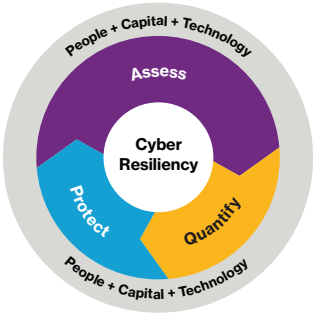


Decode coverage.

Cyberinsurance 2.0: The new wave of cyberinsurance

by Jason Krauss, Willis Towers Watson

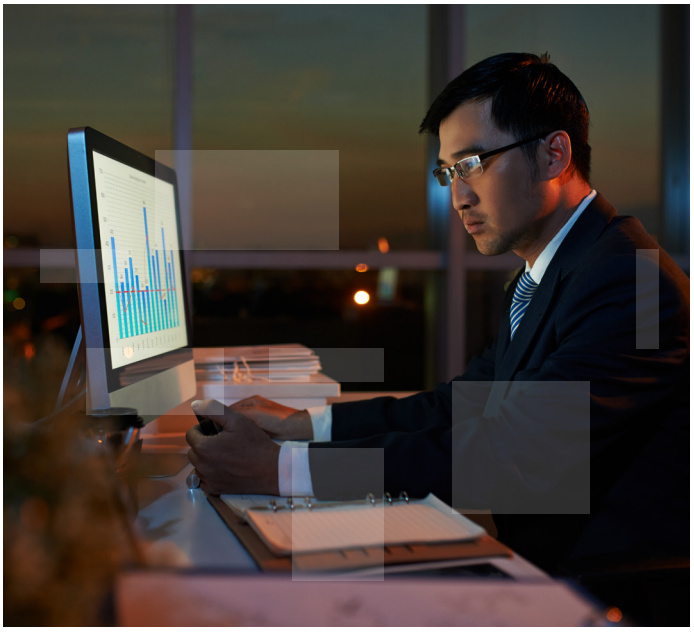
Certain property insurers' use of war exclusion policy language to deny claims for losses arising from the NotPetya worldwide cyberattack has created significant media attention. In response, some pundits warned that cyberinsurance in the future could be worthless[1]. What the media seemed to gloss over was that these coverage denials were made under property policies, not dedicated cyber policies. The coverage at issue was not designed or intended to pick up claims and losses resulting from a cyber event. In other words, these organizations were relying on "silent cyber coverage" or inexplicit cyber coverage within their property policies.

In light of the above, it is timely and important to revisit the evolution and current state of the cyberinsurance policy. A review helps illustrate the immense value of cyberinsurance to organizations across all industries in properly managing their cyber risk. Cyberinsurance is the key component to any cyber risk management strategy and should be part of every organization's holistic approach to combating cyber risk.

The evolution of cyberinsurance

Cyberinsurance was initially only sought after by organizations in the technology, media and telecommunications industries, and only third party liability coverage was offered. We have come quite a long way. There is now demand for stand-alone cyberinsurance across all industries, and not only retail, health care and financial services companies that handle confidential customer information. An increased reliance on automation and remotely operated equipment and a great likelihood that cyberattacks can lead to extended network outages and complete work stoppages have ramped up demand for cyberinsurance in industries such as manufacturing, construction and logistics.

Increased demand has steadily expanded cyber coverages. Once unique and ground breaking coverages, like system failure and intentional shutdown coverage, are now regularly incorporated into base cyber policies.



Increased demand has steadily expanded cyber coverages. Once unique and ground breaking coverages, like system failure and intentional shutdown coverage, are now regularly incorporated into base cyber policies, often without sub-limits or additional premiums. It is important to note that even with the right coverages in place, some cyberattacks could cause damage that exceeds the coverage limits in place. Therefore, it is essential to work with your broker to ensure appropriate and tailored coverage solutions and adequate policy limits that reflect an organization's cyber risk strategy.

Willis Towers Watson

Cyber insurers have progressed in developing client-focused insurance solutions, as our evaluation of cyber market offerings and our own Willis Towers Watson cyberinsurance policy indicates. The advance of cyberinsurance from specialized coverage with limited solutions to an essential part of every organization's risk management strategy, has made us strive to make coverage more accessible to those who aren't cyber experts while still retaining the agility to respond to an ever evolving cyber landscape. Three guideposts – clarity and simplicity, flexibility and relevancy – help us assess and develop cyberinsurance policies as the cyberinsurance market continues to evolve.

