Chapter 5: Real Claims. Real Costs. Real Lessons

What cyber claims can cost

This chapter explores how costs can quickly escalate. It's covers different attack types and businesses.

Incident Type	Claim Items	Micro (1-9 staff)*	Small (10-49)*	Medium (50-249)*
Phishing / Credential Theft	Incident Response, Email security reviews and remediation, Business Interruption losses	**£3,000 – £6,000**	**£6,000 – £10,000**	**£12,000 – £25,000**
Business Email Compromise (BEC)	Incident Response, Legal advice, Funds tracing and recovery support	**£5,000 – £8,000**	**£8,000 – £15,000**	**£20,000 – £50,000+**
Ransomware (Contained)	Incident Response, System restoration and data recovery, Legal advice, Ransom demand and negotiation costs, PR	**£6,000 – £10,000**	**£10,000 – 25,000**	**£40,000 – £150,000**
Data Breach (Limited Personal Data)	Incident Response, Legal advice, Notification and credit monitoring, Regulatory support	**£4,000 – £7,000**	**£7,000 – £12,000**	**£20,000 – £60,000**
System Outage (No Data Exfiltration)	Incident Response, Recovery support, Business continuity measures, Business Interruption losses	**£2,000 – £5,000**	**£5,000 – £9,000**	**£15,000 – £40,000**
Total		**£20,000 - £36,000**	**£36,000 - £71,000**	**£107,000 - £325,000**

*Ranges and total amounts on this table reflect Brit experience.

Real claims do not follow neat averages
In 2026, we reserved £350,000 on a cyber claim where the annual premium was less than £3,500.
A reminder that significant cyber losses are not limited to large organisations or high premium policies.

The Backups Worked. The Claim Still Exceeded £500,000



Business: Regional Law Firm
Location: UK
Sector: Legal Services
Incident: Ransomware

The firm suffered a ransomware attack that left staff unable to access most of its data and systems. Email services remained available, but core files and critical business operations were inaccessible. Initial investigations indicated the threat actors had exfiltrated a significant volume of data prior to encrypting systems.

Although backups were available and restoration efforts could begin immediately, the incident quickly became much more than a system recovery exercise. Specialist incident response providers were required to determine the scope of the compromise, assess any data exposure and support the organisation's recovery.

How the Costs Developed

Claim item	Cost drivers	% of Claim	Cost
Incident Response & Digital Forensics	Investigators, cyber response specialists	**22%**	**£120,780**
Breach Response & Legal Expenses	Breach counsel, legal advice, regulatory guidance	**16%**	**£87,840**
System Restoration & Data Recovery	Recovery, restoration, technical remediation	**18%**	**£98,820**
Business Interruption	Lost income, increased operating costs	**24%**	**£131,760**
Privacy & Data Breach Response	Data review, notifications, communications	**10%**	**£54,900**
Privacy Liability & Regulatory Costs	Third-party claims, investigations, fines where insurable	**10%**	**£54,900**
Total			**£549,000**

Broker takeaway: Backups may help recover systems, but they do not prevent the wider costs of a ransomware incident. Incident response, legal advice and business interruption losses can quickly exceed the costs of restoring systems.

A Seven-Figure Cyber Event

Business: National Accountancy & Advisory Firm
Location: UK
Sector: Accountancy and Business Advisory
Incident: Ransomware

A firm suffered a ransomware incident which disrupted access to systems and required the engagement of specialist advisers and response providers from the Brit vendor panel. The scope of the response grew as investigations progressed and the impact on operations became clearer.

Like many ransomware incidents, the costs were not limited to incident response and forensic investigations . Legal support, specialist consultants and forensic accountants were also required to support recovery and assess the resulting business interruption loss

How the Costs Developed

Claim item	Cost drivers	% of Claim	Cost
Incident Response & Digital Forensics	Incident response services, forensic investigations	**18%**	**£243,000**
Breach Response & Legal Expenses	Breach counsel, legal advice, regulatory guidance	**12%**	**£162,000**
System Restoration & Data Recovery	Recovery, restoration, technical remediation	**24%**	**£324,000**
Business Interruption	Lost income, increased operating costs	**30%**	**£405,000**
Privacy & Data Breach Response	Data review, notifications and stakeholder communications (if required)	**8%**	**£108,000**
Privacy Liability & Regulatory Costs	Third-party claims, investigations, fines where insurable	**8%**	**£108,000**
Total			**£1.35m**

Broker takeaway: The cost of a cyber incident often extends beyond incident response costs. Wider recovery efforts, legal fees and business interruption losses can rapidly drive claims into the seven-figure range.

