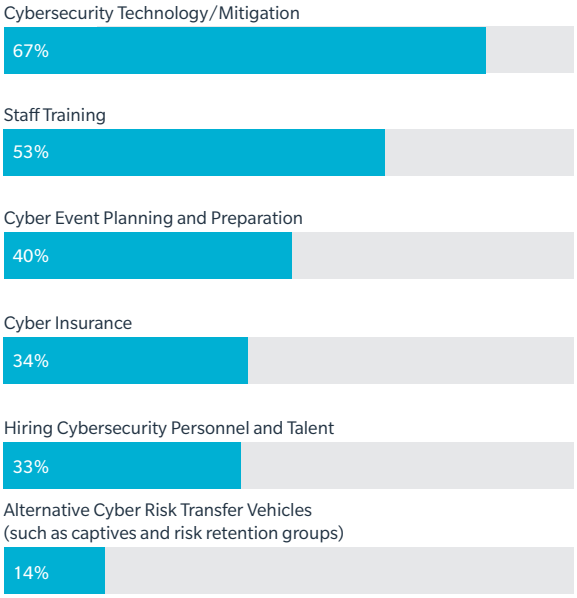
Base: All answering: n=1303 (2019); n=1312 (2017)

Different Context

FIGURE 4

Cybersecurity technology and mitigation top the list of future investment allocations for risk management.

Q: How do you expect your investment allocations in the following areas of risk management to evolve over the next three years?



% expecting to spend some or significantly more on each area
Base: All answering: n=885 (2019)

As companies increasingly consider cyber insurance to be a critical aspect of their cyber resilience strategy, they will start to think about budget allocation in a different context. Financial decisions will be made from a place of understanding what the worst case scenario loss looks like and how effective controls are at mitigating that risk. This understanding will help businesses to better allocate budget appropriately, as they will know what risk their cyber security spend will mitigate, how much cyber insurance they need to buy, and what residual amount is within their appetite to retain.

There has also recently been a shift in attitude towards cyber cover. Organizations are approaching risk quantification exercises with more rigor, and subsequently prioritizing investment into mitigating cyber risk, as their knowledge on the topic evolves.

Embracing Cyber Insurance to Build Resilience

In closing, businesses purchase insurance solutions for risks they understand and where they perceive insurance is an effective method of treatment. Cyber insurance is only about 20 years old, so in comparison to insurance covering physical losses, it is admittedly in its infancy.

Dedicated and appropriately designed cyber insurance is a proven and effective way to transfer residual risk, after thoughtfully understanding the risk and implementing appropriate controls.

However, companies that fail to appreciate that spending indiscriminately may not always reduce their risk, will unfortunately spend money needlessly. Those that clearly understand and articulate the risk in financial terms will have the keys to mindful budget allocation.

Senior management and board-level leadership must embrace cyber risk as an issue so the conversation can be driven top down and bottom up. Only then can we create cyber resilience and the virtuous cycle of risk management that an effective insurance market filled with engaged risk managers can create.

A version of this article was previously published in the February 2020 edition of Computer Fraud & Security.

SARAH STEPHENS
Head of Cyber, International and
Cyber, Media & Technology Practice Leader, UK FINPRO
Marsh JLT Specialty
+44 (0)207 558 3548
sarah.stephens@marsh.com