Charles Taylor Adjusting

# Cyber Risk Services

Our global team of over **55 specialist adjusters** provide a holistic approach with full cooperation between industry teams covering aviation, marine, natural resources, property, casualty, technical and special risks and recognised service providers.

They have a great understanding of the potential risks, both financial and reputational, which can stem from such incidents.

# Adapting to your needs

**Charles Taylor has handled cyber claims since 2014 and our services have continuously developed to cover all types of cyber incidents from initial notification to final resolution.**

Cyber risks remain one of the greatest threat's businesses face and overall costs as well as business interruption and physical collateral damage is often underestimated. Cyber policies have evolved but there are still some disparities, overlaps and gaps. Lloyd's is leading the way towards affirmative covers.

As businesses are becoming increasingly aware of their potential liabilities and pressures under new regulations, there is a growing demand for covers to be more adaptive and for support services to meet client's needs.

# Cyber Claims Service

**Charles Taylor's Global Cyber Team delivers an immediate response to any cyber incident, managing the entire process end-to-end.**

**Our expertise:**

- Expertise across thousands of claims involving cyber incidents ranging from ransomware, data breaches as well as Tech professional indemnity, social engineering and crime.
- Ongoing training (internally and with panel vendors) enables us to respond to moving tactics from threat actors and provide specific responses on new major incidents.
- Multi lines specialty; adjusters come from various fields of expertise which allows us to consider complex losses in the context of sophisticated operating systems and commercial operations (i.e. BIM and SCADA).
- A dedicated team of business interruption (BI) specialists and forensic accountants with knowledge of cyber-related BI work to quantify claims.
- A dedicated team of multilingual adjusters across regions ready to assist in cross-border incidents 24/7.

Charles Taylor Adjusting

# Incident Management Services

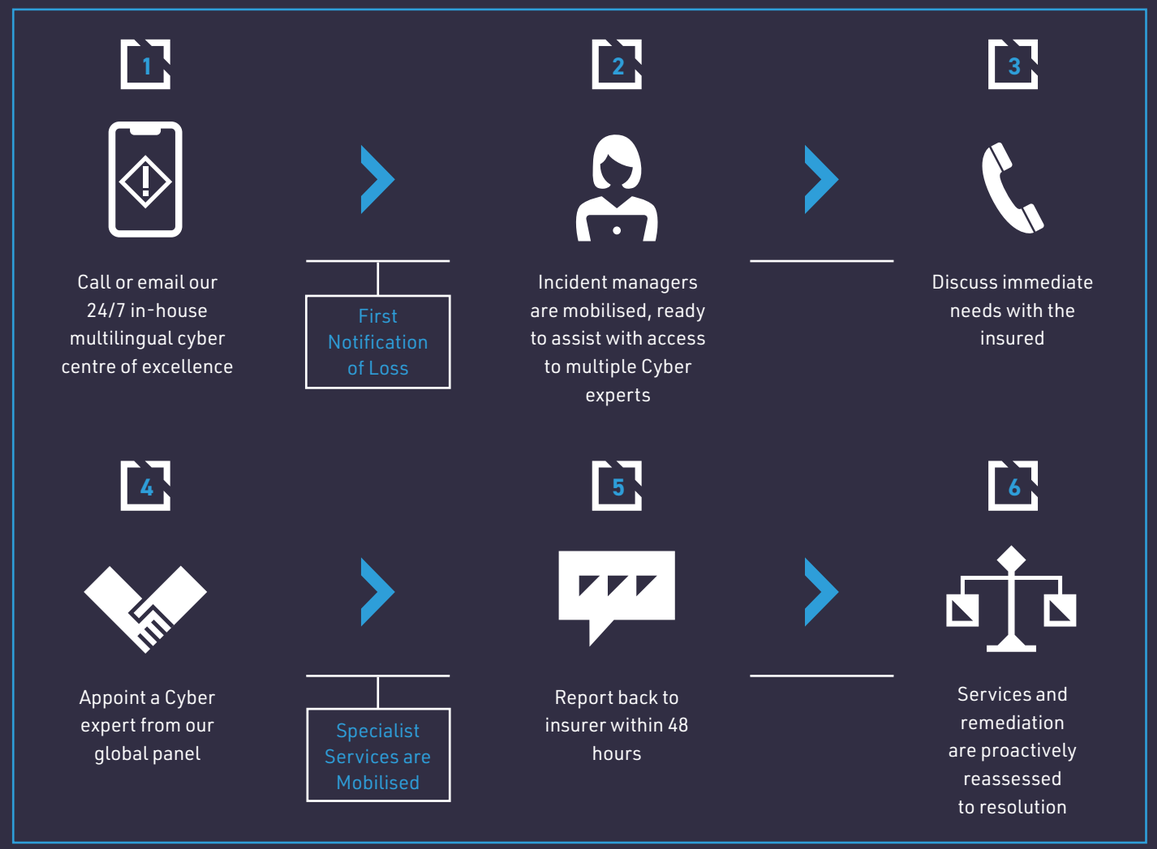
**Charles Taylor has built long-term relationships with insurers and brokers and has had the benefit of working with a wide range of high-quality vendors with a global reach in various fields.**

