

BRIT

The Broker's Guide to Cyber Risk and Insurance

A practical guide designed specifically for insurance brokers

Tools, real-world examples and ready-to-use questions to help you have better cyber conversations

In this guide

Broker conversation starters

Ready-to-use questions designed to open more meaningful client conversations.

60 Second Claim Example

Example cyber incidents. No jargon.

Client says / Reality says

Common cyber myths and simple ways to challenge them.

Key takeaways

Summaries you can take straight into client conversations

Claims Case Studies

Real claims showing how the costs quickly add up.

Want to explore this further?

Resources on Brit's Cyber Knowledge Hub.

A one hour read or dip into a chapter at a time

Chapter 1:	Why cyber insurance is no longer optional
Chapter 2:	The incidents your clients are most likely to face
Chapter 3:	Cyber risk looks different for different businesses
Chapter 4:	How AI is changing cyber risk?
Chapter 5:	Real Claims. Real Costs. Real Lessons
Chapter 6:	What cyber insurance actually does?
Chapter 7:	What happens when a client calls for help?
Chapter 8:	Meet the cyber response experts
Chapter 9:	Turning client objections into better cyber conversations
Chapter 10:	Five simple ways clients can reduce cyber risk
Chapter 11:	Five cyber questions every broker should ask
Chapter 12:	Cyber Jargon Buster

New AI section

13 real claim examples

Handling objections

Brit's Brokers Guide to Cyber is backed-up by the results of our 2026 SME research.

Look out for the speech bubbles throughout and read the whitepaper here.

37% of SMEs who don't hold cyber insurance say they are very likely to take out a policy in the next year.

Chapter 1: Why cyber is no longer optional

Let's start with one client

Think about one of your clients.

Not the largest.

Not the most sophisticated.

Just a typical client.

Now imagine they walk into work tomorrow and discover they can't:

- Access email
- Log into their systems
- Process payments
- Raise invoices
- Access customer records
- Contact suppliers

How long could they continue operating normally? An hour? A day? A week?

For many businesses, the honest answer is: **Not very long.**

And that's why cyber insurance matters.

A third of SME decision-makers fear their business might not survive a cyberattack.

Nearly 2 in 5 SMEs say their cyber security is unprepared to keep pace with growth.

The cyber conversation most brokers have heard

"We're too small."

"Our IT company looks after that."

"We don't have anything worth stealing."

"We're not a target."

These common objections are some of the biggest cyber myths.

Modern cybercriminals aren't always looking for the biggest business.

They're looking for the easiest opportunity. Increasingly this involves a smaller business directly, or via a supply chain.

Client says / Reality says

Client says:
"We're too small to be targeted."

Reality says:
Cybercriminals don't need to choose victims one by one anymore. AI has accelerated automated phishing campaigns, credential theft and supply chain attacks allowing them to target thousands of organisations at once.

Here's the uncomfortable truth

Every business is now a technology business.

The retailer, the manufacturer, the accountant.

Different industries. Same dependency

If technology stops, the business feels it.

And that's why cyber risk is no longer an IT issue.

It's a business resilience issue.

55% of SMEs say larger clients now expect them to meet their cyber security standards.

Broker conversation starter

The next time you're talking to a client, don't start with: "Do you buy cyber insurance?"

Start with:

"What happens to your business if your technology stops working tomorrow?"

The answer will usually tell you everything you need to know.

Key takeaway



Cyber risk follows dependency.

If a client relies on technology to communicate, trade, get paid or serve customers, they already have a cyber exposure.

That's why every broker should be having the conversation.

Want to explore this further?

Visit the Cyber Knowledge Hub:

Addressing the Cyber Gap with SMEs
Why many businesses still underestimate their exposure.

Overcoming Barriers to Buying Cyber Insurance for SMEs
Common client objections and how to challenge them.

From Corner Shops to Corporates: Why Every Business Is Now a Tech Company
A deeper look at why cyber risk follows business dependency.

Chapter 2: The incidents your clients are most likely to face

Most cyber incidents start with something simple:

- An email
- A text message
- A phone call
- A payment request
- A trusted supplier

Cybercriminals don't always break in.

Quite often, they're let in.

44% of SMEs fear a cyberattack on a supplier could stop them trading.

The four incidents every broker should understand

1. Payment fraud

- → A member of the finance team receives a request to make an urgent payment
- → Everything looks genuine
- → The email signature is right
- → The timing feels right
- → The payment is made
- → The money is gone

These attacks often rely on impersonation and trust rather than technical hacking.

Broker conversation starter

> **"What controls are in place if somebody asks to transfer £5,000 today?"**

60 Second Claim Example

A professional services firm discovered they had transferred funds to a fraudulent bank account after receiving altered payment instructions from a threat actor. The payment appeared genuine and followed an existing transaction.

The result was a significant financial loss, an urgent investigation and the involvement of legal and cyber specialists to establish what had happened and whether any funds could be recovered.

Broker takeaway: Businesses do not need to suffer a system breach to experience a cyber loss. A convincing email can be enough.

Typical Cover Sections

- ✓ Cybercrime & Funds Transfer Fraud
- ✓ Incident Response Services
- ✓ Potentially Privacy Liability and Regulatory Defence Costs if third-party claims or regulatory investigations emerge.

This demonstrates that cyber policies often respond through several sections at the same time, rather than a single insuring clause.

---

2. Ransomware

- A link is clicked
- A password is compromised
- An attacker gains access
- Systems are encrypted
- Operations grind to a halt
- Headlines focus on the ransom demand

Businesses usually feel the pain from lost trading, downtime and recovery costs.

Ransomware can also create privacy and regulatory exposure where data has been accessed or stolen and the threat actor threatens to publish it. If sensitive information is released, the impact can extend to reputational harm, regulatory scrutiny and potential privacy claims. Cyber insurance can help with the legal costs of defending the insured, as well as settlements arising from privacy actions or class actions.

Broker conversation starter



"How long could your business operate if staff couldn't access systems for a week?"

60 Second Claim Example



A law firm suffered a ransomware attack which left it unable to access most of its data and systems. The attackers claimed to have stolen information and threatened further action.

Recovery required specialist forensic investigation, legal support and system restoration. The cost of the response quickly exceeded the cost of the technology affected.