The Business That Had Backups But Still Couldn't Work

Business: Mid-Sized Manufacturing Business
Location: Canada
Sector: Manufacturing
Incident: Ransomware

A manufacturing business experienced a ransomware attack which affected systems supporting day-to-day operations. The company engaged legal advisers and cyber specialists to investigate the incident and coordinate recovery efforts.

Whilst backups were available, extensive forensic investigations were required before systems could be safely restored and normal operations could resume As with many ransomware events, the resulting disruption to operations became a significant driver of the overall loss

A common misconception is that the ransom payment is the largest cost of a ransomware attack. In reality, significant costs can arise even where no ransom is paid, as the business still needs to undertake forensic investigations, restore systems, manage the response and deal with the impact of operational downtime and business interruption losses.

How the Costs Developed

Claim item	Cost drivers	% of Claim	Cost
Incident Response & Digital Forensics	Investigators, cyber response specialists	**17%**	**£135,000**
Breach Response & Legal Expenses	Breach counsel, legal advice, regulatory guidance	**6%**	**£45,000**
System Restoration & Data Recovery	Technical recovery support, system validation and restoration	**23%**	**£180,000**
Business Interruption	Operational downtime and disruption to manufacturing activities	**39%**	**£315,000**
Incident Response Management & Specialist Support	Cyber specialists, coordination and recovery management	**11%**	**£90,000**
Cyber Extortion	Extortion response, ransom demand and negotiation costs (if applicable)	**4%**	**£35,000**
Total			**£800,000**

Broker takeaway: Backups can help restore systems, but they do not eliminate the wider cost of a ransomware incident. Legal support, forensic investigations, recovery efforts and business interruption losses can quickly become the primary drivers of a claim, even where no ransom payment is made.

The Removal Company That Could No Longer Schedule Jobs

Business: Multi-Site Logistics & Removals Company
Location: USA
Sector: Logistics and Removals
Incident: Ransomware

The company discovered that several servers appeared to have been encrypted and they later identified a ransom note from a known threat actor group. Management immediately disconnected systems and shut down affected technology to contain the incident and prevent further damage.

The decision helped contain the incident and limit further impact but it created a new challenge. The business relied heavily on its systems to organise and schedule customer removals. With those systems unavailable, the organisation struggled to plan future work while forensic investigations and recovery activities were ongoing.

How the Costs Developed

Claim item	Cost drivers	% of Claim	Cost
Breach Response & Legal Expenses	Breach response counsel	**8%**	**£15,000**
Incident Response & Digital Forensics	Technical investigations and incident analysis	**21%**	**£40,000**
System Restoration & Recovery Planning	Recovery planning and restoration activities	**18%**	**£35,000**
Specialist Incident Response Services	Specialist advisers and recovery coordination	**11%**	**£20,000**
Business Interruption	Loss of income from disruption to scheduling, inability to organise future jobs and revenue generation	**37%**	**£70,000**
Cyber Extortion	Extortion response, ransom demand and negotiation support (if applicable)	**5%**	**£10,000**
Total			**£190,000**

Broker takeaway: Cyber incidents can have an affect future revenue as well as current day-to-day operations. If key systems become unavailable, businesses may struggle to take bookings, schedule work or service customers which results in significant business interruption losses.

The Customer Who Spotted the Attack

Business: International Food Manufacturer
Location: UK
Sector: Food Manufacturing
Incident: Business email compromise

A finance team employee responded to what appeared to be a legitimate multifactor authentication request. The request was fraudulent and attackers gained access to the employee's account. From there, criminals sent revised banking instructions to customers and reviewed sensitive financial information held within the mailbox.

> 61% said they could be held responsible if a cyberattack on them disrupted a customer's business.

The compromise was not immediately detected. It only came to light after a customer noticed unusual banking details and contacted the business. The organisation subsequently engaged specialist advisers to investigate the incident, assess the extent of any information accessed or compromised, and determine whether any regulatory or customer notification obligations had been triggered.

