Cyber Claims Examples

An aid to evaluating if you have adequate insurance in place

CHUBB®

CHUBB

Cyber Claims Examples

The following claims examples are based on actual claims. Costs and expenses will differ in every scenario, and your policy wording should be reviewed in detail to see how your insurance will respond.

Scenario 1: Employee Error	Potential Impact	
An HR recruiter for a healthcare organisation accidentally attached the wrong file when sending an email to four job applicants. The file included HR demographic data consisting of 43,000 former employee names, addresses, and national ID numbers. The insured telephoned the Chubb Incident Response Hotline for assistance and an incident response manager was assigned. Legal services were brought in to manage regulatory implications.	**Privacy Liability** - mismanagement of personal and/ or corporate confidential information, violation of company privacy policy. - Defence expenses arising from regulatory investigation. - Defence and settlement costs for claims employees that had identity stolen **Incident Response Expenses** - Incident response manager fees - Notification to affected individuals - Identity theft monitoring services for affected individuals - Legal consultation fees	 £55,000 £100,000 £5,000 £3,000 £13,000 £10,000
Takeaways As innocent as it may seem, human error can be very costly, and it occurs more frequently than expected. It's important to understand that cyber is not only related to technological incidents. Many of the claims we see stem from very simple mistakes.		**Total Cost: £186,000**

Scenario 2: Denial of Service Attack	Potential Impact	
The data centre which hosted an online retail company's website became the target of a distributed denial of service attack. The attack, which utilised hacked internet of things devices, flooded the data centre's network with so much traffic that their network failed. This made the online retail company's website inaccessible for a period of six hours before backup systems were able to restore 100% functionality. The insured in this scenario is the online retailer. After telephoning the Chubb Incident Response Hotline, an incident response manager was assigned.	**Recovery Costs** - Increased cost of working required to get website functioning properly - Costs to subcontract with external service provider **Business Interruption** - Lost sales and revenue from website downtime **Incident Response Expenses** - IT forensics firm - Legal consultation fees - Incident response manager fees	 £9,000 £12,000 £95,000 £12,000 £10,000 £6,000
Takeaways Distributed Denial of Service (DDoS) attacks are becoming more powerful as the use of easily hacked internet of things devices increases. To minimise impact of a scenario like this one, it is important to build a business continuity plan that ensures critical business applications, systems, and activities do not rely on only one critical IT provider. Chubb's incident response managers and vendors are experienced in dealing with DDoS attacks and will assist in getting your business back on track as soon as possible.		**Total Cost: £144,000**

Scenario 3: Ransomware Attack	Potential Impact	
An employee of a car components manufacturing company clicked on a malicious link in an email and malware was downloaded onto the company server, encrypting all information. A message appeared on the employee's computer demanding £10,000 to be paid by Bitcoin in the next 48 hours in exchange for the decryption key. The company telephoned the Chubb Incident Response Hotline for assistance. The assigned incident response manager brought in IT forensic investigators to assess the validity of threat and to determine whether the company could avoid paying the ransom.	**Network Security Liability** - failure of insured's network security in defending against computer malicious acts **Cyber Extortion** - costs associated with addressing extortion threats to release information or malicious code unless extortion monies were paid - Information technology consultant fees to assess backup capabilities **Incident Response Expenses** - Forensic investigation costs to locate malware, analyse impact, ensure containment, and calculate extent of loss - Legal consultation fees - Incident Response Manager fees **Data Asset Loss** - costs associated with replacing lost or corrupted data	See Incident Response (Below) £14,000 £18,000 £7,000 £6,000 £15,000
Takeaways While the Bitcoin demand was less than the costs incurred under the insurance policy, it is encouraged by both Europol and the FBI that cyber ransoms should not be paid. Not only does paying the ransom perpetuate criminal activity, but it also highlights a company's lack of effective and responsible backup procedures. Backups should be stored off-site and off-network. Chubb understands that there are certain scenarios when paying a ransom is the last but best option, which is why Chubb's incident response vendors are equipped with Bitcoin wallet capability if necessary.		**Total Cost: £60,000**

Scenario 4: Media - Disparagement via Email	Potential Impact	
An employee for a consultancy company sent an internal email containing negative comments regarding a service provider. The email was forwarded to others within the organisation and eventually was sent externally. The email was seen by the service provider and a defamation lawsuit was brought against the consultancy company for harming the service provider's reputation.	**Media Liability** - third party claims arising from Insured's Internet media activities. Wrongful Acts include product defamation, disparagement, trade libel, false light, plagiarism, and more - Defence and settlement costs for claims from service provider **Incident Response Expenses** - Crisis communication services - Public relations expert fees to minimise reputational impact - Incident response manager fees	£150,000 £12,000 £16,000 £3,000
Takeaways Due to the sensitivity of such a claim and the potential damage to a client's reputation, it is important for companies to act quickly to mitigate any potential loss or damage. By ringing the Chubb Incident Response Hotline we can ensure the correct specialists are appointed to work with the client and communicate effectively with the service provider to resolve issues and bring the matter to a conclusion.		**Total Cost: £181,000**

