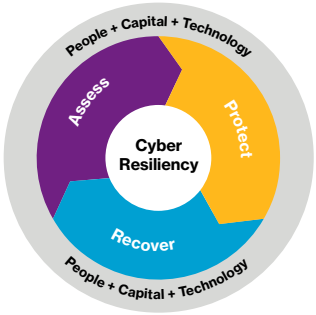

Decode cyber risk.

Here comes the next wave of cyberinsurance buyers

by **Heather Wilkinson**

Over the last two years, cyberattacks have negatively impacted productivity, revenue generation and company reputation across all industries, especially those once considered low risk. Industries such as manufacturing, construction and logistics traditionally have not purchased cyberinsurance, due in part to a perceived lack of need. However, recent events have shown that such thinking could leave them exposed to potentially catastrophic losses.

A majority of companies in these industries viewed their potential exposure from a cyber hack as almost nonexistent for the following reason:

- Unlike the health care and financial industries, they do not store personally identifiable customer data and are therefore not subject to heavy regulatory scrutiny.

These companies tend to underestimate the level of exposure that could result from network interruption. As of yet, there has been a dearth of reliable statistics to quantify the frequency and severity of business interruption loss connected to cyber hacks. These factors combined with perceived coverage limitations drove many in these industries to devalue the benefit of cyber policies. Many off-the-shelf, first-generation cyber policies excluded coverage for property damage and bodily injury, making the coverage appear less relevant at first glance. Additionally, many believed a loss of revenue due to network unavailability would be covered under the broad business interruption component of a general liability policy. As a result, these industries have typically directed their insurance budgets, and their attention, elsewhere. However, the number of cyber events resulting in significant losses to companies that are highly dependent on network availability to sustain their operations has been increasing.

Equal opportunity cyberattacks

According to Willis Towers Watson's Reported Cyber Claims Index, which includes claim data gathered over the last 12 months, cyber hacks and social engineering attacks represent two of the top three cyber events experienced across all industries.

Type	Count of grouped type of loss %
Accidental Disclosure	23%
Hack	22%
Social Engineering	18%
Denial of Service	10%
Rogue Employee	9%
Other	8%
Lost/Stolen Device	7%
Unknown	2%
Grand Total	**100%**

*Percentages may not equal 100% due to rounding.

Willis Towers Watson

According to security firm SonicWall's 2017 Annual Threat Report, ransomware use grew 167 times year over year, as the rate of attempted attacks rose from 3.8 million in 2015 to 638 million in 2016. This spike can be attributed to the reliance on aging technology, ease of access to an organization's network through email, and the lack of awareness and focused employee training.

Some recent examples of ransomware attacks include:

- Two well-known logistics companies were victims of the NotPetya ransomware attacks. System-wide shutdowns cost these companies more than $700 million combined, and the impact to operations and revenue continue. Costs associated with reputational loss and customer dissatisfaction are harder to measure, but certain.
- A construction company suffered almost $400 million in losses when ransomware shut down critical supply chain and IT functions.
- Consumer goods companies reported almost $500 million in losses due to ransomware attacks that affected network operations or interrupted sales platforms and financial networks.

As more companies within the manufacturing, logistics, construction and other industries turn to automation and remotely operated equipment, the likelihood of extended network outages and complete work stoppages resulting from cyberattacks increases. For logistics and manufacturing companies, which rely on intricate network interfacing to handle supply chains and move goods and services, a cyber hack can instantly cripple operations. In fact, according to the Willis Towers Watson Reported Claims Index, a high percentage of claims reported against manufacturing companies resulted from hacking incidents, compared to other industries.

Manufacturing Industry	
Hack	**36%**
Social Engineering	29%
Accidental Disclosure	14%
Lost/Stolen Device	14%
Other	7%

*Percentages may not equal 100% due to rounding.

Thoroughly modern cyber policies

As risk factors become more apparent, and more data emerges on potential costs to companies experiencing network interruptions due to cyberattacks, the interest in cyberinsurance and the scope of its coverage has broadened. Cyber policies that include coverage for property damage, bodily injury, service delays and other first-party losses are now available. Ancillary services provided by carriers and brokers to enhance security standards and aid in vendor management are being recognized as highly valuable to ensuring the fastest and most efficient incident response possible.

Senior executives are also increasingly focused on mitigating cyber risk. According to a 2016 survey of Fortune 1000 companies, 86% of management boards across all industry types cite cybersecurity as a major concern and an area for renewed focus.

Decision makers increasingly understand that technological defenses, while important, can take them only so far. There is also a greater appreciation for the potentially devastating impact of a failed or wrong technology on an organization's revenue and reputation. These once-considered "low risk" industries have moved toward reallocating resources to purchase stand-alone cyberinsurance policies. Further, more companies are being contractually required to carry cyberinsurance. In the construction industry, for example, some companies must provide evidence of network security coverage before they are allowed to bid on jobs.

As our reliance on technology in all aspects of business continues to grow, cyber risk has followed suit. Costs associated with high-profile cyberattacks have mounted against all types of industries, even those that might not have seemed likely targets. It's become abundantly clear that a renewed focus on cyber risk transfer to mitigate future loss is imperative. As cyberinsurance products continue to evolve, companies that may have brushed aside the idea of purchasing cyberinsurance in the past now consider it a key component in a well-designed risk management strategy.

Contact

Heather Wilkinson
Willis Towers Watson
949 930 1767
heather.wilkinson@willistowerswatson.com

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

WTW-NA-2018-WTW36557

willistowerswatson.com

Willis Towers Watson