Broker takeaway: The biggest cost of ransomware is often the disruption to the business, not the ransom itself. Although breach response costs are typically incurred within the first 24-48 hours, business interruption costs and class actions claims take longer to develop. and are often the most expensive cost of a ransomware claim.

Typical Cover Sections

- ✓ Incident Response Services
- ✓ Data Restoration
- ✓ Cyber Extortion
- ✓ Privacy & Liability Covers
- ✓ Business Interruption

---

3. Data breaches

- Not every attacker wants money immediately
- Sometimes they want information
- Customer data
- Employee records
- Commercial information
- Intellectual property

The costs often extend far beyond the breach; including investigations, notifications and reputational damage.

Broker conversation starter



"What information would cause the most damage if it became public tomorrow?"

---

4. Supplier incidents

- This is the one many businesses forget
- Your client may do everything right
- But what happens if a software provider, cloud platform or outsourced service provider suffers a cyber incident?

Broker conversation starter



"Which supplier would cause the biggest disruption if they went offline for a week?"

60 Second Claim Example



A business was unable to access critical data after a third-party software provider suffered a cyberattack. The organisation's own systems had not been compromised.

Despite this, operations were disrupted while the supplier investigated and restored services.

Broker takeaway: Cyber risk does not stop at the edge of a company's network. Suppliers can become a single point of failure. Breaches increasingly stem from vendors or suppliers and not insureds themselves.

Typical Cover Sections

- ✓ Incident Response Services
- ✓ Business Interruption

Client says / Reality says

Client says:
"We've never had a cyber incident."

Reality says:
Most businesses haven't experienced every major risk they insure against. The important question isn't what happened yesterday. It's whether the business could cope tomorrow.

52% of SMEs recognise that attackers could target them to reach a larger client.

Key takeaway

Most cyber incidents start with ordinary business activities:

- Opening emails
- Making payments
- Trusting suppliers
- Responding to requests

A single incident can lead to operational disruption, financial loss, privacy issues and the need for several areas of cyber cover.

For brokers, the important question is not simply how an incident might happen, but how it could affect the client's ability to operate and recover

Want to explore this further?

Visit the Cyber Knowledge Hub:

Common cyberattacks and threat actors
A practical overview of phishing, ransomware, social engineering and common attack techniques.

Why do people fall for phishes?
Explains why phishing works and why intelligent people still get caught out.

The Rise and Rise of Social Engineering
How cybercriminals exploit trust, urgency and human behaviour.

The MOVEit Transfer Event and the Corresponding Impact
A useful example of how supplier and third-party risk can affect organisations of every size.

Dissecting Ransomware
A deeper look at why ransomware is much more than a ransom demand.

Chapter 3: Cyber risk looks different for different businesses

Think about your last three client meetings

Perhaps a solicitor, an accountant and a manufacturer.

At first glance, they may not have much in common.

But ask one question and the connection becomes clearer:

What happens if their technology stops working?

Different businesses. Different impacts. Same underlying dependency.

Organisations now rely on technology to communicate, trade, get paid, serve customers and work with suppliers. Cloud software, online banking, digital suppliers and AI-powered applications may look different from sector to sector, but they create a shared exposure.

That is why cyber risk follows dependency, not sector. Every business may have cyber risk. The difference is how that risk shows up.

---

1. The legal firm

- A solicitor's business runs on trust
- Client confidentiality
- Sensitive information
- Fund transfers
- Regulatory obligations

A cyber incident can quickly become more than an IT problem. It can disrupt client relationships, affect operations and create significant reputational challenges.

Law firms are increasingly attractive targets because of the sensitivity of the information they hold. Where client data has been accessed or stolen, the threat of publication can create intense pressure to resolve the incident quickly, particularly when confidentiality and client relationships may be affected.

Broker conversation starter

> **"What information would cause the biggest issue if it became public?"**

---

2. The accountancy firm

- Accountants sit at the centre of some of the most sensitive financial information a business owns
- Payroll
- Tax records
- Financial statements
- Banking information

Cybercriminals know this. That's why accountancy firms are often attractive targets for phishing, credential theft and payment fraud.

Broker conversation starter

> **"How would your clients be affected if you couldn't access their records for several days? How would this affect key deadlines such as tax or regulatory filings?"**

---

3. The manufacturer

- Manufacturers often think cyber is a data problem
- In reality, it can be an operational problem
- If systems are unavailable, production lines can stop
- Orders may be delayed
- Customers may be impacted

For many manufacturers, the cost of downtime can quickly outweigh the cost of the original attack.

Broker conversation starter

> **"Could you cope with losing data or losing production for a week?"**

---

4. The retailer

- Retailers depend on transactions
- Payment systems
- Inventory platforms
- E-commerce websites
- Customer data
- When those systems fail, revenue can stop almost immediately

Cyber incidents don't need to involve a major data breach to create a major business problem.

Sometimes the disruption alone is enough.

Broker conversation starter

> **"How long could you trade if your payment systems went offline?"**

Client says / Reality says



Client says:
"Cyber isn't really a concern for our industry."

Reality says:
Cyber incidents don't target industries. They target opportunities. The impact might look different in a law firm than it does in a factory, but almost every business now relies on technology to operate.

Key takeaway



Different businesses experience cyber risk differently.

- A solicitor worries about confidentiality.
- A manufacturer worries about production.
- An accountant worries about financial information.
- A retailer worries about transactions.

But they all rely on technology.

Every business is now a technology business.

And that's why cyber risk and insurance is a business resilience conversation for almost everyone.

Want to explore this further?

Visit the Cyber Knowledge Hub:

📖 **Cyber Risk in Legal Firms: Talking Points for Brokers and Businesses**
Practical guidance on the cyber risks facing legal practices.

📖 **Why Cyber Risk Matters for Accountancy Firms**
Explores the unique cyber exposures within accountancy practices.

📖 **Cyber Risk Presents Material Risk for Manufacturing**
A closer look at operational disruption and manufacturing cyber exposures.

📖 **From Corner Shops to Corporates: Why Every Business Is Now a Tech Company**
Why cyber risk is increasingly driven by technology dependency rather than company size or sector.

Chapter 4: How AI is changing cyber risk

The email looked perfect

Imagine a client receives an email from their Managing Director.

- → The tone sounds right
- → The spelling is perfect
- → The request seems reasonable
- → There are no obvious warning signs

The problem?