Scenario 5: Unauthorised Access	Potential Impact	
Hackers gained unauthorised access to account information located on a school district's network due to an unknown vulnerability. The account information included names, email addresses, national ID numbers, and financial account information of 20,000 past and present faculty and students. After multiple students and teachers reported suspicious activity on their email, IT discovered that an unauthorised user was in the system. The school district telephoned the Chubb Incident Response Hotline and an incident response manager was assigned.	**Privacy Liability** - mismanagement of personal and/or corporate confidential information - Defence expenses arising from regulatory investigation due to irresponsible management of private information - Defence and settlement costs for claims from individual that had identity stolen **Network Security Liability** - failure to effectively protect insured's network from malware, hacking, denial of service attacks or unauthorised use or access **Incident Response Expenses** - Forensic investigation costs to locate vulnerability, analyse impact, ensure containment, and calculate extent of loss - Notification to affected individuals - Identity theft monitoring services to affected individuals - Costs to set up and operate a call centre for enquiries - Public relations expert fees to minimise reputational impact of the incident - Legal consultation fees - Incident response manager fees	 £75,000 £40,000 £80,000 £1,000 £6,000 £9,000 £13,000 £10,000 £9,000
Takeaways This scenario highlights the importance of storing sensitive information under the necessary protections. Up to date firewalls, intrusion detection software, and encryption of databases are just a few ways to responsibly maintain the privacy of employee and customer information. This example also highlights the many ways Chubb's policy may respond to cyber events. The incident response manager provides assistance in organising the nearly ten different services associated with this one event, from defence costs to public relations expenses and more.		**Total Cost: £243,000**

Scenario 6: Crime - Funds Transfer Fraud	Potential Impact	
An employee received a call purporting to be from the company's bank saying there had been a problem with a payment, possibly caused by a virus. The caller told the employee that the payment would have to be made manually and managed to extract some, but not all, of the bank security code. The employee became suspicious and alerted managers who immediately informed the bank. The bank pld a stop on the account but not before eight transactions had been made, totalling more than £430,000.	**Crime Loss** - fraudulent taking, obtaining, or appropriation of money, securities, or property	£430,000
Takeaways Social engineering that results in fraudulent payments is more appropriately addressed in a crime policy as opposed to a cyber policy. In some scenarios, social engineering can result in loss of sensitive or private information, which could impact the cyber policy. Identifying social engineering tactics from the start can help mitigate both of these loss scenarios.		**Total Cost: £430,000**

Scenario 7: Hack - Resulting in Extortion	Potential Impact	
A medium-sized law firm's network was hacked. Sensitive client information was potentially at risk including; a public company's acquisition target, another public company's prospective patent technology, the draft prospectus of a venture capital client, and a number of class-action lists containing plaintiffs' personally identifiable information. The firm then received a call requesting £25,000 to not sell the information on the black market. The law firm initiated contact with Chubb's Incident Response Hotline, an incident response manager was assigned, and IT forensic investigators and legal counsel were brought in to address the incident.	**Privacy Liability** - mismanagement of personal and/ or corporate confidential information **Network Security Liability** - liability arising out of the failure to effectively protect insured's network from malware, hacking, denial of service attacks or unauthorised use or access - Defence and settlement costs for class action lawsuits **Incident Response Expenses** - Forensic investigation costs to locate vulnerability, analyse impact, ensure containment, and calculate extent of loss - Costs to set up and operate a call centre for enquiries - Public relations expert fees to minimise reputational impact of the incident - Legal consultation fees - Incident response manager fees **Cyber Extortion** - costs associated with addressing extortion threats to release information or malicious code unless paid extortion monies - Crisis negotiator fees - Legal consultation fees - Information technology consultant fees - Extortion payment	£100,000 £44,000 £8,000 £12,000 £28,000 £8,000 £4,000 £2,000 £22,000 £25,000
Takeaways Cyber ransoms should not be paid, but many clients may not be aware of this. By telephoning the Chubb Incident Response Hotline, the incident manager can assist the client from the outset on what steps to take. We have seen cases where the ransom has been paid and the information has still been published online. There is a risk that if the ransom is not paid, the information will be released, but the incident response manager will make sure the correct experts are appointed to deal with this situation.		**Total Cost: £243,000**

Contact

Chubb
100 Leadenhall Street
London, EC3A 3BP

chubb.com/uk

Chubb. Insured.℠

UK3642-JD 01/19