sedgwick®

Cyber claims services

Experts in insurance – Asia

Overview

Cyber and technology incidents can cause considerable difficulties and substantial costs for businesses and insurers, as well as providing a stark reminder of the fragility of business dependent systems.

To handle cyber claims you need a comprehensive understanding of technical issues and a calm and organised approach. Remediation options need to be swiftly investigated and evaluated, while costs must be kept under control. If not handled properly, cyber claims can disrupt and damage businesses' brands and reputations.

Consistent approach

An important aim of our approach to cyber and technology risks is to demystify the subject. We support businesses through to recovery and conclusion during a period when they are suffering disruption and loss.

We have a global reach

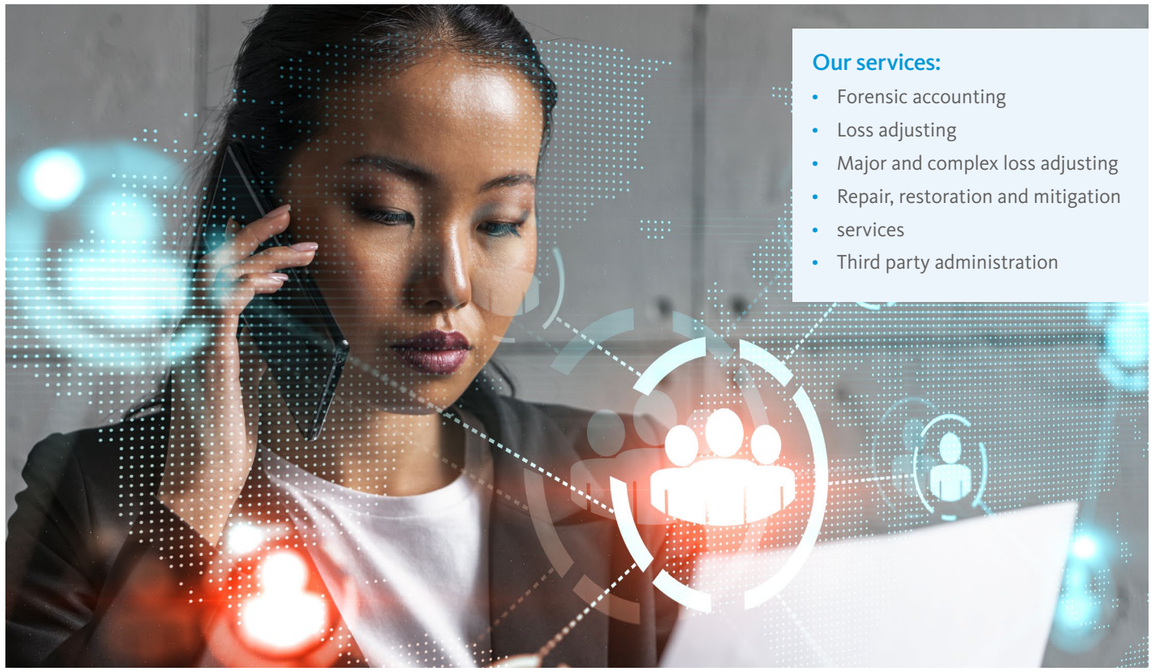
Sedgwick is the world's largest risk services, loss adjusting and claims management company. We offer expert and impartial advice to insurers, brokers and customers across the whole insurance industry.

We provide focused solutions that contribute to our clients' success and inspire continued brand loyalty in their customers. With over 21,000 employees worldwide, our services are enhanced by our collective global experience and expertise.

Contact us

Whether you are looking for high volume claims management, complex loss adjusting, third party administration, risk consultancy or repair and restoration, you can rely on us to get the job done.

We get the right people, in the right place, at the right time. To find out more about how we can help you and your customers, please contact a member of our team or visit our website at Sedgwick.com.



Our services:

- Forensic accounting
- Loss adjusting
- Major and complex loss adjusting
- Repair, restoration and mitigation
- services
- Third party administration

Our cyber solution

To make sure your customers receive a prompt service of the highest standard, we have brought together a network of services to manage all elements of cyber claims.