The Managing Director never sent it.

Welcome to the AI era.

> 68% of SMEs say AI makes them more likely to purchase cyber insurance.

AI isn't creating new cyber threats

It's making existing threats better.

Cybercriminals have always used phishing emails, fake invoices, impersonation and fraud.

AI simply helps them do it faster, at greater scale and with fewer mistakes.

Client says / Reality says

Client says:
"I'd spot a phishing email."

Reality says:
Modern phishing attacks don't always look suspicious. AI can help attackers create highly convincing messages that closely mimic genuine communications.

Seeing is no longer believing

AI isn't limited to emails.

It can generate:

- ✓ Voice messages
- ✓ Phone calls
- ✓ Videos
- ✓ Images

> 79% of SMEs say AI is making cyberattacks more sophisticated and harder to prevent.

In one widely reported example, an employee was allegedly tricked into transferring millions after participating in a video call populated entirely by AI-generated deepfakes.

Broker conversation starter

> "How would your team verify a payment request from a senior executive if the email, voice and video all looked genuine?"

Could AI take over your mailbox?

A growing area of risk involves AI agents that can take actions rather than simply generate content. Businesses are increasingly connecting AI systems to email, knowledge bases, cloud platforms and operational workflows. While this can improve efficiency, it can also create new governance challenges if AI systems are granted excessive permissions or allowed to act without appropriate oversight.

A simple example

An AI-powered mailbox assistant might be asked to:

- Read incoming emails
- Route requests automatically
- Draft responses
- Trigger workflows

If a malicious email contains hidden instructions designed to influence how the AI behaves, known as a prompt injection attack, the AI could potentially be manipulated into taking actions that were never intended.

AI creates opportunity as well as risk

Businesses are increasingly using AI to draft content, analyse information, automate tasks and support decision-making. In many organisations, adoption is happening faster than governance.

Key questions include:

- → **What information is being shared?** Employees may upload customer data, contracts, financial information and other sensitive material into AI tools.
- → **Who can access AI tools?** Many businesses have limited visibility over which platforms are being used and by whom.
- → **What decisions can AI influence?** AI can support recommendations, content creation and operational decisions, but accountability remains with the business.
- → **How is its use monitored?** Governance, oversight and employee guidance often lag behind adoption.

AI and Data Exposure

A weak AI policy is not a claim in itself.

However, the consequences can quickly become significant where AI use contributes to a:

- Data exposure
- Privacy incident
- Regulatory investigation
- Reputational issue

Employees may upload sensitive customer information, contracts or financial data into external AI platforms. Businesses may also face allegations that AI-generated content reproduces or infringes third-party intellectual property.

In some cases, organisations may need to investigate:

- What information was shared
- Whether it was retained by the platform
- Whether any legal or regulatory obligations arise

Insurance relevance

While AI introduces new technology risks, many of the resulting losses fall into familiar cyber insurance categories such as Incident Response Services, Privacy Liability and Business Interruption.

Depending on the circumstances, AI-related issues around copyright infringement may also involve: Multimedia Liability - if arranged as a policy extension or specific cover.

Key takeaway



AI doesn't change the fundamentals of cyber risk. It amplifies them.

Attackers still exploit trust, people still make decisions and sensitive information still needs to be protected.

Businesses should understand:

- What information is being shared with AI tools and whether sensitive data, contracts or customer information could be exposed.
- Who can access AI platforms, what systems they can connect to and how their use is governed.
- How AI-generated content is reviewed before use and whether appropriate controls exist to manage intellectual property, privacy and regulatory risks.

The technology may be evolving, but the need for good governance, oversight and cyber resilience remains the same.

Want to explore this further?

Visit the Cyber Knowledge Hub:

Can a Single Email Take Over Your AI Mailbox?
Explores how AI-powered tools can introduce new risks if malicious instructions are hidden within content.

Dabbling with Deepfakes
A practical look at AI-generated voice and video impersonation and what businesses can do about it.

Risk Versus Reward: Using AI in Business
A broker-friendly introduction to AI, its benefits and the emerging risks organisations should understand.

The Generational Shift in Cyber Extortion
How AI is helping threat actors scale attacks and evolve extortion tactics.

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.

Chapter 6: What cyber insurance actually does

Let's clear something up

Ask 10 people what cyber insurance does and you'll probably get 10 different answers.

So let's start with a better question:

What does a business actually need when a cyber incident happens?

The answer isn't just money.

- ✓ **It's expertise**
- ✓ **It's support**
- ✓ **It's a plan**

Cyber insurance is more than a policy

Modern cyber insurance combines three things:

Prevention: Helping businesses identify and reduce cyber risk before an incident occurs.

Response: Providing access to specialist support when something goes wrong.

Recovery: Helping businesses deal with the financial and operational impact of an incident.

Cyber insurance isn't just for after a breach

A modern cyber policy often includes practical support designed to help businesses strengthen cyber security **before** anything goes wrong. This may include:

- ✓ **Awareness training:** Helping staff recognise common cyber threats.
- ✓ **Risk visibility:** Helping businesses understand where vulnerabilities may exist.
- ✓ **Threat alerts and intelligence:** Providing awareness of emerging risks and vulnerabilities.
- ✓ **Access to cyber expertise:** Specialist guidance on Cyber security, resilience and preparedness.
- ✓ **Incident planning:** Helping businesses understand how they would respond if the worst happened.
- ✓ **Outside-in security scanning:** Monitoring of internet-facing systems to identify emerging threats and exposures.
- ✓ **Discounted cyber security services**: Access to trusted cyber security tools and services at preferential rates.

Think of cyber insurance as a team of first responders

They can include specialists who can help to:

- Investigate what happened
- Contain the incident
- Restore systems
- Manage legal obligations
- Communicate with customers and stakeholders
- Handle claims and recovery

Understanding First-Party and Third-Party Cover

One of the unique features of cyber insurance is that it can respond to both the insured's losses and claims brought by others.

First-party cover



First-party cover focuses on the direct impact a cyber incident has on the insured business itself.

These are often the costs that arise immediately after an incident, such as:

- Investigating what happened
- Containing and managing the incident
- Restoring systems and data
- Recovering from business interruption
- Managing extortion demands
- Recovering from cybercrime and fraud losses

In simple terms:

First-party cover helps your client recover from the incident itself.

