Cyber Event Claims Management

Crawford Cyber Solution

Crawford & Company

World's largest publicly listed independent provider of claims management solutions

Organized across global service lines:

- ✓ P&C adjusting solutions (Crawford Claims Solutions)
- ✓ Large or complex claims (Global Technical Services)
- ✓ Global TPA solutions (Broadspire)
- ✓ Managed repair services (Contractor Connection)

$14 Billion
Claims Payments Annually

7.1 Million
Claims Handled Worldwide

9,000
Total Employees

CRD A&B
Low Debt Ratio
Traded on NYSE

Crawford Cyber Solution

Two parallel and complementary service models

Global Incident Response and Loss Adjusting
Key components comprise 24/7 FNOL, access to our accredited Incident Managers and contracted Experts. This solution is primarily positioned for the Global Corporate market or for larger risks.

SME Incident Response and Claims Management – This model mirrors the Global Incident Response but builds in additional desktop Claims Management capabilities delivered at a local level. In developing this solution we recognise the need for effective and efficient response, whilst still providing access to the services needed to respond to the more complex incident.

Crawford Cyber Solution

- Launched in 2015
- Innovative, first to market
- Truly global, scalable
- Rapid growth, over 30 carriers
- Over 1,000 cyber claims handled to-date

Complete End-to end Turnkey Solution

First Notification of Loss

- Single global intake centre
- Dedicated telephone number
- Available 24/7/365
- 200 languages
- Guaranteed response

Claims Management

- Dedicated, centralised resource
- Trained and experienced team
- Triage to specialists as required
- Management of claim

Crawford Incident Manager

- Single coordinator
- Selected individuals
- Triage to specialists as required

Specialist Provider

- Contracted network
- Extensive range of services
- Best-in-class
- Experienced
- Fast response
- Completed due diligence