**We offer cyber claims management that you can trust to deliver a rapid response, minimising any negative impact on client operations.**

## The role of the Charles Taylor Incident Manager

Each claim is assigned a dedicated Incident Manager they focus on:

- Project Managing the claim from initial notification through to resolution.
- Assessing the need for expert assistance and ensuring seamless interaction between the various parties (internet telephone service providers, IT forensics, lawyers and the insured).
- Stabilising the incident and providing the insured with support as well as looking at solutions to minimise negative impacts such as loss of revenue and/or reputational harm or third-party claims.




Charles Taylor Adjusting

## Our vendors

### IT Forensics

Provide specialist support in determining the nature and scope of the incident and need for remediation/restoration work including ransom negotiators and bitcoin wallet holders.

ankura · ASCERIS · BreachQuest · CROWDSTRIKE · CYBERSCOUT · Grant Thornton · KIVU · KROLL · PRAGMA

### Law Firms

Data Protection specialists assist with notifications to Professional/Market Regulators and responses to third party claims.

CMS Law.Tax · DAC BEACHCROFT · Kennedys · simmons+simmons

### In-house Services

Through our Third-Party Administration (TPA) and Assistance services we can provide support with claims and loss funds management as well as call centre set up.

Charles Taylor

Charles Taylor Assistance — charlestaylor.com/assistance

Charles Taylor TPA — charlestaylor.com/tpa

### Public Relations and Crisis communications specialists

Provide communications support as well as monitoring market changes which may harm an insured's reputation.

CRISOTECH BY FLANDRIN TECHNOLOGIES · FLEISHMANHILLARD

### Credit Monitoring

Offered to affected data subjects.

CYBERSCOUT · EQUIFAX · experian

**We regularly add new vendors to our panel of experts.**

# Bespoke Adjusting Services

**We offer a bespoke adjusting service for damage suffered as a result of a cyber incident:**

- Triaging and reviewing the incident circumstances, analysing root cause and causation.
- Collating all technical reports and other loss information from the insured.
- Adjusting remediation costs, including IT repairs and crisis management as well as legal notifications.
- Adjusting business interruption claims.
- Considering potential recovery actions and likelihood of success.
- Commenting, as appropriate, on potential loss-associated coverage-related issues.
- Preparing quantum report(s).
- Attending negotiation meetings/calls if necessary.

**Appointing a specialist cyber adjuster makes a huge difference on how a cyber incident is managed, its outcome and financial exposure.**

Our specialist team has the benefit of having highly trained professionals in business interruption assessment as well as forensic accountants who work hand in hand with the appointed adjuster, to ensure reputational harm and financial exposure are reduced and the business returns to normal as swiftly as possible.