Third-party cover



Third-party cover focuses on the business's legal liability to others.

This may arise where customers, employees, suppliers, regulators or other third parties suffer loss following a cyber event. Examples can include:

- Privacy claims following a data breach
- Regulatory investigations
- Defence costs
- Settlements and damages
- Claims arising from network security failures

In simple terms:

Third-party cover helps protect the business when others allege they have suffered loss because of the incident.

How the cover applies in practice

All of the examples below could occur following just one incident and yet trigger multiple sections of the policy.

If this happens...	Businesses may need help with...	Typical cover section*	First Party / Third Party
Systems become unavailable	Downtime, extra costs and operational disruption	**Business Interruption**	First Party
Data is lost (exposed), damaged or encrypted	Recovery of systems and information	**System Restoration & Data Recovery and Privacy Liability**	First Party
A cyberattack occurs	Understanding what happened and containing the incident	**Incident Response Services**	First Party
Sensitive information is exposed	Investigation, notifications and specialist advice	**Incident Response Services, Notification Services, Privacy Liability**	First & Third Party
Customers or employees bring claims after a breach	Defence costs, settlements and legal support	**Privacy Liability**	Third Party
A regulator investigates following a breach	Regulatory enquiries and legal representation	**Regulatory Investigation & Fines**	First Party
Money is transferred to criminals	Recovery efforts and financial loss	**Cybercrime & Funds Transfer Fraud**	First Party
Criminals demand payment or threaten to release data	Negotiation support and specialist advice	**Cyber Extortion**	First Party
Malware from the insured's systems affects others	Third-party claims and defence costs	**Privacy Liability**	Third Party
A critical supplier suffers a cyber incident	Loss of service and operational disruption	**Dependent Business Interruption / Supplier Outage**	First Party
Website or systems are used to attack others	Defence costs and damages	**Privacy Liability**	Third Party
The business doesn't know what to do next	Coordination and specialist support	**Incident Response Services**	First Party

*The exact title of each coverage section will vary by insurer and wording. The examples above are intended as generic illustrations of how cyber policies are commonly structured.

Support before, during and after the conversation

You may need support when a client asks about underwriting requirements, existing controls, incident response, supplier risk or how a policy would respond in practice. Those conversations can be complex, and they do not need to happen in isolation.

Brit's cyber proposition is built around access to people with specialist experience across underwriting, claims, breach response and risk management. That means you can start cyber conversations with more confidence, knowing there is practical support behind you when a client question needs a more detailed response.

Key takeaway



Cyber insurance combines prevention, response and recovery.

It can help clients strengthen their resilience before an incident, provide access to specialist expertise when something goes wrong and support their financial and operational recovery afterwards.

First-party cover helps the client recover from its own losses. Third-party cover helps protect the business when customers, employees, regulators or others allege they have suffered loss.

Cyber insurance is therefore more than financial reimbursement. It gives clients access to the people, services and support they may need before, during and after an incident.

Want to explore this further?

Visit the Cyber Knowledge Hub:

Overcoming Barriers to Buying Cyber Insurance for SMEs
Explains why cyber insurance is about far more than recovering from a breach.

Breach Response: Leave It to the Experts
Introduces the specialist support available during a cyber incident.

Digital Forensics: Managing an Online Crime Scene
Explains how forensic experts investigate incidents and help organisations understand what happened.

Ransomware Negotiation: Don't Try This at Home
Shows why specialist expertise is often needed during complex cyber incidents.

Chapter 7: What happens when a client calls for help?

The call nobody wants to make

- It's 8:17am on a Tuesday
- A client phones
- Staff can't access systems
- Emails have stopped working
- A ransom demand has appeared on screen
- Nobody knows what to do next

Who takes control?

For most businesses, this is the moment panic starts to set in. But for a well-managed cyber response, it's the moment specialists step in.

The first few hours matter most

One of the biggest misconceptions about cyber incidents is that they're purely technology problems.

They're not.

Within hours of an incident, a business may need to make decisions about:

- Containing the attack
- Preserving evidence
- Legal obligations
- Customer communications
- Regulatory reporting
- Business continuity

The insured should contact the 24-Hour Breach Response Hotline as soon as possible and refer to their policy for how to notify insurers - this is usually by email to a specific address. Early engagement helps bring in the right specialists, preserve evidence and avoid decisions in the first few hours that could increase downtime or complicate the forensic investigation. Claims can become harder to manage where businesses try to fix matters internally before insurers are involved.

What happens next?

While every incident is different, a typical response often looks something like this:

Step 1: Assess the situation

The immediate priority is understanding what has happened and what might still be happening.

Questions include:

- How did the incident occur?
- What systems are affected?
- Is the threat still active?
- Is sensitive information involved?

Step 2: Contain the problem

The next goal is limiting further damage.

That might involve:

- Isolating systems
- Restricting access
- Investigating compromised accounts
- Stopping the incident from spreading

Step 3: Coordinate the response

Once the immediate threat is understood and contained, the focus turns to managing the wider incident.

This may involve:

- Legal and regulatory advice
- Understanding notification obligations
- Coordinating forensic investigations
- Managing communications with customers and stakeholders
- Supporting decision-making during the incident

Step 4: Recover and restore

The focus shifts from managing the incident to getting the business back up and running.

Support may include restoring systems, managing disruption and coordinating ongoing recovery.

The question changes from: "What happened?" to: "How do we get back to business?"

Client says / Reality says

Client says:
"Our IT provider would sort that out."

Reality says:
A cyber incident can quickly become a technical, legal, regulatory, financial and reputational issue. Businesses often need several specialists working together simultaneously.

You won't be dealing with just one expert

Think of a cyber incident like a major emergency.

You wouldn't expect one person to do everything.

Depending on the incident, support may include:

- **Breach counsel**
- **Digital forensics experts**
- **Negotiation specialists**
- **Communications specialists**
- **Claims professionals**

We'll look at these specialists in more detail in the next chapter.

Broker conversation starter

Ask your client:

"If your business suffered a serious cyberattack tomorrow, who would coordinate the response?"

Many organisations have never considered the answer.

Key takeaway

The first few hours of a cyber incident can shape the cost, disruption and outcome.