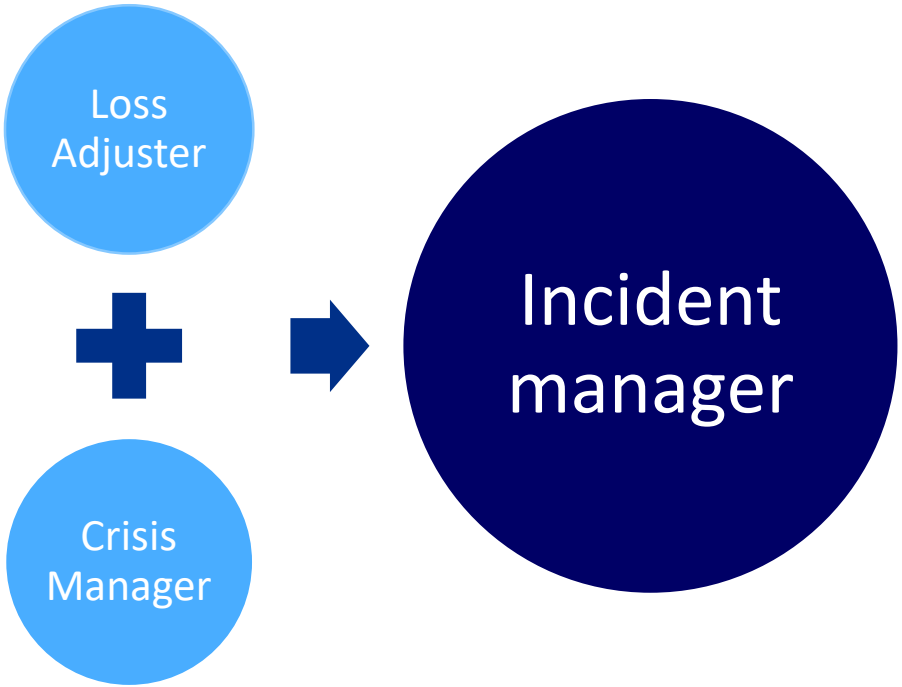
One Global Process

- Timely
- Consistent
- Flexible
- Solution driven
- Global breadth

Backed with a £50m liability cover

Crawford

Crawford Cyber Solution



Response during critical first 48 hours

24/7/365 notification

Incident manager appointed

First response to Insured

Appoint specialists

Triage call/s with stakeholders

Commence investigations

Immediate mitigations

Policy coverage reviewed

Clear discovery plan emerges

Investigations well underway

Initial indications emerging

Immediate mitigations work continuing

Regular updates to stakeholders

Initial investigations concluding

Regular updates to stakeholders continuing

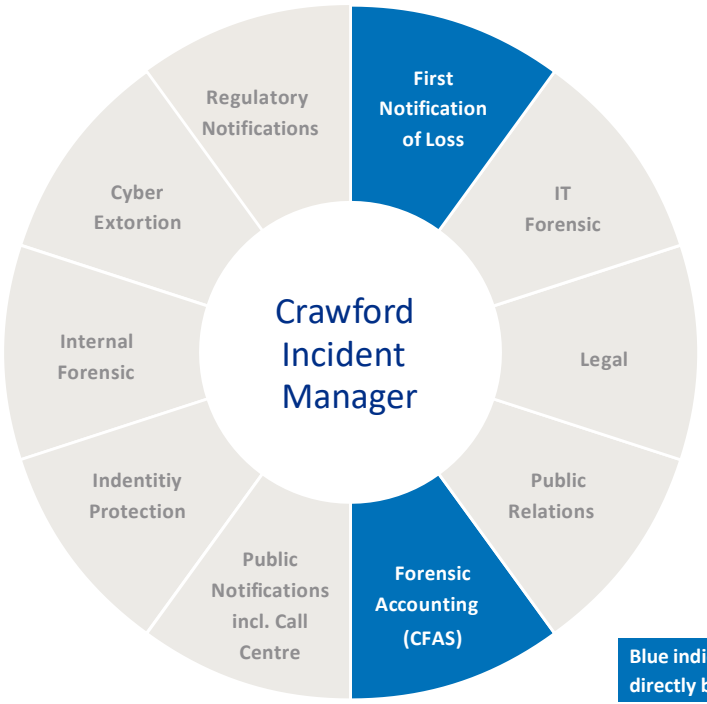
Policy coverage view emerging

Immediate mitigation work maturing

Clear solution plans emerging

Crawford Cyber Solution

Crawford Cyber Solution Wheel



We aim to provide a timely, consistent and flexible response which is solution driven, economic and expert-led.

Blue indicates services performed directly by Crawford

Crawford

Types of Cyber Incidents

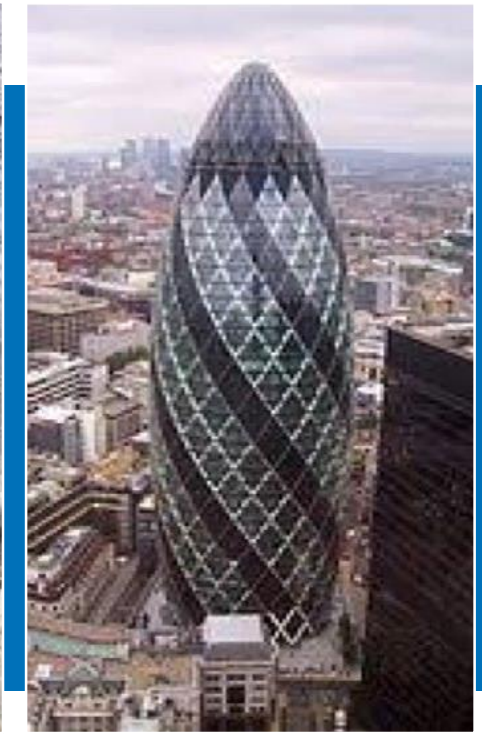
Types of cyber incidents:

1. Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
2. Man-in-the-middle (MitM) attack
3. Phishing and spear phishing attacks
4. Drive-by attack
5. Password attack
6. Eavesdropping attack
7. Malware attack

Case study 1

The cyber attack

- ✓ Design, manufacture and erection of structural steelwork
- ✓ Worldwide client base 10 manufacturing plants
- ✓ Centralised computer system in UK 3D design system
- ✓ Robotic machinery
- ✓ 1 April 2018 – cyber attack, all files are encrypted
- ✓ Ransom demand for £250,000

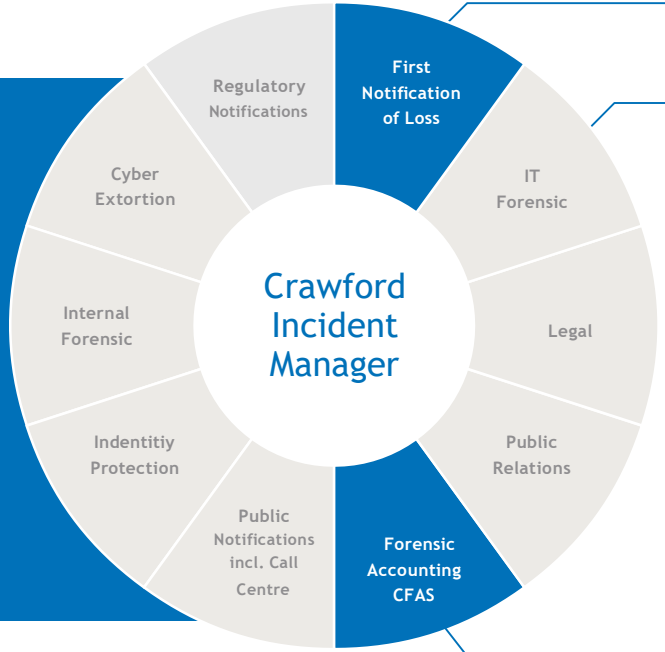


Case study

The Crawford team

File coordinated by Crawford Incident Manager

- ✓ Addressed immediate needs and assembled the team
- ✓ Coordination of response
- ✓ Communication to stakeholders Loss mitigation
- ✓ Worked closely with claims handler to reach resolution