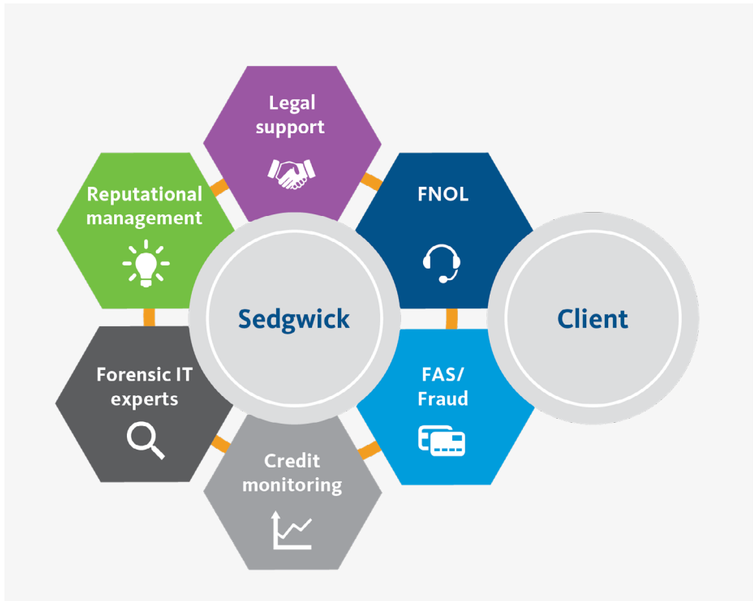
Loss adjusting

Our MCL Global team is made up of 36 of our most experienced adjusters, dedicated to managing major and complex losses in a variety of disciplines, including cyber. Having witnessed an increasing number of cyber related incidents, we have spent the last three years training and developing members of the team, so we can manage our mclients' cyber claims effectively.

When managing cyber claims, we know the speed of our response is crucial. Our adjusters will quickly identify cause, deploy mitigation strategies and bring in specialist experts when needed to help manage the claim. We have cyber adjusters in 7 countries across the region, so we make sure clients get the right resource working on the incident as quickly as possible. Our team is also experienced in recovery procedures, so if a recovery action is possible, we'll get you the best results.

We have also made a significant investment in our global cyber capabilities. We have set up a dedicated cyber and technology Specialist Practice Group (SPG) to ensure our processes are aligned and up-to-date with the global cyber market.

Our SPG is led globally by world renowned technology specialist, Dr. Mark Hawksworth.



Forensic accounting

Our team of experienced forensic accountants are specialists in quantifying economic loss under insurance policies.

We have vast experience in quantifying cyber, loss of income, crime and other financial losses.

Like our MCL Global team, our forensic advisory team has gained extensive experience in managing cyber losses over the last three years, having managed claims either in conjunction with MCL Global or as a standalone service. Our specialist team has three accountants in Asia, and is part of the global team of specialists.

24-hour customer service and third party administration (TPA)

Our staff are well versed in determining whether a cyber incident has taken place, and have access to the right expert resources within our business to call on when needed. We also have extensive experience in claim and stakeholder management, ensuring excellent claim service to your customers.

We will continually develop the service throughout our partnership, to meet your and your customers' current goals and your future goals too.

Engaging the right experts

When managing cyber claims, we understand the importance of working with specialist experts to determine cause, develop mitigation strategies and recommend rectification.

Our teams have worked with a number of industry recognised experts in the following fields:

- Data and credit monitoring
- Investigative Response (IR) and digital forensics
- Legal
- Public Relations (PR) and crisis management

We know many insurers often have pre-agreed supplier arrangements in place, so we can either work with your existing suppliers, or we can recommend experts with whom we have pre-agreed terms in place.

Data and credit monitoring

When personal data has been compromised as a result of a data breach, our data and credit monitoring partner will monitor affected personal information across the open and social web, as well as black market forums that trade in stolen data.

To help mitigate the risk of identity theft, we notify individuals immediately if we find data which matches theirs.

Investigative Response (IR) and digital forensics

Due to their complex nature, cyber claims often require IR and digital forensics expertise to ascertain the extent of loss, mitigation, rectification requirements and forensic analysis.

Our teams work with a number of firms to assist in the investigation of cyber incidents, with experts available to help with:

- Digital forensics
- Electronic data recovery
- Electronic discovery
- Executive breach simulation
- Fraud trend analytics
- Incident response
- Incident response training
- Litigation support
- Malcode analysis
- Security health checks

We have agreed terms in place with these types of firms, or we're happy to work with any of your preferred suppliers.

Legal

Cyber claims often have legal complexities, so it is sometimes necessary to seek legal advice. Our legal partners help with:

- Conducting litigated claims and recoveries
- Regulatory interventions
- Legal enforcement options – contract and intellectual property breach, defamation, privacy, trademark and copyright infringement etc.

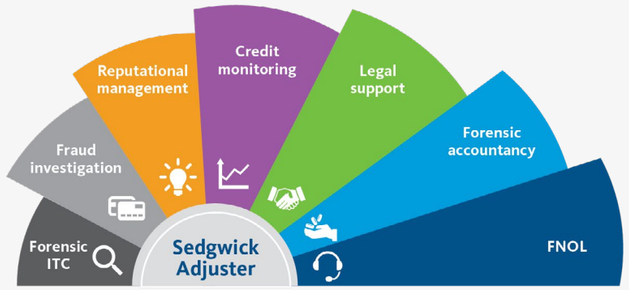
Our legal partners are closely following the introduction of new local Mandatory Legislation within each country to ensure they are ready to provide advice, when required.