Early notification allows the response services to assess what has happened, contain the threat, preserve evidence and coordinate the technical, legal, regulatory and communications response. Once the immediate threat is controlled, attention turns to restoring systems and getting the business operating again.

Cyber insurance helps clients answer three urgent questions:

- How do we stop this getting worse?
- How do we get back up and running?
- How do we manage the wider financial, legal and operational impact?

Want to explore this further?

Visit the Cyber Knowledge Hub:

📖 **Breach Response: Leave It to the Experts**
Explains the critical role of breach counsel during an incident.

📖 **Digital Forensics: Managing an Online Crime Scene**
Shows how investigators uncover what happened and help contain incidents.

📖 **Ransomware Negotiation: Don't Try This at Home**
Demonstrates why specialist expertise matters when dealing with threat actors.

Chapter 8: Meet the cyber breach response experts

Ever watched a crime drama?

- The detective arrives
- The forensic team investigates the scene
- Lawyers get involved
- Experts analyse the evidence
- Everyone has a job to do

The difference with a cyber incident is that the crime scene might be a laptop, an email account or an entire business network.

When clients buy cyber insurance, they're gaining access to specialists who deal with cyber incidents every day.

Brit maintains a global panel of pre-approved cyber specialist firms that are regularly reviewed, giving insureds rapid access to trusted experts who can help investigate, contain and recover from cyber incidents.

Meet the team

Breach counsel

Think of breach counsel as the conductor of the orchestra. They are often appointed first and help to decide which other specialists are needed.

They help coordinate the entire response, advise on legal and regulatory obligations, and make sure the right specialists are involved at the right time. They also help manage communications with regulators, customers, employees and other stakeholders, providing guidance and draft messaging where needed.

When sensitive information may have been compromised, breach counsel helps businesses understand what they need to do next, what needs to be reported and how to communicate effectively throughout the incident.

Digital forensics

Think of digital forensic investigators as cyber detectives. They help turn confusion into facts and plans into action.

Their role is to understand:

- What happened
- How it happened
- What systems were affected
- Whether the threat is still present (and potentially stop or block the attacker)

Ransomware negotiators

Most business leaders never expect to negotiate with criminals.

Negotiation specialists bring experience, threat intelligence and specialist knowledge to help businesses navigate extortion events, assess their options and avoid negotiating with criminals alone.

Data Mining Specialists

Where data has been accessed, data mining specialists review exposed data, identify personal or sensitive information and help determine who is affected. This is helpful from a claims perspective because it can materially affect the scope and cost of notifications.

The services expand as needed

The specialists above are often at the centre of the response, but they aren't the whole team. Depending on the incident, businesses may also need support from crisis communications specialists, public relations advisers, credit monitoring providers, crisis response consultants and other technical experts. Cyber insurance helps bring together the right people for the challenge at hand.

Claims professionals

While the other specialists focus on managing the incident itself, claims professionals help ensure the right support remains in place throughout the response. They work alongside the wider team, monitor progress and help businesses access the cover and services available under the policy.

Why independence matters

Independent specialists provide an objective view during a cyber incident, helping establish the facts and provide an impartial assessment of what has happened.

Where Breach Counsel is involved, communications and investigations may also benefit from legal privilege. Independent investigations can be particularly important if regulatory scrutiny, litigation or claims arise later.

Broker conversation starter

Ask your client:

"If a serious cyber incident happened tomorrow, which of these specialists would you have immediate access to?""

Key takeaway

A serious cyber incident cannot usually be managed by one person or one provider.

Breach counsel may coordinate the response, digital forensics specialists establish what happened, data mining experts assess affected information, negotiators support extortion decisions and claims professionals help the client access the relevant cover and services.

Together, these independent specialists help investigate, contain, manage and communicate the incident, while supporting the client's recovery.

Cyber insurance gives clients rapid access to the right expertise, with each specialist performing a distinct but coordinated role.

Want to explore this further?

Visit the Cyber Knowledge Hub:

📖 **Breach Response: Leave It to the Experts**
Why legal and regulatory expertise matters during a cyber incident.

📖 **Digital Forensics: Managing an Online Crime Scene**
How investigators establish what happened and support recovery.

📖 **Ransomware Negotiation: Don't Try This at Home**
An introduction to one of the most misunderstood roles in cyber response.

Chapter 9: Turning client objections into better cyber conversations

Let's be honest

Cyber Insurance can feel complicated, technical and expensive.

But most objections are not final decisions. They are signs that the client has not yet connected cyber risk to their own business.

A good objection response does three things:

- ✓ It listens to the concern
- ✓ It reframes the issue in business terms
- ✓ It opens the next conversation

The best cyber conversations start with a better question.

"We're too small."

What they are really saying

"I do not think this applies to us."

This is probably the most common objection. It is also one of the most important to challenge carefully.

Many smaller businesses do not see themselves as attractive targets. They may assume cybercriminals are only interested in large companies, household names or businesses holding huge volumes of sensitive data.

But cybercriminals do not always look for the biggest business. Often, they look for the easiest opportunity.

A small business may still rely on email, online banking, cloud software, payment systems, supplier relationships and customer information. If any of those stop working, the business can feel the impact quickly.

Broker conversation starter

Do not start by debating whether the client is a target. Start with dependency. Ask:

"If your systems stopped working tomorrow, what would be affected first?"

This moves the conversation away from company size and towards business impact.

The client may talk about:

- Not being able to invoice
- Not being able to take payments
- Staff being unable to work
- Customers not being served
- Delays to orders or projects
- Lost income

Once the client can see the dependency, cyber risk becomes much more relevant.

"The size of the business is not the only issue. The better question is how much disruption a cyber incident could cause."

"Our IT company handles that."

What they are really saying

"I think cyber risk is a technology problem for our IT provider to solve"

IT providers are an important part of cyber resilience. But a serious cyber incident can quickly become more than a technology problem.

A business may need to think about:

- Legal obligations
- Preserving evidence
- Regulatory reporting
- Customer communications
- Lost income
- Recovery costs
- Supplier disruption
- Claims support

26% of businesses believe cyber may already be covered elsewhere or that their IT provider protects them.

An IT provider may not be responsible for legal advice, regulatory notifications, customer communications, cybercrime losses or business interruption.

Broker conversation starter

Do not dismiss the IT provider. Ask:

"Who helps if the incident becomes more than a technology problem?"