Loss notified

IT specialists

- ✓ Investigation
- ✓ Reconstruction of IT systems
- ✓ Prevention measures

CFAS forensic accountant

- ✓ Early involvement
- ✓ Key drivers of loss
- ✓ Full financial loss estimate
- ✓ Loss mitigation
- ✓ Insured loss calculation

Crawford

Case study

Key considerations – loss mitigation

- ✓ What became apparent very quickly was the risk of a large uninsured loss
- ✓ Management of expectations around coverage
- ✓ Maximise loss mitigation and minimise uninsured financial impact for the policyholder
- ✓ Expert advice to inform broader decisions – legal/regulatory obligations, operational drivers, and reputational risk

The Insured's business

- Sales made through long term tendering process
- Contract based sales
- Penalty clauses for delays

The Cyber BI policy

- Net profit basis
- Three month indemnity period
- £5 million limit per loss (+ sub-limit)

Case study

Key considerations – quantum aspect

Financial data was lost in the cyber attack

- ✓ Published financial statements
- ✓ Discussions with Insured

Loss of sales

- ✓ Quantify
- ✓ Support

Policy considerations wording

- ✓ Net profit wording – potential overlap between BI and other policy sections
- ✓ Ransom demand
- ✓ Policy sub-limits

Case study

Lessons learnt

Benefit of using core forensic accounting skillset

- Unbiased evidence-based approach
- Detailed review
- Accountancy and industry knowledge

But fully integrated with Crawford Cyber Solution

- Crisis Management
  - Mitigation of key business risks
- Collaborative proactive approach
- Good knowledge of product and engagement on policy issues

Case study 2

The Cyber Attack Victim

- ✓ Engineering, procurement and construction for the energy sector
- ✓ Listed on London Stock Exchange
- ✓ Annual gross revenue circa USD 300 million
- ✓ Global client base: Middle East focused operations (onshore & offshore)
- ✓ Centralised computer system based in the UAE Head Office: advanced network with strong security protocols

Case study 2

The Cyber Attack Vector

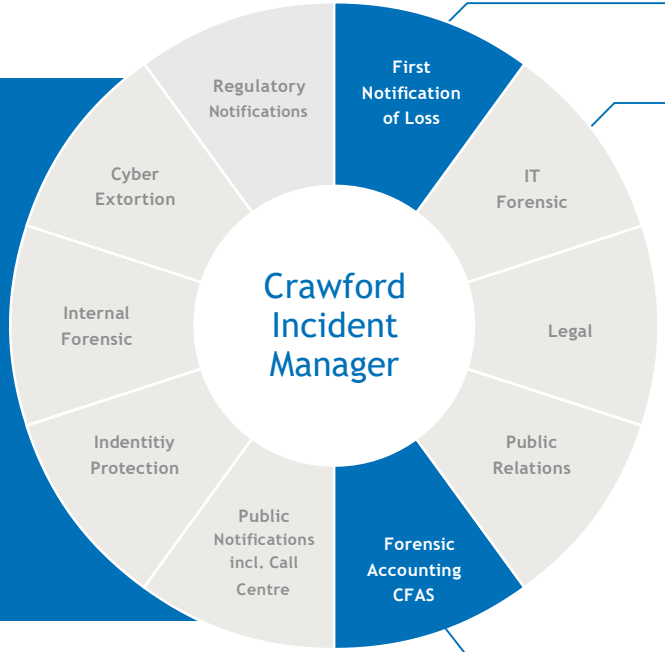
- ✓ 18 June 2019 – cyber attack, all servers encrypted (McAfee) – Workstations (Malwarebytes) unaffected
- ✓ Ransomware attack (RYUK) – no demand posted, only contact details for attackers
- ✓ RYUK is specially engineered to target enterprise environments – creates a privileged user account to spread ransomware to individual hosts within the network. Spread by TrickBot via email (spam) or Emotet malware
- ✓ Information encrypted and backup files deleted – decryption software can be obtained from attacker with ransom payment – no guarantee it will be provided – decryption process is labour intensive and complicated

