Technology Industry Practice Claim Examples

Chubb has handled technology-driven claims and cyber incidents, and underwritten exposures for specialised technology policyholders for more than 20 years. Over this time, the world has become an increasingly interconnected web of technology and data. Today, technology companies face numerous cyber risks, many of which are shared systemic cyber risks that apply across a broad array of sectors.

Widespread risks posed by Managed Service Providers (MSP). An Incident at an MSP impacts a Manufacturing Company.

We insure a global Manufacturing company who were victims of a ransomware incident. The incident occurred at a managed service provider (MSP) for whom the insured relied upon under contract to host data. The threat actor encrypted the systems and data thereon of the MSP which in turn resulted in the Insured's data being inaccessible. The incident at the MSP caused a Widespread incident affecting many clients of the MSP due to their reliance on the services provided by the MSP. In addition to the encryption, sensitive data including data belonging to clients and employees was exfiltrated requiring data subject and regulatory notifications in multiple jurisdictions. The Insured relied upon Chubb's Incident Response Manager to assist with the triage and engagement of vendors to respond to the Incident in a timely manner. The policy provided cover for numerous vendors to investigate, contain and remediate the incident, including Incident Response Managers, IT Forensic investigation, Legal advice and Public Relations specialists to mitigate adverse publicity impact. The Insured's operations were significantly impacted by the incident, causing inefficiencies in process and services with manual workarounds utilised where possible.

The Insured received a number of third party claims seeking damages for non-provision of services and products on the basis the Insured was unable to provide their products in the usual timely manner. The insured incurred significant Business Interruption loss, partially due to the Incident and partially due to wider market conditions. Chubb assisted the insured with the valuation of the Business Interruption Loss caused by the Cyber Incident by engaging a Forensic Accountant. The total cost of the incident, including Business Interruption loss, vendor costs and the exposure under the third party claims totalled well over €50m. Unlike other Ransomware incidents observed, the Insured did not engage with or pay a ransom to the threat actors.

Note - Companies often heavily rely upon MSPs who can cause Systemic events impacting many Insureds simultaneously. These incidents are largely out of the control of the Insureds. The contracts with MSPs are usually unfavourable with liability caps and clauses harming subrogation.

Exploitation of Neglected Software causes an incident at a Marketing Company.

We insure an international marketing company who operate both in the UK and US. They suffered a ransomware incident impacting the availability of systems and data thereon. Access was gained to the systems of the policyholder via an unprotected server connected to the network. The insured failed to patch the neglected software. The threat actors were able to exfiltrate over 200GB of data, including significant amounts of intellectual property and sensitive corporate data. The threat actors demanded a significant ransom in exchange for a promise not to disseminate the data exfiltrated. The insured engaged the Chubb Incident Response Manager and sought advice, engaging vendors to supplement their own retained vendors. The policy provided cover for numerous vendors to investigate, contain and remediate the incident, including incident response expenses, IT forensics, legal costs and specialist extortion and ransom negotiation services, who negotiated down the ransom demand by over 60% in order to prevent the publication of stolen data. The policy did not require the consent of Chubb in order for the insured to pay a ransom, thus expediting the payment and mitigating risk of publication. The IT forensics vendor managed to ensure that the encrypted data was reinstated via available backups. Due to the speed and efficiency of the response, the company managed to avoid significant business interruption loss. The insured incurred losses in excess of £1.5m.

Note - unpatched or unsupported servers and software, often referred to as neglected software, are a major route cause of compromise. It is important to ensure your servers and software are up-to-date on the patches available, and vulnerabilities mitigated. Thankfully the insured had a secure backup enabling the quick reinstatement of data, thus mitigating inability to provide services and avoid both 3rd party claims and BI loss.

Phishing Campaign targets a Media Distribution Company, leading to a Ransomware Incident

We insure a multinational technology company specialising in digital media distribution. The insured suffered a ransomware attack, leaving their systems and servers encrypted. The insured's software as a service product was therefore unavailable to the insured's clients, causing a widespread event. The attack was perpetrated through malicious spam in email communications, duping the employee into clicking malicious links. The policy provided cover for a number of vendors engaged through Chubb's Incident Response Management services to respond to the attack, including Chubb's Incident Response Manager expenses, IT Forensic investigators, information security consultants and legal advisors. Extortion negotiation specialists were engaged to negotiate with the threat actor, and to facilitate the ransom payment in order to obtain a decryption key and to prevent dissemination of exfiltrated data. The insured's systems were restored to a working condition within 7 days. The combined total of the vendor expenses, ransom paid to the threat actors and BI loss was in excess of £1m.

