# Simple cover for complicated problems: Our new tech policy in action

Technology companies have evolved, so we've updated our tech policy to provide relevant and comprehensive cover for the innovative tech risks of today.

Highlights of our policy include products and services liability, breach of contract, subcontractors' vicarious liability, intellectual property, network security and privacy liability, crime, business interruption and reputational harm. To demonstrate how the cover works we've applied the policy to a fictional access control system company.

The access control company entered a large contract with a multinational financial services company to provide access control systems to all their commercial locations. The contract specified that the company provide full system delivery, including software configurations and installations, as well as hardware design, manufacturing, and installation. Their solutions are deployed as a software-as-a-service (SaaS) model.

## Products and services liability

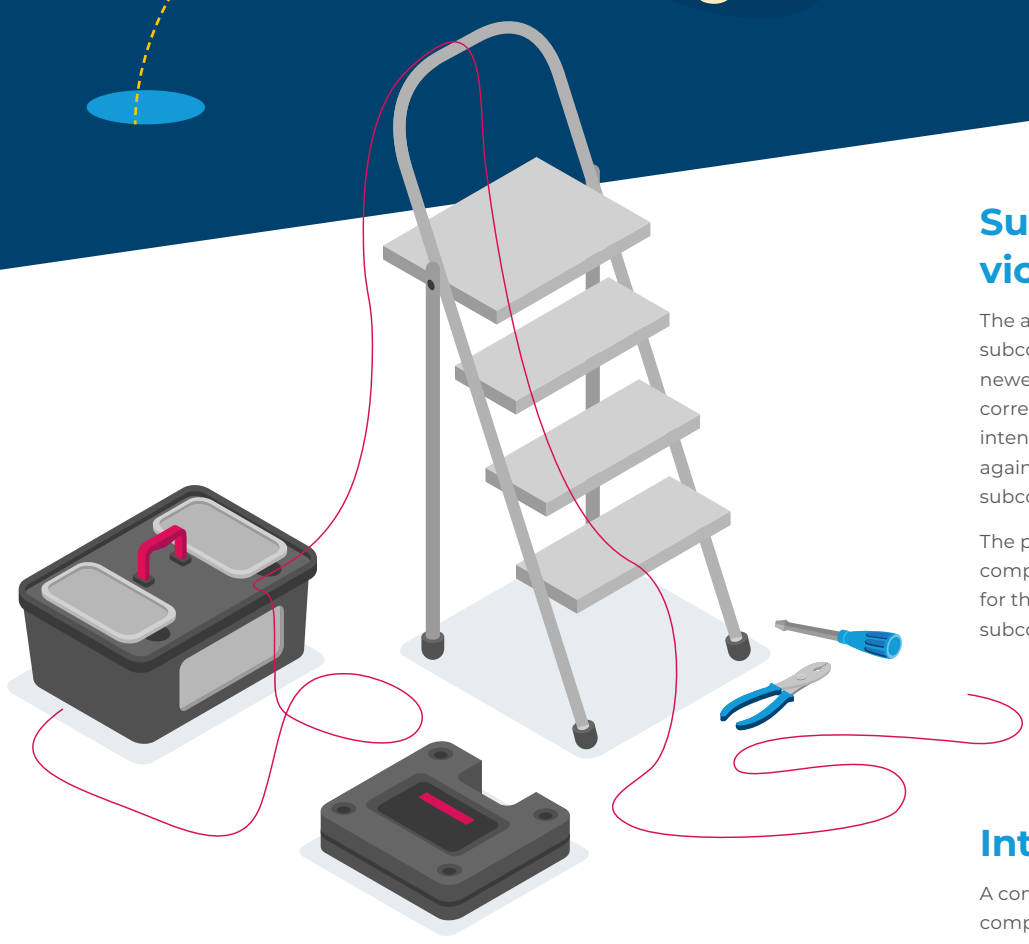
Devices were installed on all access doors as per the scope of works under the contract. The customer noticed that multiple access devices overheated during use and caused damage to the building, and in some cases injury to employees trying to gain access to the building.

The products and services liability section of the policy is unique in that it will respond to claims alleging financial loss, bodily injury and property damage associated with the failure of the access devices.

## Breach of contract

The contract between both parties specified that access should be granted to fob holders only between 6am and 8pm, however the system deployed allowed for 24 hours access meaning additional security staff were required to monitor the building overnight. The customer sued for breach of contract as the access control company did not comply with the full contract specification and was not fit for purpose which was a contractual term.

The policy will cover the costs of damages and defence associated with breach of contract. Importantly the policy covers the alleged breach of a fitness for purpose guarantee the company made, which is a liability assumed under the contract.



## Subcontractors' vicarious liability

The access control company utilised subcontractors to install the devices on the newest buildings, which were not configured correctly, so the devices failed to work as intended. The customer took legal action against the company for the work carried out by subcontractors.

The policy protects the access control company against claims made against them for the alleged defective work carried out by subcontractors working on their behalf.

## Intellectual property

A competitor alleged that the access control company infringed on their design rights and commenced legal proceedings. As part of the defence investigation into design right ownership was undertaken to determine the merits of the action.

The policy covers all defence costs and specialists' costs to investigate the matter.

## Network security & privacy liability

SaaS applications are susceptible to malware propagation. A file containing malware was uploaded to the access control company's SaaS application, which simultaneously synced across all users and devices. This resulted in the distribution of malware seamlessly to the customer's entire network.

The policy covers claims resulting from the transmission of malware to third party computer systems, including a customer.

## Crime

A DDoS attack against the access control company rendered their SaaS unavailable, but the DDoS attack was a distraction from a more complex ransomware attack that completely crippled the systems and encrypted their data.

The policy offers access to CFC's IR team who can appoint a forensic team to investigate and resolve the issue, including negotiating a ransomware payment to obtain a decryption key. The policy also reimburses the payment and provides ongoing IR services.

## System business interruption

The decryption key obtained from the threat actor allowed for partial restoration of data. The access control company used their own employees, outside business hours, to rebuild the remaining data and engaged an external data restoration firm to assist further. It took four weeks to restore the systems.

The cyber section of the policy will cover all the costs associated.

## Consequential reputational harm

As a result of the cyber incident the access control company lost considerable income because 25% of their current customers decided against renewing their contracts following the incident.

The policy covers the loss of income sustained by the access control company as a result of the damage to their reputation due to the cyber event.

**No matter how simple or complicated a technology business is, CFC's comprehensive technology policy offers complete peace of mind to any tech company ensuring there are no gaps in cover.**

Find out more about CFC's updated tech wording, or you can ask us a question tech@cfcunderwriting.com.