Our adjusting team works closely with legal teams in all areas of insurance and have built strong relationships within the industry.

Public Relations (PR) and crisis management

Communicating a data breach to customers and the public can be a complex matter, so a good PR and crisis management firm is essential for preparing and managing communications around a data breach resulting from a cyber attack.

We have partnered with a specialist firm to help mitigate reputational fallout and make sure the right message is delivered to customers and the public. We work with our PR and crisis management partner and insurers' own providers to develop clear decision-making processes to communicate quickly and thoughtfully following a data incident.



Case studies

The following case studies are examples within the MCL Global division

Case Study 1 - Ransomware

This company manufactures tools for the drilling, mining and construction industry. They received a phone call from their manufacturing staff advising that the programme their machines needed to operate had been converted into another format. They immediately contacted their IT provider to investigate the cyber event.

The IT provider discovered which computers were impacted by the event and disconnected the computers from the network. The cause of the cyber event could not be identified at first, so the company sent a number of computers to their IT provider for further investigation and repairs. On further investigation, the IT provider discovered the company's systems had been infected by a CryptoLocker virus. The IT provider was able to recover a portion of data from the computers, but the majority had to be reprogrammed.

As a result of the incident, the company experienced loss of productivity for several days They claimed for the cost of the manufacturing hours lost, wages which continued to be paid and additional costs for the transportation of computers to and from the IT provider. We were engaged by insurers to review the claim and assist the company and their IT provider where necessary.

We found the manufacturing costs relating to lost production hours did not translate to a shortfall in revenue.

Also the administrative wage costs claimed by the company related to ordinary costs, rather than additional overtime costs. As a result these claims were not covered by the policy.

Only the cost of the IT provider's work was settled as presented.

Case Study 2 – Hacking

This company operates an accounting firm specialising in wealth planning, tax assessments and consulting and business structuring. They discovered that a number of important client files had been deleted from their IT infrastructure. They immediately employed the services of their IT consultants, who performed a review of Windows logs, and ran anti-virus and anti-malware software. However, the IT consultants were unable to find any evidence of malicious activity.

We appointed our Investigative Response (IR) firm to perform further detailed analysis of the company's systems. By comparing data from before and after the incident, our IR firm confirmed that around 80GB of data was missing from the company's hard drive.

The IR firm performed further investigations by examining users who had accessed the systems in the days leading up to the deletion of files. It was discovered that a legacy account, no longer used by the company or any of their staff, had breached the system from Ghana, where no authorised person had access. They also discovered a number of potentially malicious files throughout the company's infrastructure. While the root cause of the intrusion hadn't been investigated, it was evident that the company had experienced a cyber event.

As a result of the event, the company had experienced a reduction in turnover as they were unable to perform to normal volumes for around two months. Our forensic accountants looked at the company's financial performance over the previous 12 months to calculate the financial cost of the reduction in turnover, and the claim was settled on that basis. The claim for the company's IT consultant costs was also settled as presented.

Case study 3 – Man in the middle attack

This company operates a medical centre providing a variety of health services, including general medical, men's and women's health services and counselling.

They were performing a number of online banking transactions, including several large payments to third party accounts. One of the third parties advised the medical centre that they had not received the funds.

The company immediately reviewed their online banking transactions.

Despite having a two-level authorisation process, they discovered someone had intercepted the payment between the first and second authorisation points.

The recipient's bank details had been changed and two payments were re-directed to other unauthorised accounts.

The company immediately contacted the fraud department of their bank and their IT consultant. The company's IT consultant found that whoever had stolen the money had attempted to cover their tracks by infecting the company's IT infrastructure with a CryptoLocker virus.

The virus encrypted a number of files, rendering individual computers unusable. The company's IT consultant began cleansing each system and server to remove any trace of the virus.

We engaged with our Investigative Response (IR) partner to complete a full review of the company's IT infrastructure in collaboration with their IT consultant.

Our IR firm discovered four different IP addresses in China and Indonesia, which had gained unauthorised access to the company's systems.

Our IR partner recommended that the company increase its infrastructure security, including adding firewall rules, reducing individual user privileges and tightening the rules around account passwords.

They also recommended the company rewrite its back-ups/disaster recovery, cloud back-ups and image-base back-ups for each machine to include Virtual Service Replication.

Following their review, the company's bank refunded the stolen money, and we settled the claim for the IT consultant and IR partner costs as presented.

Case study 4 – Third party data centre supply chain failure

This company outsources data storage to a third party IT infrastructure provider with a data centre which houses a Distributed Control System (DCS).