Note - We often see attacks targeting the employees of the policyholders in order to gain access. Staff should be trained to spot phishing emails. Multi-Factor Authentication (MFA) should also be implemented across networks to best protect against credential theft and limit access if access is gained to systems. The inability to provide software services to clients could cause a widespread event amongst clients, and result in significant BI Loss or 3rd party liability claims for non-provision of services.

Logistics industry disrupted by an attack on a software-as-a-service Technology provider.

We insure a technology company servicing the logistics industry. The insured discovered their servers across multiple locations had been encrypted. Access was gained through a Common Vulnerability and Exposure (CVE) exploit. The threat actors demanded an extortion payment in exchange for the decryption key. The attack prevented the entirety of the company's customers from accessing their stock management software and systems for several days, causing a widespread event which disrupted clients and cause inability to fulfil orders efficiently. The Police and GCHQ were duly notified with assistance from Chubb's Incident Response Management services and Breach Coach. The policy provided cover for a number of vendors in managing and containing the incident, including IT forensic firms, legal advisors and extortion negotiation specialists who negotiated payment of the ransom and obtained a valid decryption key allowing the insured's systems to be recovered. The insured also had cover for Data and System recovery costs which assisted in the rolling

out of a business continuity plan, mitigating losses as best possible. From a 1st party cover perspective, the total vendor costs, business interruption loss and the ransom payment totalled in excess of £1.1m. The policy also responded to cover settlements resulting from the numerous claims made against the insured with a total value in excess of £630k.

Note - A technology failure or incident at a software as a service supplier, caused by malicious ransomware or other peril, is likely to cause a widespread event for the clients of the insured. Widespread events cause disruption to a number of clients who will likely seek damages for losses or additional expenses incurred as a result. It's important to review contractual liability clauses and caps entered into with clients, seeking to protect against a wide range of liabilities which could arise.

Data aggregation risk to industries like Healthcare/Medicine when an incident occurs.

We insure a Medical software company who were affected by a malware virus. The virus was used to facilitate unauthorised access to unprotected database infrastructure in a number of countries which hosted sensitive data belonging to employees and clients. The breach required regulatory notifications to be made by the company in multiple jurisdictions. The insured utilised Chubb's Incident Response Management service to triage and advise on available vendors to assist with the Incident. The policy provided incident response costs which included cover for legal advice and notification costs to regulators, as well as forensic costs to investigate, contain and remediate the incident. As a result of the forensic investigation, it was concluded that while data had been accessed there was no evidence of any information having been extracted or published. A number of third party claims were presented against the company for breach of contract and warranties, as well as breach of privacy claims by individuals. The total covered costs of the incident, including both first party expenses incurred by the company and third party claims was USD850,000.

Note - Technology providers will sometimes host large quantities of data, acting as a data custodian. This poses a significant data aggregation risk potentially affecting a number of direct clients of the Insured. There will likely be onerous notification obligations to regulators and clients.

The importance of security hygiene for Technology Service companies.

We insure a technology services company who provide end to end services to major global clients, specifically in the communications and networking industries. The insured were the victims of a ransomware attack, encrypting the majority of the servers and data thereon. The insured spoke to an Incident Response Manager albeit ultimately chose to utilise their own vendors, something the Chubb policy enables. During the course of the incident, the insured incurred Incident Response Expenses for IT and legal advisors, costs to recover data and systems, a ransom payment to obtain a decryption key and mitigate the risk of publication of exfiltrated data, and BI Loss. In order to assist the insured with their BI Loss calculation, Chubb engaged a forensic accountant. The policy provided cover for the forementioned costs and expenses incurred, and provides 3rd party liability cover (damages and defence costs) for claims brought by clients against the policyholder for non-provision of services. The incident took place due to negligent set up of systems leaving them open to exploitation and attack. A third party contractor was responsible for the safeguarding of the insured's systems and therefore subrogation was considered. The cost of contractual analysis to determine liability clauses and assess viability of subrogation was covered under the policy. The costs incurred are in excess of $3.2m.

Note - Adversaries will seek to exploit vulnerabilities in software and systems. Whilst some may be zero day exploits, with little or no mitigation techniques available, others will be known common vulnerabilities and exposures (CVEs). Good security hygiene, including patching, help mitigate vulnerability exploitation.

Chubb. Insured.℠

COG8255-MD 02/23