This helps the client understand that cyber insurance is not trying to replace IT support. It is designed to sit alongside it.

"A good IT provider is important, but cyber incidents often create legal, financial, regulatory and communications challenges too. Cyber insurance helps bring the wider support together."

Do not make this an IT versus insurance conversation. Make it about the wider response the business may need.

"We don't have anything worth stealing."

What they are really saying

"I think cyber risk is only about data."

Many clients hear "cyber" and immediately think about stolen customer data. But cyber risk is broader than data theft.

26% of SMEs say holding little sensitive is a main reason not to buy cyber insurance.

Cybercriminals may target:

- Payment processes
- Email accounts
- Login details
- Supplier relationships
- Business operations
- Employee information
- Client communications

And sometimes attackers do not need to steal anything to cause serious disruption. If a business cannot access systems, communicate with customers or continue trading, the impact can be immediate.

Broker conversation starter

Move the discussion from data to disruption. Ask:

"What would be more painful: losing your data or losing access to your business for a week?"

This helps the client think about cyber as an operational risk, not just an information risk.

"Cyber risk is not only about what criminals might steal. It is also about what the business could lose access to."

If the client says they do not hold valuable data, talk about access, operations and income.

"We've never had a cyber incident."

What they are really saying

“I do not see this as likely enough to worry about.”

Many businesses have never had a major cyber incident. But that does not mean the exposure is not there.

Many businesses have also never had a serious fire, flood or liability claim. They still insure against those risks because the impact could be significant if they happened.

Cyber insurance works in the same way. The question is not whether something has happened before.

The question is whether the business could respond and recover if something happened tomorrow.

Broker conversation starter

Do not focus on fear. Focus on preparedness. Ask:

”If something happened tomorrow, how quickly could the business recover?”

This moves the conversation away from probability and towards resilience.

The client may start thinking about:

- Who would make decisions ?
- Who would contact customers ?
- Whether backups work
- Whether suppliers could help
- How long the business could trade without systems
- What cashflow impact downtime could create

”Past experience does not remove future risk. The real question is whether the business could recover if something happened tomorrow.”

Do not argue about whether the client will suffer an incident. Help them think through what recovery would look like.

"Cyber insurance is too expensive."

What they are really saying

"I don't see the value."

Cost always matters. But if the conversation starts and ends with premium, the client may never understand what they are actually buying.

Cyber insurance is not just a payment after a loss. It can provide access to expertise, support and a plan when a business is under pressure.

A cyber incident can create costs linked to:

- Business interruption
- System recovery
- Forensic investigation
- Legal advice
- Customer notification
- Regulatory response
- Specialist support
- Fraud recovery
- Reputation management

Price is the single most influential provider-selection factor for 55% of SMEs.

The value of cyber insurance is often easier to explain when the client understands what help they would need.

Broker conversation starter

Do not simply compare premium to a worst-case loss. Ask what the client would be most worried about.

"What would concern you most after a cyber incident?"

The answer helps tailor the conversation.

- If they say lost income, talk about business interruption
- If they say customers, talk about communications and response support
- If they say regulators, talk about legal and regulatory support
- If they say systems, talk about recovery and restoration

"It is worth thinking about cyber insurance not only as a cost, but as access to specialist help including legal, digital, ransom negotiation and communications services when the business needs it most. Policies also include tailored pre-breach advice and training to best mitigate the risk of an incident."

Do not sell the cheapest answer. Help the client understand what problem they are trying to solve.

"Cyber insurance requirements are too complicated."

What they are really saying

"I am worried we will not qualify, or that this will be too difficult."

Some clients assume cyber insurance comes with unrealistic security expectations.

They may worry they need a large IT team, expensive tools or perfect cyber security before they can even have a conversation.

The goal is not perfection. The goal is understanding risk.

Insurers generally want to see reasonable cyber hygiene that matches the size, complexity and exposure of the business.

Broker conversation starter

Reassure the client that improvement can be gradual. Ask:

"Which cyber controls do you already have in place?"

Then explore the basics:

- Multi-factor authentication
- Backups
- Staff awareness
- Supplier dependency
- Incident response planning

Many clients may already have more in place than they realise.

"Cyber insurance does not require every business to look the same. The aim is to understand the risk and identify sensible, proportionate controls."

Do not let the client assume cyber security has to be perfect. Help them see what they already have and what they could improve.

"Just send me some information."

What they are really saying

"I am not convinced enough to have the conversation yet."

This is one of the most typical ways for a cyber conversation to stall.

The client may genuinely want more information. But sometimes this is a polite way of ending the discussion.

If you send a generic policy summary, the client may not read it or may not see why it applies to them.

A better approach is to send something specific to the concern they have raised.

Broker response

Before sending anything, ask one more question.

"Of course. What would be most useful: something on claims examples, common cyber incidents, or what cyber insurance actually helps with?"

You could follow up with:

- A short claims example
- A sector-specific risk example
- A simple explanation of what happens during an incident
- A myth-busting piece on one of their objections
- A link to a relevant Cyber Knowledge Hub article

"I'll send something practical rather than a long policy summary. It may help to look at how this type of incident affects businesses like yours, then we can pick the conversation back up."

Do not let "send me some information" become the end of the discussion. Use it as a bridge to a better follow-up.

A simple objection-handling framework

1. Acknowledge

Show that you have heard the concern.

"That is a fair point."

"A lot of businesses say the same thing."

2. Reframe

Move the conversation from cyber jargon to business impact.

"The question is not just whether you are a target. It is what would happen if your business was disrupted."

"This is not only an IT issue. It can become a legal, financial and operational issue too."

"The value is not just in the policy. It is in the support available when something goes wrong."

3. Ask the next question

Use a question that helps the client apply the risk to their own business.

"What would stop first if your systems went down?"

"Who would coordinate the response?"

"What would concern you most after an incident?"

The aim is to help the client see the relevance.

Key takeaway



Most objections are not really objections. They are signals.

They show where the client needs more clarity, more context or a more relevant example.

The best cyber conversations are not about having the perfect rebuttal. They are about asking the next useful question.

Want to explore this further?

Visit the Cyber Knowledge Hub:

Overcoming Barriers to Buying Cyber Insurance for SMEs
A detailed look at the misconceptions that commonly prevent businesses from buying cyber insurance.