How the Costs Developed

Claim item	Cost drivers	% of Claim	Cost
Incident Response & Digital Forensics	External cyber security specialists, mailbox investigations	**27%**	**£42,000**
Cybercrime Response	Banking reviews and compromise assessment	**11%**	**£18,000**
Privacy & Data Breach Response	Assessment of information accessed by attackers	**17%**	**26,000**
Breach Response & Legal Expenses	Breach counsel and legal advice	**14%**	**£22,000**
Customer Notification & Communications	Customer communications and stakeholder engagement	**9%**	**£14,000**
Regulatory Investigation Costs	Regulatory assessment and reporting obligations	**11%**	**£18,000**
Privacy Liability	Defence costs and third-party claims (if applicable)	**11%**	**£18,000**
Total			**£158,000**

Broker takeaway: The full impact of an email compromise is not always immediately apparent. Even where the initial incident appears limited, businesses may still need to investigate potential data exposure, engage specialist advisers and manage customer and regulatory obligations.

The £400,000 Payment That Never Arrived



Business: Design & Engineering Business
Location: USA
Sector: Construction Supply Chain
Incident: Invoice fraud and payment diversion

A design and engineering business believed it was paying legitimate invoices to a long-standing supplier using genuine payment instructions. Unknown to either party, a threat actor had inserted themselves into communications and issued fraudulent payment details.

The insured subsequently transferred £400,000 to fraudulent bank accounts. The issue only came to light when the supplier queried why expected payments had not been received. Fortunately, one of the later payments was identified as suspicious and recovery efforts began immediately.

How the Costs Developed

Claim item	Cost drivers	% of Claim	Cost
Cybercrime & Funds Transfer Fraud	Financial loss arising from payment diversion fraud	**69%**	**£135,000**
Fraud Investigation	Fraud investigation and compromise assessment	**9%**	**£18,000**
Incident Response Services	Incident response support and response coordination	**6%**	**£12,000**
Breach Response & Legal Expenses	Legal support and advice	**5%**	**£10,000**
Funds Recovery & Asset Tracing	Funds tracing, banking recovery efforts and recovery support	**11%**	**£20,000**
Total			**£195,000**

Broker takeaway: Invoice fraud often goes undetected until expected funds fails to arrive. By that stage, businesses may need to investigate the compromise, trace and recover funds, and manage the resulting financial impact.

The Fraud That Came From a Trusted Conversation

Business: Independent Media & Marketing Agency
Location: UK
Sector: Media & Publishing
Incident: Business email compromise leading to (Automated Clearing House) ACH fraud

Attackers gained access to business communications and used that access to facilitate ACH fraud. Because the communications appeared authentic and originated from established business interactions, there were few warning signs.

The incident demonstrated how cyber criminals increasingly exploit trust and familiarity rather than relying on malware or sophisticated technical attacks. By the time concerns were raised, funds had already been transferred and financial exposure had arisen.

How the Costs Developed

Claim item	Cost drivers	% of Claim	Cost
Incident Response & Digital Forensics	Forensic investigations	**20%**	**£12,000**
Cybercrime & Funds Transfer Fraud	Financial fraud arising from compromised communications	**47%**	**£28,000**
Fraud Investigation & Analysis	Fraud analysis and compromise assessment	**12%**	**£7,000**
Account Compromise Response	Response services and incident management	**8%**	**£5,000**
Funds Recovery & Recovery Support	Recovery support and remediation activities	**13%**	**£7,000**
Total			**£59,000**

Broker takeaway: Cyber criminals are increasingly exploiting trusted business relationships rather than technical vulnerabilities. By the time the issue is identified, businesses may already be facing financial losses and recovery costs.

The Fake Support Call



Business: Architectural Practice
Location: USA
Sector: Professional Services
Incident: Social engineering attack

An employee received a phone call from an individual claiming to be from the support team at a software firm. The caller appeared credible and persuaded the employee to allow remote access to their computer to resolve what was described as a software issue.

Shortly afterwards, the employee contacted the software firm directly and learned that the original call had not been genuine. The organisation immediately began incident response procedures and launched an investigation into whether systems, credentials or other information had been compromised.

How the Costs Developed

Claim item	Cost drivers	% of Claim	Cost
Incident Response Services	Incident response support and coordination	**17%**	**£12,000**
Digital Forensics & Technical Investigation	Technical investigations and compromise assessment	**36%**	**£25,000**
Threat Containment & Remediation	Threat containment activities and response actions	**21%**	**£15,000**
Security Assessment & Recovery Support	Security assessments and recovery planning	**14%**	**£10,000**
Breach Response & Legal Expenses	Legal support, notifications or regulatory advice (if required)	**12%**	**£8,000**
Total			**£70,000**

Broker takeaway: Even where no compromise is ultimately confirmed, businesses may still incur significant investigation, containment and response costs to understand what happened, assess potential exposure and protect their systems.

