Cyber Insurance for Asset Management Industry

Cyberattacks, operational errors or technical failures have the ability to paralyze an organization leading to significant financial loss, regulatory actions and fines, halt productivity or operations and create lasting reputational harm. At Willis Towers Watson we strive to provide end-to-end solutions to mitigate organization's cyber risk.

Challenges arising from cyberattacks

Financial institutions will always be targeted by hackers. Regulators will continue to focus on how fund managers will protect themselves and investors against the threat and the potential loss arising out of or caused by a cyberattack. The challenges that cyberattacks bring to fund and hedge fund managers can be illustrated by claims statistics and explained by regulatory trends.

Financial significance of cyberattacks

The 2020 Claims Analysis Report published by Willis Towers Watson show the prevalence, magnitude and significance of cyber events. The headline figures on the right suggest the financial significance.

Figure 1. Headline figures of cyber claims

Analysed claims	1150+
Average event cost	$4.88m
Median event cost	$103k

Regulatory trends

The tightened cybersecurity regulations around the world will substantially increase financial consequences in the event of cyberattacks. Particular to prominent Asian hedge fund hubs, in Hong Kong, the reform proposals to combat doxxing were presented to the Legislative Council in January 2020. In Singapore, adherence to the Cybersecurity Act and the upcoming amendments to Personal Data Protection Bill play a significant part in hedge fund operations.

How cyber insurance helps: Transferring cyber risk

The transfer of cyber risk through the purchase of cyber insurance will help protect an organization's balance sheet when faced with a cyber event, and as such, should be part of any organization's holistic cyber risk strategy.

Figure 2. Key cyber exposures and the applicable cyber coverages

Key Cyber Exposures	Applicable Cyber Coverages
Loss of data – PII, PCI, breach of any data protection legislation	Breach response costs (includes legal, crisis management and notification/credit monitoring costs) and security and privacy liability
Regulatory compliance, investigations and fines	Legal costs/compliance costs/Regulatory fines
Cloud or third-party compromise	Vicarious liability
Ransomware	Extortion costs/ransom specialist/legal costs
Liability from website/multimedia activities	Legal costs/damage from liability arising from multimedia activities
Network security breach/malware attack	Forensic IT specialist/Data and computer system reconstruction

Willis Towers Watson is a recognized specialist at placing programmes for fund and hedge fund managers and we seek to provide insurance solutions for the liabilities you face. We can arrange the following either on a stand-alone basis or as a combined package, helping fund and hedge fund managers to manage the array of liabilities they are exposed to in their daily business.

Third-party liability coverage

Privacy liability and outsourcing liability: Liability associated with your inability to protect personally identifiable information or corporate confidential information of third parties. The information can be in any format and breached intentionally or negligently by any person, including third-party service providers to which you have outsourced information. Third-party service providers include, but are not limited to, IT service providers.

Network security liability: Liability associated with your inability to prevent an attack against your computer network.

Media liability: Tort liability associated with content you create, distribute or is created and distributed on your behalf, including social media content.

Crisis costs and expenses

Privacy breach costs: Direct costs expended to mitigate a privacy breach. Costs typically include public relations expenses, notification cost (to regulators and to Data subject, credit monitoring services and forensic/remediation expenses).

Pro-active forensic costs: Forensic investigation. Hire external IT- experts to determine the incident, making recommendation as to how to mitigate and contain the security breach.

Repair reputation: Hire public relations firms to prevent and mitigate the potential adverse effect post breach, including design and management of a communication strategy.

Regulatory costs and expenses

Regulatory and Data/Privacy reporting and investigation costs: Costs incurred in the assessment of adherence requirements to regulation of self-reporting in the event of a cyber incident or data breach. The costs incurred in notifying regulators of a cyber incident and data breach, the costs involved and fines arising from an investigation resulting from a cyber incident and/or data breach.

First-party coverage

Data and computer system reconstruction: Your costs to recreate, recollect data lost, stolen or corrupted due to your inability to prevent an attack against your computer network.

Extortion costs: Your costs expended to comply with a cyber extortion demand and the extortion specialists to give advice and to meet, eliminate an extortion threat.

Claim scenarios

Scenario 1: The laptop of a Fund Manager's employee, containing sensitive Investment strategy and Investors data, went missing. Upon forensic IT specialists' application of sophisticated data monitoring processes where put in place, it was discovered the data had been compromised. Multiple lawsuits ensured by Investors whose data has been compromised, additionally regulators, conducted an investigation to assess if their cyber minimum due diligence and corporate governance and reporting regulation had been adhered to. The insurance pays out the costs of the forensic specialists monitoring costs, legal costs in complying with the regulatory filing and legal cost of complying with the investigation and defending the lawsuits and ultimately any damages awarded against the manager.