Addressing the Cyber Gap with SMEs
Why so many businesses remain exposed despite increasing reliance on technology.

From Corner Shops to Corporates: Why Every Business Is Now a Tech Company
Practical examples of why cyber risk affects organisations regardless of size or sector.

Why Do Cyber Insurers Insist on IT Security?
A practical explanation of why insurers ask about reasonable cyber controls.

Chapter 10: Five simple ways clients can reduce cyber risk

Cyber resilience isn't about eliminating every risk

It's about making life harder for cybercriminals and making recovery easier if something goes wrong.

74% of SMEs plan to take some form of cyber action in the next year.

1. Turn on multi-factor authentication (MFA)

Think of MFA as an extra lock on the front door.

Even if a criminal steals a password, MFA can make it much harder for them to gain access.

Many cyber incidents begin with compromised credentials, making MFA one of the simplest and most effective controls available.

Broker conversation starter

"Where is MFA currently switched on within your business and crucially, where isn't it?"

60 Second Claim Example

An employee clicked a phishing link and entered their credentials, including their multi-factor authentication code. This resulted in a compromised account and follow-on phishing activity.

While the incident was contained quickly, the organisation still needed specialist support and investigation.

Broker takeaway: Security controls significantly reduce risk, but they do not eliminate it. Preparation and response remain important.

Typical Cover Sections

- ✓ Incident Response Services
- ✓ Privacy & Security Liability involving regulatory investigations if the impact extends beyond the initial compromise.

---

2. Back up critical data

If a business loses access to systems, backups can make the difference between inconvenience and catastrophe.

But here's the important bit: Backups need to be tested.

There's little comfort in having a backup strategy if nobody knows whether it works.

Broker conversation starter

"When was the last time you tested the restoration of your backups?"

---

3. Train people, not just systems

Most attacks still involve human interaction:

- A clicked link
- A trusted email
- A fraudulent payment request

People are often the first and last line of defence and one of the most important.

Cyber awareness doesn't need to be complicated. It needs to be regular.

Employee error ranks among SMEs' top three cyber risks, yet a third provide no cyber-security training.

Broker conversation starter

"How confident are staff in identifying a suspicious email?"

60 Second Claim Example

A finance employee received what appeared to be a legitimate security request and entered their credentials. The account was compromised and used to send convincing messages to customers and other contacts.

The incident required investigation, customer communications and a review of what information may have been accessed.

Broker takeaway: Good businesses with security controls and experienced staff can still be caught out by sophisticated phishing attacks.

Typical Cover Sections

- ✓ Incident Response Services
- ✓ Notification Services
- ✓ Privacy & Security Liability
- ✓ Regulatory Investigations & Fines

---

4. Know your critical suppliers

Think about:

- Cloud providers
- Software vendors
- Payroll systems
- Managed service providers
- Accounting platforms
- Payment providers

If one of those suppliers experiences a cyber incident, the impact can quickly spread.

Understanding these dependencies is an important part of cyber resilience.

Broker conversation starter

> **"How would you continue operating if a key supplier became unavailable tomorrow?"**

---

5. Have an incident response plan

The best plans aren't necessarily complicated.

They're clear.

- Who makes decisions?
- Who gets called?
- Who communicates with customers?
- Who manages recovery?

Answering those questions before an incident can significantly improve the response.

Many cyber policies provide access to pre-breach support such as virtual CISO services, awareness training, exposure assessments and incident response planning tools. These services help businesses understand their cyber risk and build a practical response plan before they are under pressure.

Why cyber insurers ask about security

The goal is not perfection. It's understanding risk.

For example:

- Evidence of reasonable cyber hygiene
- Controls that match the size of the organisation
- Controls that match the exposure
- Willingness to improve
- Awareness of critical risks

Client says / Reality says

Client says:
"We're not technical enough to improve our cyber security."

Reality says:
You don't need an enterprise-sized IT budget to improve cyber security. Many businesses already have access to core security features through platforms such as Microsoft 365 and Google Workspace. Combined with good processes, planning and staff awareness, these can provide a strong foundation for reducing cyber risk. Small improvements can make a significant difference.

Key takeaway

Cyber resilience doesn't start with buying technology.

It starts with asking better questions about:

- Strong passwords
- MFA
- Backups
- Awareness
- Planning

Together they can make a business significantly harder to attack and much easier to recover.

Want to explore this further?

Visit the Cyber Knowledge Hub:

Why Do Cyber Insurers Insist on IT Security?
A practical explanation of why insurers ask about controls such as MFA, backups and access management.

Why Multi-Factor Authentication (MFA) Matters
One of the simplest and most effective cyber protections available.

How Cybercriminals Exploit MFA Reset Prompts
Demonstrates how criminals often target processes around security controls rather than the controls themselves.

How Cybercriminals Exploit MFA Reset Prompts
Learn why good controls still need good processes.

Why Do People Fall for Phishes?
A useful resource for understanding the human side of cyber risk.

Privileged Access Management Is a Critical Element of Internal Cyber Security
An introduction to managing access to critical systems and information.

Chapter 11: Five cyber questions every broker should ask

You don't need to be a cyber expert to ask these questions.

And you definitely don't need to become your client's IT consultant

You do need to:

- ✓ **Help clients understand risk**
- ✓ **Help them understand impact**
- ✓ **Help them make informed decisions**

Often that starts by asking better questions.

Question 1

"What happens if your systems stop working tomorrow?"

This is usually the best place to start.

It moves the conversation away from technology and towards business impact.

Clients rarely know what ransomware is.

They absolutely know what happens when they can't trade.

Question 2

"Which technology could your business least afford to lose?"

- Email?
- Payments?
- Customer records?
- Production systems?
- Cloud software?

Every answer reveals something about cyber exposure.

And every answer creates a useful conversation.

Question 3

"Who would you call first after a cyber incident?"

Many businesses assume the answer is IT. But serious cyber incidents often involve:

- Legal advice
- Forensic investigations
- Customer communications
- Regulatory issues
- Business interruption

The answer can tell you a lot about how prepared a client really is.

Question 4

"Which supplier would cause your business the biggest disruption if they couldn't operate?"

Cyber risk isn't limited to the business itself.

Many organisations depend heavily on technology providers, cloud platforms and third-party suppliers.

