Decode protection.

Cyber Insurance

Protecting your company's critical assets

As technology has become a driver of business models, cyber risk has grown into a systemic threat to successful businesses. Now more than ever, businesses need to protect themselves from threats that could jeopardize their financial success.

In our experience, nearly seven out of every 10 cyber insurance claims are related to events caused by employees. Armed with your risk profile and our decades of global experience, Willis Towers Watson will implement best-in-class solutions designed to minimize and mitigate the risks we've identified in your people, technologies and financial assets. We'll also help you insure and transfer the risks that remain.

Cyber attacks, operational errors or technical failures have the ability to paralyse an organisation leading to significant financial loss, regulatory issues and lasting reputational damage. These risks will only increase further as a tech-savvy employees utilise agile working solutions and put more and more pressure on an organization's critical infrastructure.

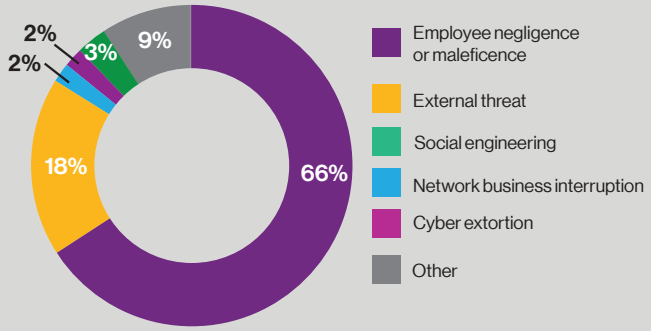
Key considerations that increase the likelihood or severity of a cyber-event:

- Big Data: Increasing volumes of confidential customer information.
- Expanding network perimeter: Supply chain risk and the myriad of interconnected service providers.
- New threat vectors: Ransomware and social engineering.
- Increased regulatory burden: Global privacy regulation continues to tighten with substantially increased financial consequences in the event of a privacy breach.
- Internet of Things: increasing number of connected devices that capture and share data with one another.

The Cyber Insurance Response

Cyber insurance policies have been developed to address the first and third party impacts (see fig. 1) which can result from a cyber incident whether malicious or accidental.

Figure 1. Percentage of claims by breach



Source: Willis Towers Watson claim data

Cyber attacks, operational errors or technical failures have the ability to paralyse an organisation leading to significant financial loss, regulatory issues and lasting reputational damage.

Willis Towers Watson

Mind the GAP!

Traditional insurance policies may not respond to these new risks. They were developed to protect against physical triggers (e.g. fire, explosion, theft, flood etc.) leading to physical outcomes (e.g. property damage, bodily injury) rather than data, networks and intangible assets.

	Crime/ Bankers Blanket Bond	"General Liability"	Kidnap and Ransom	Professional Liability	Property/ Business Interuption	Cyber
First Party Cyber Losses						
Network Interruption due to:						
▪ Computer Crime					■	■
▪ Employee Sabotage					■	■
▪ Operational Errors and Administrative Mistakes						■
▪ Cyber Terrorism					■	■
Restoration, Recollection, Recreation of Digital Assets due to:						
▪ Computer Crime	■				■	■
▪ Employee Sabotage	■				■	■
▪ Operational Errors and Administrative Mistakes						■
▪ Accidental Damage to Hardware					■	■
Cyber Extortion			■			■
Data Privacy and Security Third Party Losses						
Breach of Sensitive Third Party Information				■		■
Data Breach Caused by a Third Party Outsourcer				■		■
Corruption of Third Party Data by Malicious Code				■		■
Distributed Denial of Service or Malicious Code Delivered via your Network				■		■
Corruption or Deletion of Third Party Data				■		■
Lost/Stolen Laptop or Hardware Containing Sensitive Third Party Data				■		■
Data Breach due to a Security Breach				■		■
Intellectual Property Infringement, Plagiarism and Defamation		■		■		■
Data Privacy and Security First Party Losses						
Data Protection Fines and Penalties						■
Data Protection Investigation and Defence Expenses						■
Public Relations Costs						■
Data Protection Legal Expenses						■
Data Breach Notification Expenses						■
Credit/Identity Theft Monitoring Expenses						■

No cover provided

■ Possible cover provided

■ Cover provided

Please note standard policy wordings have been considered, not considering endorsements that may be obtained. For true comparison of policies individual policies and facts of claims would be required.

Coverage is provided on a modular basis meaning that cover can be tailored to specific elements, to protect against:

First Party Network Loss
- Loss of income following a Non-physical Network Interruption and Increased Cost of Working.
- Costs to restore digital assets which are lost, corrupted or destroyed.

Privacy and Security Liability
- Third party damages and defence costs following a privacy or confidentiality breach or unauthorised access or use of a computer system, transmission of a virus and DDOS attack.

Privacy regulatory defence costs
- Fines and penalties (where insurable by law).

Crisis management costs
- IT forensics costs, costs to notify affected individuals, provision of credit monitoring services and public relations expenses

Cyber extortion
- Costs to engage a crisis management expert and any subsequent ransom payment

Payment Card Industry (PCI)
- Fines and Assessments.

Why Willis Towers Watson

More than half of all cyber incidents begin with employees, so it's a people problem. And the average breach costs $4 million, so it's a capital problem, too. No one decodes this complexity better than Willis Towers Watson. As a global leader in human capital solutions, risk advisory and broking, we are well prepared to assess your cyber vulnerabilities, protect you through best-in-class solutions and radically improve your ability to successfully recover from future attacks.

A holistic approach to cyber risk evaluates all threats – from people to technology – and ensures you are best prepared to protect and grow your business.

Assessment:
Measurement & analytics

We bring deep data from a diversity of categories and companies like yours to assess and quantify your risk profile, via proprietary risk assessment tools addressing people, technologies, and financial assets.

Protection:
People solutions & Risk Transfer

We leverage our analyses and global experience to develop a strategic array of best-in-class solutions designed to minimize and mitigate risk exposure; addressing people, technologies and financial assets. We help our clients insure and transfer risk that remain after all mitigation is in place.

Recovery:
Incident resiliance

We remain uncompromising in protecting our clients even after a cyber incident occurs, by the speed with which we provide support, recover losses, and provide deep forensic analysis to learn causes and quickly develop new defensive solutions.

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

17128/04/17

willistowerswatson.com

Willis Towers Watson