Case study 2

The Crawford team

Incident Manager

- ✓ Addressed immediate needs and assembled the team
- ✓ Coordination of response
- ✓ Communication to stakeholders
- ✓ Loss mitigation
- ✓ Liaise with claims handler to update on incident and address potential issues



Loss notified: BC & FNOL

IT specialists: Mandiant

Investigation: attack vector & system impact – 3 weeks

Reconstruction of IT systems – 4 weeks

Prevention measures – ongoing

CFAS forensic accountant

Early involvement

Identification of key loss drivers

Assist with preparing loss estimate

Loss mitigation measures

Crawford

Case study 2

Key considerations

- ✓ It quickly became apparent that this was a large scale incident with infiltration of entire system – complete disruption to operations
- ✓ Management of expectations around coverage
- ✓ Maximise loss mitigation and minimise uninsured financial losses
- ✓ Expert advice to inform broader decisions – legal/regulatory obligations, operational drivers, and reputational risk

The Insured's business

- Contract based projects
- Penalty clauses for delays and non-performance
- Future projects secured through long term tendering processes

The Cyber policy

- Gross profit / gross earnings / net income basis and extra expense
- 180 Day indemnity period
- USD 10 million limit per loss
- Comprehensive cover

Case study 2

Key considerations – quantum aspect

Consequences of cyber attack

- ✓ Network disabled but eventually mostly restored from backups except 2 no. servers
- ✓ Data loss – contractual and operational information relating to an ongoing contentious project
- ✓ Commercially sensitive lost (tender bid information)

Business Interruption

- ✓ Difficulty in quantifying impact to business as all divisions and multiple projects affected
- ✓ IM & CFAS supporting Insured with identifying insured and uninsured losses
- ✓ Ransom demands being investigated to recover essential lost data

Policy considerations wording

- ✓ Income loss to be calculated by one of three methods – detailed in Policy
- ✓ The potential BI losses (delay penalties) will mostly be realised after the indemnity period expires

Case study

Lessons learnt – claim ongoing

Benefits of vendor panel

- ✓ Collaborative proactive approach led by IR
- ✓ Specialised consultants provide expert response to obtain best outcomes – IT forensic, legal and accountants / BI specialists
- ✓ Excellent support and guidance for Insured
- ✓ Crisis Management – swift response by specialists
- ✓ Loss mitigation measures – insured and uninsured

Crawford Cyber Solution Contacts

Global Leadership
Paul Handy
D: +44 20 7265 4320
M: +44 7827 879187
E: Paul.Handy@crawco.co.uk

Central Europe
Hector Hamaker
D: +31 10 45 35 599
M: +31 6 55 79 60 95
E: HectorHamaker@crawco.nl

Canada
Neal Jardine
D: +1 416 957 5040
M: +1 416 458 7476
E: Neal.Jardine@crawco.ca

United Kingdom
Mark Harris
M: +44 7860 951 612
E: Mark.Harris@crawco.co.uk

Nordics
Henrik Brandt
D: +47 675 52 500
M: +47 959 38 125
E: Henrik.Brandt@crawco.no

Eastern Europe
Robert Pazikowski
D: +48 22 622 40 14
M: +48 505 121 321
E: Robert.Pazikowski@crawco.pl

Asia
Ian McDonald
D: +852 2101 0915
M: +852 9211 1762
E: Ian.Mcdonald@crawford.asia

USA
Robert Welsh
D: +1 212 824 2475
M: +1 646 627 5713
E: Robert_Welsh@us.crawco.com

Middle East/ Africa
Brian Clark
D: +971 4 223 6370
M: +971 50 144 8874
E: Brian.Clark@crawco.me

LATAM
Jose Goggi
D: +55 11 3879 7559
M: +55 11 9880 01007
E: Jose.Goggi@crawfordbrasil.com.br

Italy
Fabrizio Bufacchi
D: +39 06 42 01 49 49
M: +39 346 60 30 744
E: F.bufacchi@crawco.it

Australia/ New Zealand
Jane Amling
D: +61 392 056 703
M: +61 437 591 040
E: Jane.Amling@crawco.com.au

Spain
Jesús García Fernández
D: +34 933 900 747
M: +34 619 419 400
E: Jgarcia@crawford-spain.com

Crawford

Crawford

Derek Patterson

Regional Technical Director

Middle East

T: +971(0) 4 223 6370

M: +971(0) 50 455 0870

E: derek.patterson@crawco.me

Eddie Walsh

Middle East Regional Cyber Lead

T: +971(0) 2 622 8114

M: +971 (0) 56 153 4770

E: eddie.walsh@crawco.me