Scenario 2: A Fund Manager experienced a sophisticated malware attack, where hackers encrypted their system preventing from retrieving data, accessing their current trading positions and trading. The insurance paid for the forensic IT to assess, quantify and report on the strength and impact of the malware, the cost of a third-party negotiator with those making the ransom. Ultimately the malware was deemed to be weak enough to be resolved by forensic IT, the data retrieved and the positions and NAV to be regenerated by back up files. The insurance paid of the forensic IT to assess, quantify and stem the malware, assess the ransom position and important assess no outflow of data. Additionally, it paid the legal costs in assessing and complying with regulatory filing requirement.

Scenario 3: A Fund Manager's employee resigned, and it was discovered the employee had emailed himself a spreadsheet with confidential trading information. An anonymous email was sent to investors sighting intricate details of the trades with minor changes to sight the trades breached SFO regulation. The insurance paid for an independent forensic IT and legal audit to assess where the information had been leaked, assess the trades and rebuff the allegations in the malicious anonymous email to investors.

Willis Towers Watson

How cyber insurance helps: Incident management

The following chart plots out how, from the first point of contact on the policy, the respective specialist parties are enlisted to play their separate roles.

It is important that before you get to this point, you have an internal “playbook” which clearly sets out how information and respective responsibilities are defined between individuals and external stakeholders. We can arrange for this consultancy as part of our offering.

Figure 3. Generic flowchart to typical cyber event notification

Incident	Initial	5 Hours	24 Hours	48 Hours	48-72 Hours
• 24/7/365 Notification • Incident manager appointed • First response to insured	• Appoint specialists • Triage calls with stakeholders • Commence investigations • Immediate mitigations • Policy coverage reviewed • Clear discovery plan emerges	• Investigations well underway • Initial indications emerging • Immediate mitigations continuing • Regular updates to stakeholders	• Initial investigations concluding • Regular updates to stakeholders continuing • Policy coverage view emerging • Immediate mitigation work maturing • Clear solution plan emerging	• Ongoing monitoring of the incident management • Taking the necessary steps in relation to the authorities • Executing the action plan	

Why Willis Towers Watson? A global cyber team

Willis Towers Watson is a leading innovator in addressing the changing risk landscape through solutions and services designed to help organizations mitigate the myriad of risks they are facing today. At Willis Towers Watson, we strive to provide innovative solutions using our unparalleled analytics and people solutions to not only identify exposures, but also to find meaningful solutions to transfer that risk. The transfer of the risk through the purchase of cyber insurance will help protect an organization’s balance sheet when faced with a cyber event, and as such, should be part of any organization’s holistic cyber risk strategy.

Figure 4. Global Connectivity – Highly experienced, dedicated FINEX cyber/E&O consultants, placement brokers and Claim Specialists

How Willis Towers Watson helps – Our cyber risk solutions

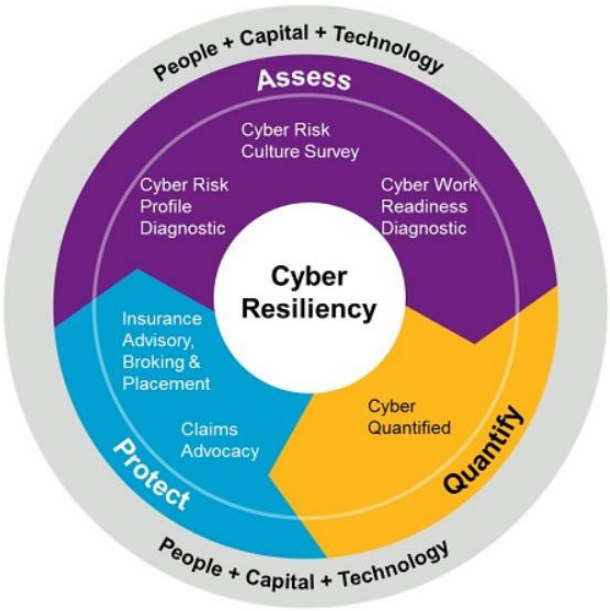
We have developed a suite of offerings ranging from risk identification and assessment tools, to core analytics, to risk transfer, and to post-breach crisis management solutions.

Our holistic vision will provide end-to-end solutions to mitigate your cyber risk.

Cyber risk profile diagnostic

Measures your cybersecurity practices against the NIST

- Cybersecurity framework or ISO “gold standards” to rapidly identify your greatest cyber risk areas
- Clarifies, in an easy-to-understand format, which cybersecurity investments would provide the greatest cybersecurity bang for the buck given your company’s unique cyber risk circumstances
- Can be applied to supply chain and other vendors, extending your company’s cybersecurity perimeter to potentially its weakest link(s)



People – Market-leading human capital consultants and risk advisors

Capital – In-depth risk quantification through modeling and analysis

Technology –Innovative advisory services provided through leading-edge technology

For more information, contact:

Martin Giggins

Martin.giggins@willistowerswatson.com

+852 2195 5633

Joanne Liu

Joanne.liu@willistowerswatson.com

+852 2195 5632

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. 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.