The DCS is responsible for receiving and allocating client information to the data centre.

The data centre experienced a catastrophic failure, which caused their Network Attached Storage (NAS) array to detach from the DCS. As a result the DCS failed, causing the data centre to become offline, leaving the company without their outsourced IT functionality – databases, communication portals and billing services – for almost three days.

We were appointed to manage the following aspects of the claim:

1. Investigating the cause of the outage and whether it was a cyber incident

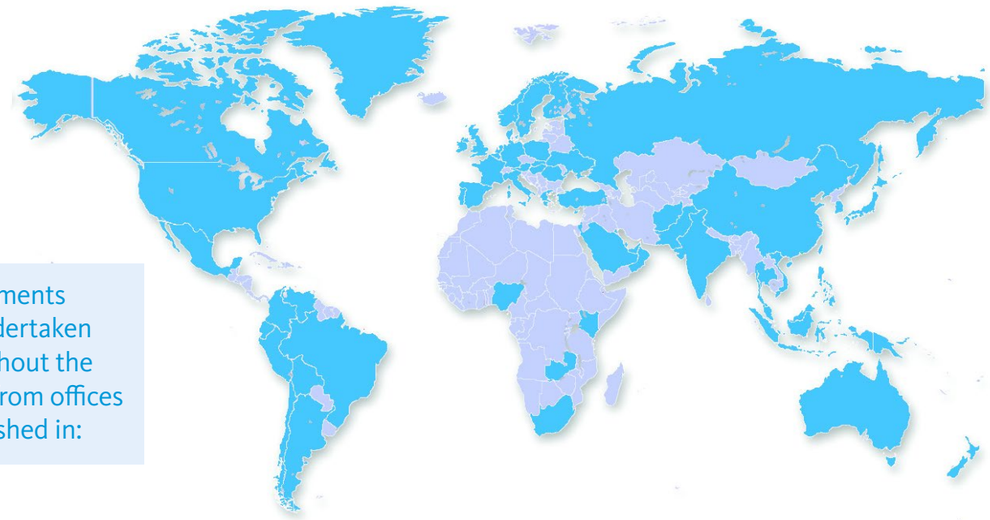
2. Investigating the contract terms with the IT infrastructure provider to determine the extent to which they could be held liable for losses

3. Making sure the necessary steps were taken to reinstate service and mitigate losses

4. Quantifying losses associated with the rebuilding of lost data and reduction in turnover using our specialist forensic accounting team.

Global network coverage

Sedgwick is a truly global organisation operating in over 65 countries, offering a fast, efficient and consistent service from our operating platform around the world with more than 21,000 colleagues.



Assignments are undertaken throughout the world from offices established in:

Regional Resources

James Ong	Chief Executive Officer - Asia	+65 8126 9698	james.ong@sedgwick.com
Ben Chin	Chief Operating Officer - Asia	+65 9781 3318	ben.chin@sg.sedgwick.com
Linda Sim	Head of Forensic Advisory Services - Asia	+65 9728 8880	linda.sim@sg.sedgwick.com

Country Managers

Patrick Au	Senior Manager - Hong Kong	+852 9101 1743	patrick.au@hk.sedgwick.com
Ivor Khong	IT Support Associate – Singapore	+65 9680 0896	ivor.khong@sg.sedgwick.com
Higurashi Shogo	Adjuster - Japan	+81 80 7364 7290	shogo.higurashi@jp.sedgwick.com
Thatchawut Chaychayanon	Manager - Thailand	+66 81 400 6460	thatchawut@th.sedgwick.com
Arisandi	Adjuster - Indonesia	+62 852 2899 0313	arisandi@cl-int.com
Vincent (Kyunghyun) Kim	Director - Korea	+82 10 3088 0458	vincent.kim@kr.sedgwick.com
Joseph Lee	Claims Manager - Korea	+82 10 4107 6423	joseph.lee@kr.sedgwick.com
Chin Lit Ching	Assistant Manager - Malaysia	+60 19 387 6870	litching.chin@my.sedgwick.com
Venodthan Gunandram	Loss Adjuster - Malaysia	+60 163 503 391	venodthan.gunandram@my.sedgwick.com
Lisa Kuo	Manager - Taiwan	+886 9 1934 1208	lisa.kuo@tw.sedgwick.com
Swing Sun	Assistant Manager - Taiwan	+886 9 1934 1185	swing.sun@tw.sedgwick.com
William Huang	General Manager - China	+86 138 1668 8658	william.huang@sedgwick.cn
Barry Yang	Director, Head of International Claim Services - China	+86 139 1612 7304	barry.yang@sedgwick.cn

Global solutions.
Local expertise.