Charles Taylor Adjusting

# Cyber Case Studies

Charles Taylor Adjusting

## A costly voyage

**Sector:** Marine
**Type:** Ransomware

**The insured, a shipping company, was contacted by their Internet Service Provider (ITSP) as they had identified issues with one of the insured's servers. On further investigation the ITSP discovered two servers had been encrypted, the system had been accessed via an employee's email account. The servers contained financial and operational software as well as shipping information and personal details of several hundred crew members from various countries.**

### Our response

We deployed our IT forensics team to provide initial advice on evidence preservation and options available to resolve the incident. No ransom was paid as recovery via backups was possible. The forensics team established that no exfiltration had occurred, and no data had been accessed. Lawyers were engaged and confirmed that there was no need to lodge any legal notifications.

Solicitors reviewed crew members to determine which countries of origin required urgent notification.

## A travel shambles

**Sector:** Travel
**Type:** Data Breach

**Due to an IT misconfiguration on the insured's, a travel agent, website personal client data, including passport and address information, were publicly available via Google and Bing searches. Initial analysis confirmed that this was a notifiable data breach affecting 20-40 of the insured's clients.**

### Our response

Legal, PR and IT forensics were appointed to assist the insured. A forensic investigation established that 3,200 UK and international data subjects had had their data compromised. The legal team reported the breach to the Information Commissioner's Office (ICO) on behalf of the insured and provided advice and support throughout.

The ICO requested information on the incident but were confident that the insured was complying with remediation requirements. PR specialists managed the notification process to the relevant data subjects to mitigate reputational damage.



## A dubious link

**Sector:** Financial Services
**Type:** Email Compromise

**A fraudulent email containing a malicious link to a Request for Proposal document was sent from an Executive VP at the insured, an insurance broker, to their contact list. The link led to a Microsoft OneNote login/password request page. A number of staff clicked on the link, and one entered their credentials. The email was determined to be suspicious, and it was confirmed that the VP wasn't the author. Staff were advised to delete the email and not to click on the link.**

### Our response

Our IT forensics team confirmed that no data privacy breach or third-party loss exposure had occurred. A communication to all policy holders was issued on the same day to ensure customer retention. On recommendation the insured appointed an independent forensic investigator to review their system to ensure there was no longer access to the system.

