

Job description

Job title	Cyber Incident Response Manager (London)
Employment type	Full-Time Permanent
Reporting to	Cyber Claims Director
Working hours	9.30am – 5.30pm - Monday to Friday (Role requires out of hours work and potential travel)
Location	85 Gracechurch Street, London EC3V 0AA
Salary	£ Competitive
Bonus	Discretionary Bonus Plan

At CFC we pride ourselves on being an employer of choice. We were delighted to be recognised in the *'Sunday Times 100 Best Companies to Work For 2019'* including a placing within the Top 30 for London!

CFC Benefits include 25 days holiday, private medical insurance (plus dental and optical cashback benefit), life insurance scheme, income protection scheme, pension plan, season ticket loan, subsidised gym membership, employee wellbeing programme (including on-site massages), 24/7 employee assistance programme and dress down Fridays. CFC social events include the summer party weekend, Halloween and Christmas parties.

About CFC

CFC is a specialist insurance provider and a pioneer in emerging risk. With a track record of disrupting inefficient insurance markets, CFC uses proprietary technology to deliver high-quality products to market faster than the competition while making it easier for brokers to do business. Our broad range of commercial insurance products are purpose-built for today's risks, and we aim to give our customers everything they need in one, easy-to-understand policy.

Headquartered in London and backed by Lloyd's, CFC serves more than 70,000 businesses in over 80 countries. We're privately held and growing faster than any of our competitors in the market.

Although insurance is a serious business, our culture isn't too corporate and we never take ourselves too seriously. We are 'one-team' and enjoy a culture of openness and encouragement. We invest heavily in the learning and development of our people and enjoy a fast paced working atmosphere that is friendly, supportive, and fun.

Role definition

With 28,000 cyber policyholders in over 60 countries around the world, we have the largest specialist team of cyber underwriters in the London market and the second largest portfolio by gross written premium. In order to remain at the front of this exciting market it is critical that we continue to innovate with our products and service offerings.

As a result, we are looking to recruit a Cyber Incident Response Manager to lead and manage the cyber incident response team in London. The role will take accountability for delivering a market leading cyber incident response service, managing the London incident response team and developing the team's capability.

You will provide urgent support to insureds' with cyber incidents; advising on the best course of action and performing initial analysis where appropriate. You will also work with, manage and review our extensive network of incident response, forensic, legal and PR vendors to provide insureds' with a high quality and cost effective service.

In addition to this 'front line' support; you'll work closely with our claims, products and underwriting teams in London to deliver improvements to the service and products CFC offer. This includes working on risk management services including desktop exercises and IR plan reviews for insureds.

This role is ideal for someone from a client facing background as a technical consultant with experience in incident handling who wishes to dive into the world of cyber insurance with a leader in the field.

Key responsibilities & Accountabilities

Cyber Incident Response

- Overarching responsibility for information security within CFC and on behalf of our clients, including the management of our Computer Emergency Response Team (CERT) and cyber incident management process;
- Direct and manage the implementation and maintenance of our own internal information security management framework;
- Own and manage the security risks associated with the storage of sensitive client data as part of our cyber underwriting process;
- Provide high quality and efficient support and advice to insureds' with cyber incidents, and providing expertise and general guidance on cyber security matters to internal and external stakeholders as appropriate;
- Work with the cyber claims adjusters to efficiently and fairly review incident claims and coverage;
- Perform preliminary analysis and triage for incidents and help to develop CFCs technical in-house capabilities;
- Overseeing penetration tests and assessing and reporting on the results to the board;
- Act as the primary contact point for emergency cyber incidents;

- Build and share knowledge and experience of the current cyber threat landscape facing both our business and our clients.
- Develop a clear understanding of the potential risks and impacts from a range of threat actors with varying levels of sophistication and communicate these appropriately;
- Develop and implement cyber claims management strategies for most likely loss scenarios;
- Provision of standard IT security advice to cyber clients (“Virtual CISO” service);
- Support cyber marketing efforts, including the development and delivery of presentations and marketing collateral;
- Ensure CFC’s claims department continues to act as an effective TPA for its capacity providers in accordance with binding authority and claims handling agreements, with adherence to Treating Customers Fairly (TCF) and Conduct Risk.

Stakeholder Management

- Actively manage a panel of response vendors during cyber claims incidents to ensure a consistent and market leading response service is offered to insureds
- Work with the incident response, underwriting and products team along with external vendors to develop and deliver a variety of risk management services, tools and products;
- Foster good relationships with policyholders, brokers, underwriters and capacity providers, and drive excellent customer service;
- Liaising with key stakeholders within the business in order to design and evaluate appropriate information security solutions within the business and on behalf of our clients;

People Management

- Effective people management and oversight of the incident response team to ensure the team are able to operate to their full potential;
- Working closely with the Cyber Claims Director, Cyber Claims Manager and Claims Director to drive the strategic direction of the cyber claims and incident response teams to ensure goals and objectives for team members align with our strategic objectives;
- Conducting regular 1:1s with team members, checking in to inspect progress against performance goals/objectives, personal development plan and CPD objectives;
- Completing and documenting performance and development reviews as part of our six-monthly performance management process;
- Responsible for ensuring all team member sickness and absence is managed and recorded on HRIS;

- Recruitment of new talent, working with Cyber Claims Director, Claims Director and HR to attract new hires;
- Coaching and support for new and existing team members as well as hands-on training (working with L&D and Claims Director) to support the team fulfil their potential within their roles.

Skills & Ability

- Skilled at managing teams delivering cyber incident response, in particular those of vendors. Experienced with reviewing and challenging scopes of work;
- Able to deal with external customers and brokers in high stress situations;
- Capable of managing both the technical and non-technical aspects of dealing with cyber incidents and/or forensic investigations;
- Excellent communication skills and capable of credibly speaking to clients and partners regarding cyber incidents and the value CFC's products and services provide in responding to them;
- Personable, willing to learn and challenge the status quo;
- Excellent attention to detail with a high standard of written and verbal English;
- Willingness to learn and understand cyber policy wordings.

Knowledge & Experience

- A minimum of five years of cyber security related experience, preferably in a client facing role;
- Previous experience of working in a cyber incident response team, with substantive experience in leading cross border and international cyber incidents or forensic investigations;
- Demonstrable experience of having led a team with excellent people management skills;
- Demonstrable experience of having led and delivered substantial and complex security projects from project inception through to completion;
- Experience developing incident response plans, playbooks, and delivering customer facing presentations and workshops;
- Experienced at working with cyber incident response vendors, in particular legal and forensic providers;
- Knowledge on appropriate remediation and recovery actions, as well as longer term preventative measures, including a good awareness of awareness of cloud and mobile platform security;
- Experienced at utilising and developing intelligence around threats;

- General knowledge of the insurance industry, particularly cyber insurance.

Education & qualifications

- Honours Degree, preferably with a focus on a technical area (computer engineering, computer science, information security, etc.);
- Industry certifications in cyber security and/or incident response (e.g. CISSP, GCIH, CCFP, or CREST incident response qualifications).

Our Core Values



CFC Core Values

- Passion & Perseverance**

We're passionate about what we do and it shows.
- Respect & Humility**

We treat everyone as we would want to be treated.
- Intensity**

We hold ourselves to the highest standards, always.
- One Team**

We show up as one team to achieve outstanding results.

[Apply now](#)

Our mission is to radically simplify the way commercial insurance is bought and sold.