Sometimes the biggest cyber risk sits outside the organisation entirely.

Question 5

"What would concern you most after a cyber incident?"

Some clients worry about:

- Lost income
- Lost customers
- Regulatory issues
- Damaged reputation
- Operational disruption

Understanding what matters most to the client often makes the cyber conversation more productive.

Client says / Reality says



Client says:
"I don't really understand cyber risk"

Reality says:
They don't need to. Most cyber risk conversations are really business conversations about dependency, disruption and resilience.

Key takeaway



Brokers do not need to be cyber experts to start a valuable cyber conversation.

Five simple questions can help identify the client's reliance on technology, the systems and suppliers it cannot operate without, its preparedness for an incident and the consequences it is most concerned about.

The broker's role is to help the client connect cyber risk to business impact and make an informed decision. When the conversation becomes more technical, Brit's cyber team can provide the specialist support needed to take it further.

Want to explore this further?

Visit the Cyber Knowledge Hub:

📖 **Addressing the Cyber Gap with SMEs**
Practical insights into why brokers play such an important role in cyber education.

📖 **Overcoming Barriers to Buying Cyber Insurance for SMEs**
Useful guidance for handling common client objections.

📖 **From Corner Shops to Corporates: Why Every Business Is Now a Tech Company**
A useful resource for helping clients understand why cyber risk exists regardless of size.

Cyber Jargon Buster

AI (Artificial Intelligence)

A broad term for technologies that allow computers to analyse information, learn or identify patterns, and generate responses, recommendations or content. This includes systems that can work with language, images, audio and large amounts of data.

What brokers need to know

AI is helping businesses become more productive. It's also helping cybercriminals create more convincing phishing emails, scams and impersonation attacks.

Breach Counsel

Specialist lawyers who help organisations respond to cyber incidents.

What brokers need to know

They often coordinate the incident response, advise on legal obligations and help businesses understand what they need to do next.

---

24 hour Breach Response Hotline

A dedicated incident reporting service available to insureds following a cyber event.

What brokers need to know

Early notification allows breach counsel and other specialists to be engaged quickly, often reducing disruption and improving outcomes. It’s important to refer to the policy wording for how to notify claims to insurers.

Business email compromise

A type of fraud where criminals gain access to, impersonate or spoof a legitimate email account to trick individuals into transferring funds or disclosing information.

What brokers need to know
Many cybercrime claims involve BEC rather than a traditional "hack". A convincing email can result in significant financial loss without any systems being encrypted.

Business Interruption Losses

The financial impact of a business being unable to operate normally.

What brokers need to know

The biggest cost of a cyber incident is often the disruption caused to trading, production or service delivery rather than the attack itself.

Data Breach

Unauthorised access to sensitive or confidential information.

What brokers need to know

A data breach can trigger legal, regulatory, operational and reputational consequences, even when no money is stolen.

Data Mining

The process of reviewing compromised data to identify what information has been affected and who may need to be notified.

What brokers need to know

Data mining can significantly reduce notification costs by identifying exactly which individuals are impacted.

Deepfake

An AI-generated image, video or voice designed to appear genuine.

What brokers need to know

Deepfakes are increasingly being used to impersonate trusted individuals and support fraud or social engineering attacks.

Digital Forensics

The process of investigating how a cyber incident happened.

What brokers need to know

Think of digital forensic specialists as cyber detectives. Their role is to understand what happened, how it happened and what needs to happen next.

Funds Transfer Fraud

The fraudulent transfer of money following deception, impersonation or compromised communications.

What brokers need to know

Often linked to BEC incidents and can lead to substantial losses before the fraud is detected.

Incident Response

The coordinated process of investigating, containing, managing and recovering from a cyber incident.

What brokers need to know

Early incident response can significantly reduce costs and business disruption

MFA (Multi-Factor Authentication)

An additional security check used alongside a password.

What brokers need to know

One of the simplest and most effective cyber security controls available. It's often a key topic in cyber insurance conversations.

OSINT (Open-Source Intelligence)

Information gathered from publicly available sources such as websites, social media and public records.

What brokers need to know

Cybercriminals often use publicly available information to make phishing and impersonation attacks more convincing.

Phishing

A fraudulent email, text or message designed to trick someone into clicking a link, sharing information or taking an action.

What brokers need to know

Phishing remains one of the most common causes of cyber incidents.

Ransomware

Malicious software that prevents access to systems or data until demands are met.

What brokers need to know

The real cost often comes from operational disruption, recovery costs and lost revenue rather than any ransom demand.

Ransomware-as-a-Service (RaaS)

A criminal business model where ransomware developers provide tools and infrastructure to affiliates in return for a share of the proceeds.

What brokers need to know

This has made ransomware more frequent and accessible, allowing criminals with limited technical skills to conduct sophisticated attacks.

Social Engineering

The use of manipulation, trust and persuasion to influence people into taking actions they normally wouldn't.

What brokers need to know

Many cyberattacks target people before they target technology. Social engineering is often at the heart of phishing, fraud and impersonation attacks.

Threat Actor

A person or group responsible for carrying out a cyberattack.

What brokers need to know

Not all threat actors are the same. Some are financially motivated criminals, others are organised groups, insiders or activists.

Vishing

Short for "voice phishing".

A scam carried out by telephone where an attacker pretends to be somebody trusted.

What brokers need to know

If you've ever heard of somebody receiving a convincing call from "IT Support" or their bank, that's often a vishing attack.

Zero-Day Vulnerability

A software flaw that is unknown to the software provider when attackers first begin exploiting it.

What brokers need to know

These vulnerabilities can be particularly valuable to attackers because organisations may not yet have a fix available.

This document provides examples of incidents and does not constitute an expression of coverage under any insurance product. This is not a solicitation or offer for insurance. Coverage is only available from licensed brokers. Coverage is subject to the full terms and conditions of the policy

Cyber risk isn't really about technology.

It's about people, businesses and resilience.

The technology changes.

The jargon changes.

The threats evolve.

But the broker's role remains the same:

Helping clients understand and mitigate risk.

Get in touch with our cyber team via our website

britinsurance.com/insurance/cyber

Continue your learning

For more cyber insights, emerging threats, broker resources and client-friendly content, visit the Brit Cyber Knowledge Hub. The guide is designed to start the conversation; the Knowledge Hub helps you continue it.