## Grinding to a halt

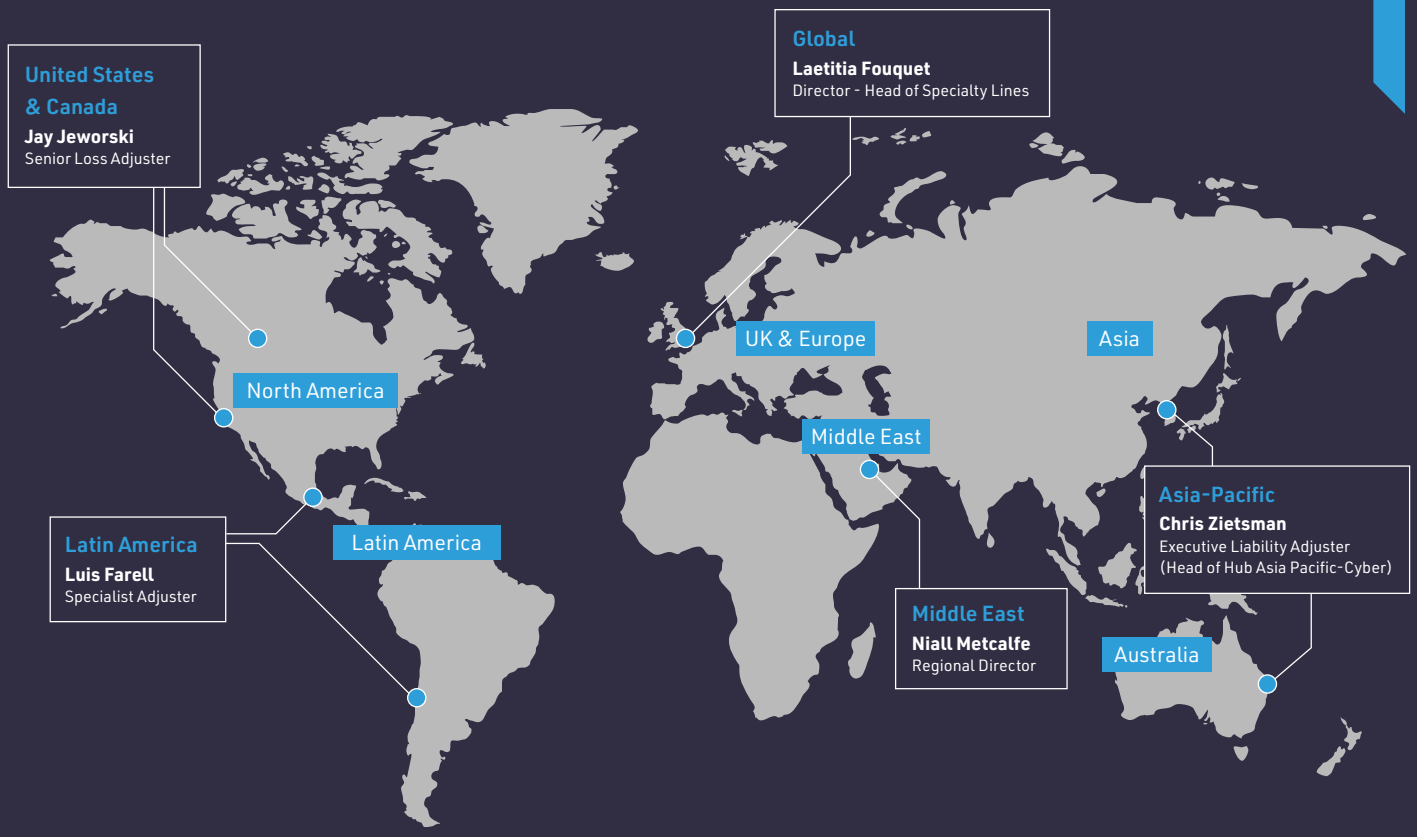
**Sector:** Construction and Transport
**Type:** Ransomware

**A ransomware attack on a shared server at the insured, a SME in construction and transport, encrypted all the shared files. Staff at the insured were unable to access files or emails which meant the company was effectively unable to trade. The insured's own IT support was able to restore the encrypted files using the latest daily back-ups but, they were unable to prevent further attacks being attempted.**

### Our response

An IT forensics team was appointed to review the situation and prevent further attacks. They quickly identified the issues and made recommendations to secure the system and prevent further attacks. Our internal forensic accountants assisted in determining the insured's Business Interruption loss.

# Cyber Team Key Contacts





### Global Head

**Laetitia Fouquet**, ACILEx
Director - Head of Specialty Lines
T: +44 207 015 2024
M: +44 782 793 7786
E: laetitia.fouquet@charlestaylor.com

### Latin America

**Luis Farell**
Specialist Adjuster
T: +52 55 3000 1880
M: +52 1 55 3223 0038
E: luis.farell@charlestaylor.com

### Asia-Pacific

**Chris Zietsman**
Executive Liability Adjuster
(Head of Hub Asia Pacific-Cyber)
T: +61 738 399 999
M: +61 455 600 334
E: chris.zeitsman@charlestaylor.com

### United States & Canada

**Jay Jeworski**, BBA, PMP, FCIP, CRM
Senior Loss Adjuster
M: +1 403 819 1946
E: jay.jeworski@charlestaylor.com

### Middle East

**Niall Metcalfe**
Regional Director
T: +44 2038 898 233
M: +971 52 350 4526
E: niall.metcalfe@charlestaylor.com


Charles Taylor Adjusting

For more information visit: charlestaylor.com/adjusting

Charles Taylor

@CTcharlestaylor

@ctcharlestaylor