1. **Clarity and Simplicity** – As the cyberinsurance market matures and general demand increases, efforts are underway to remove industry jargon from insurance policies and replace it with clear and simple language that is understandable to all. For instance, streamlining terminology can help simplify and shorten an insurance policy. And we have encouraged carriers to create a single term of art for all private or protected information, whether, personally identifiable information (PII), protected health information (PHI) or corporate confidential information.
2. **Flexibility** – Not all coverages or enhancements are appropriate for every client. Clients should not pay for coverage that they do not need, but should work with brokers to craft tailored solutions to maximize benefits of the coverage while reducing the overall cost of the program. Developing a modular or semi-modular form will allow for greater flexibility when an organization's stakeholders are deciding which cyber coverages are right for them. We also advocate moving existing coverage into explicit insurance contracts rather than grants of coverage within exclusions.
3. **Relevancy** – Cyber risk is constantly changing, increasing the urgency for cyber policies to remain relevant. Clients should consider:
   a. Certain provisions, such as the period of restoration, should be scheduled items, so that the policy can be easily updated as needs change.
   b. Computer system or network definitions should be carefully crafted to include the systems or networks of unscheduled outsource providers.
   c. The cyber extortion threat definition should be broad enough to include new ransomware iterations.
   d. Regulatory coverage must be expansive enough to take into account new privacy regulations.

Tailor solutions to reflect your cyber strategy

Even as some traditional lines of insurance are rethinking their exposure to cyber risk, we continue to push boundaries to find tailored solutions for our clients. While there are limitations to cyberinsurance policies, they are not necessarily the ones identified by the latest media coverage. Certainly, the cyberinsurance market will need to continue to innovate in the face of new challenges, and develop new solutions with cyberinsurance markets to meet our clients' evolving needs. Most relevant to the NotPetya attacks, we regularly deliver the following solutions for our clients:

1. Full limits for system failure coverage, which does not require an actual security breach.
2. Enhanced business/network interruption coverage, which is the coverage that has received the most attention since the NotPeyta attack, and includes:
   a. The replacement of waiting periods with qualifying periods, so that all loss is recognized from the beginning of an event if the qualifying period has been exceeded.
   b. No waiting or qualifying periods for extra expenses, only a dollar retention.
   c. The inclusion of forensic accounting costs in the definition of business interruption loss.
   d. The inclusion of both voluntary and regulatory shutdowns in what constitutes a business interruption incident.
   e. Consequential reputational loss coverage, which insures net income loss due to adverse publicity from an actual or alleged cyber incident.
3. In response to the General Data Protection Regulation and state privacy laws, expanded regulatory claim coverage, most significantly for claims alleging the wrongful collection and retention of personal information, which does not require a cyber breach.
4. Other insurance optimal recovery provisions to provide the insured with the option to designate a cyber policy as primary, excess or contributing in order to maximize the total indemnity available for a claim or loss under the cyber policy and other policies that may be in effect.
5. In response to Mondelez[2], a further narrowing of the war exclusion, to include only declared war or kinetic war or insurrection, and a continued expansion of the explicit grant of coverage for cyberterrorism to include nation state attacks.

Cyberinsurance innovation will continue

We are fully engaged with cyberinsurance carriers in an effort to deliver meaningful solutions to our clients as they seek to manage a dynamic risk landscape. Cyberperils are relevant to all lines of insurance, and we are seeing more carriers willing to integrate other coverages, like crime, property & casualty, into the cyber offering. The insurance market will need to continue to innovate with new cyber coverages and enhancements in response to the evolving cyber risk landscape. Tomorrow's stand-alone cyber policy could very well look quite different from the cyber policies on the market today.

Source

[1] Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong, *The New York Times*, April 15, 2019.
[2] https://www.databreachninja.com/wp-content/uploads/sites/63/2019/01/MONDELEZ-INTERNATIONAL-INC-Plaintiff-v-ZURICH-AMERICAN-INSURANCE-COMPANY-Defenda.pdf

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 45,000 employees serving more than 140 countries and markets. 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.

Contact

Jason Krauss
FINEX Cyber/E&O Thought and Product Leader
+1 212 915 8374
jason.krauss@willistowerswatson.com

willistowerswatson.com/social-media

willistowerswatson.com

Willis Towers Watson