The Teams Message That Reached 170 Employees

Business: Financial Services Organisation
Location: UK
Sector: Financial Services
Incident: Teams-based phishing attack

Attackers used Microsoft Teams to distribute a malicious file to approximately 170 employees. While most recipients ignored the file, a small number interacted with it, triggering an alert and response from the organisation's security provider.

One affected device was immediately quarantined and extensive forensic investigations followed. While no evidence of widespread compromise was identified, the business was required to determine the extent of the incident and review the integrity of its systems before normal operations could continue.

How the Costs Developed

Claim item	Cost drivers	% of Claim /	Cost
Incident Response Services	Incident response support and incident management	**17%**	**£18,000**
Digital Forensics & Security Investigation	Security investigations and compromise assessment	**36%**	**38,000**
Threat Containment & Remediation	Device isolation and containment activities	**15%**	**£16,000**
Threat Intelligence & Threat Assessment	Threat intelligence reviews and analysis	**12%**	**£12,000**
System Integrity & Recovery Assessment	Validation of systems and review of environment integrity	**20%**	**£21,000**
Total			**£105,000**

Broker takeaway: Rapid containment does not necessarily mean a low-cost incident. Organisations may still incur significant investigation, remediation and validation costs to determine the extent of the threat and confirm that systems remain secure.

The Business That Wasn't Hacked

Business: Home Care Provider
Location: USA
Sector: Healthcare
Incident: Supplier ransomware outage

The insured relied on a third-party software to access critical operational information. Following a cyberattack against the provider, the insured was suddenly unable to access the data required to support key business functions

While the insured's own systems had not been compromised, the loss of a critical service provider still resulted in business disruption. The organisation was required to assess the impact of the outage, implement alternative operating arrangements and manage the resulting interruption to its operations.

How the Costs Developed

Claim item	Cost drivers	% of Claim	Cost
Dependent Business Interruption / Supplier Outage	Lost income arising from supplier service unavailability	**55%**	**£110,000**
Incident Response Support	Incident response assistance and coordination	**7.5%**	**£15,000**
Business Continuity Assistance	Alternative operating arrangements and continuity planning	**20%**	**£40,000**
Breach Response & Legal Expenses	Legal review and advice	**5%**	**£10,000**
Third-Party Supplier Breach Assessment	Assessment of supplier compromise and impact on operations	**12.5%**	**£25,000**
Total			**£200,000**

Broker takeaway: A business doesn't need to be directly compromised to suffer a cyber loss. When a critical supplier experiences a cyber incident, the resulting disruption, response costs and business interruption losses can still have a significant impact on the customer.

Thousands of Patient Records Impacted by a Supplier Breach

Business: Community Healthcare Network
Location: USA
Sector: Healthcare
Incident: Third-party data breach

The organisation was informed by its service provider that a subcontracted technology platform had suffered unauthorised access. Investigations indicated that sensitive information relating to more than 12,000 patients may have been accessed, including personal data and protected health information.

The breach did not occur within the organisation's own environment. However, the consequences still landed with the healthcare provider, which had to consider, legal and regulatory notification requirements and wider response arising from the incident.

How the Costs Developed

Claim item	Cost drivers	% of Claim	Cost
Privacy & Data Breach Response	Breach response support and incident management	**19%**	**£75,000**
Breach Response & Legal Expenses	Legal advisers and breach counsel	**15%**	**£60,000**
Notification & Communication Costs	Notification planning and communications with affected individuals	**30%**	**£120,000**
Regulatory Investigation & Assessment Costs	Regulatory assessments and compliance advice	**12%**	**£50,000**
Third-Party Supplier Breach Response	Assessment of the supplier breach and impact on patient information	**9%**	**£35,000**
Privacy Liability	Defence costs and third-party claims (if applicable)	**15%**	**£60,000**
Total			**£400,000**

Broker takeaway: Third-party providers may suffer the incident, but the legal, regulatory and notification obligations often remain with the organisation that collected and entrusted the data to them.

The Address That Should Never Have Been Shared



Business: Specialist Law Firm
Location: UK
Sector: Legal Services
Incident: Privacy breach

A fee earner disclosed a bank statement during legal proceedings which contained a protected address relating to a vulnerable individual. The document was subsequently received by a party who should not have had access to the information.

The issue did not involve hackers or malicious software or a system compromise. Nevertheless, the potential consequences were significant. Concerns centred around the individuals personal safety and welfare, as well and legal and regulatory obligations, including notification to the Information Commissioner's Office.

How the Costs Developed

Claim item	Cost drivers	% of Claim	/ Cost
Privacy & Data Breach Response	Incident assessment and breach management	**22%**	**£22,000**
Breach Response & Legal Expenses	Specialist privacy advice	**28%**	**£28,000**
Regulatory Investigation & Response Costs	Regulatory guidance and ICO engagement	**18%**	**£18,000**
Notification & Communication Costs	Communications and notifications (if required)	**7%**	**£7,000**
Privacy Liability	Third-party claims and defence costs (if applicable)	**25%**	**£25,000**
Total			**£100,000**

Broker takeaway:
Not all cyber claims arise from hackers or malware. Human error can still result in significant privacy, regulatory and liability exposures, particularly where sensitive personal information is involved.

The Payroll Mistake

Business: Payroll Services Provider
Location: UK
Sector: Accountancy and Payroll Services
Incident: Payroll data disclosure

A payroll services provider sent payslip information which subsequently reached the wrong individual. Questions were raised regarding data accuracy, responsibilities between data controller and processor, and the controls in place to prevent personal information from being disclosed incorrectly.

The incident demonstrates how privacy incidents often arise from routine business processes rather than sophisticated cyberattacks. A series of ordinary administrative actions can still result in significant regulatory and reputational concerns, requiring specialist advise and a coordinated response.

How the Costs Developed

Claim item	Cost drivers	% of Claim	Cost
Privacy & Data Breach Response	Privacy assessments and breach evaluation	**16%**	**£18,500**
Breach Response & Legal Expenses	Breach counsel, egal costs and specialist advice	**24%**	**£27,000**
Regulatory Investigation & Response Costs	Regulatory considerations and compliance guidance	**15%**	**£16,500**
Incident Management Support	Incident management and response coordination	**8%**	**£9,000**
Notification & Communication Costs	Notifications and stakeholder communications (if required)	**6%**	**£6,500**
Privacy Liability	Third-party claims and defence costs (if applicable)	**31%**	**£36,000**
Total			**£113,500**

Broker takeaway:
The incident arose from a payroll process, not a cyberattack. Administrative errors still created regulatory, legal and reputational consequences that required specialist support and response.

The Stolen Laptop

Business: Accountancy & Business Advisory Firm
Location: UK
Sector: Professional Services
Incident: Lost device

An employee left the office to attend after-work drinks and later discovered that their work laptop had been stolen. Attention immediately turned to the information held on the device and the potential implications if that information was accessed by an unauthorised third party.

Although there was no evidence of a network intrusion, the organisation still needed to consider potential data exposure, regulatory and legal obligations and evaluate the potential impact on clients whose information may have been stored on the device.

How the Costs Developed

Claim item	Cost drivers	% of Claim	Cost
Privacy & Data Breach Response	Privacy assessments and investigation of data exposure	**22%**	**£26,000**
Breach Response & Legal Expenses	Breach counsel, Legal advice and notification obligations	**24%**	**£28,500**
Device & Data Exposure Assessment	Device security reviews and assessment of information held on the laptop	**17%**	**£20,000**
Incident Response Support	Incident response management and coordination	**10%**	**£12,000**
Regulatory Investigation & Response Costs	Regulatory engagement and compliance considerations	**12%**	**£14,500**
Privacy Liability	Third-party claims and defence costs (if applicable)	**15%**	**£18,000**
Total			**£119,000**

Broker takeaway:
Stolen devices can create significant privacy and regulatory exposures, even where there is no evidence that an organisation's systems have been compromised.

Five Lessons From Real Claims



Businesses Do Not Need to Be Hacked to Suffer a Cyber Loss

Several claims arose because a supplier, software provider or third party experienced a cyber incident. The insured's systems remained secure, but the consequences were still very real.



Human Error Remains One of the Most Common Causes of Claims

Phishing emails, social engineering attacks, misdirected information and mistaken disclosures appeared repeatedly across claims. Many incidents began with people making what seemed like perfectly reasonable decisions at the time.



Cyber Claims Are About More Than Stolen Money

Many losses were driven by forensic investigations, legal advice, business interruption, recovery services and notification obligations rather than direct financial theft.



Backups Help, But They Do Not Make Incidents Cost-Free

Several organisations were able to restore systems successfully. However, investigations, legal obligations, specialist support and operational disruption still generated substantial costs.



Early Response Matters

Across multiple claims, rapid engagement with forensic specialists, legal advisers and incident response teams helped organisations understand the scope of an incident and make informed decisions during critical stages of the response.