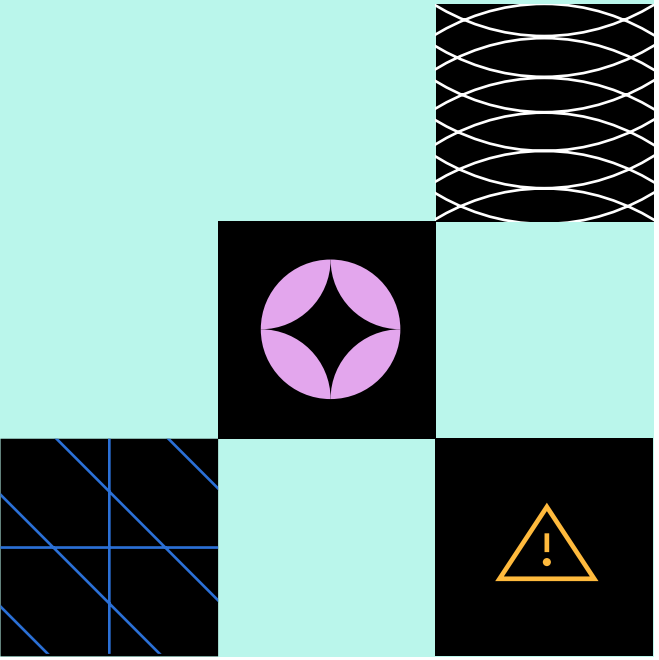
Coalition®

# Cyber Insurance Buyer's Guide

UK EDITION

COALITIONINC.COM

# Table of Contents



# Introduction

**Cyber insurance helps to protect against risks created by the digital economy**

**The business world has changed.** Brick-and-mortar offices have been replaced with digital storefronts, in-person meetings happen remotely, customer communications happen over email and chat, and business assets are increasingly digital and intangible. Technology is now an integral part of every organisation.

All of these technologies can make businesses more efficient and interconnected than ever before, but the benefits come with potential new risks that must be proactively addressed.

**Cyber risk is considered the most important risk for business leaders globally**.[1] Cyber criminals are actively looking to exploit digital risks, and many businesses are unprepared and unable to respond to a cyber incident. Far too often, cyber attacks result in significant financial losses, reputational damage, and in some instances force businesses to cease operations.

## What is cyber insurance?

In light of these growing threats, cyber insurance can be considered as an essential aspect of the modern business' risk management framework. Cyber insurance can provide protection from the financial impact of cyber attacks and digital threats, offering coverage for the financial losses associated with data breaches, cyber extortion, business interruption, and other cyber-related incidents. Cyber insurance can also help your business access a wide range of specialised services to help mitigate the impact of cyber threats, including incident response teams, legal and forensic experts, public relations support, and credit monitoring services.

Cyber risk is constantly changing and evolving, which can make businesses feel helpless. However, if your cyber insurance provider actively monitors your risk and sends routine security alerts, it can help your business improve its cybersecurity posture to prevent digital risk before it strikes.

**No two cyber insurance policies are identical**. When selecting a policy, businesses should consider looking for comprehensive coverage that provides protection from dynamic cyber risks and addresses the most pervasive types of cyber events. **We created this guide to help businesses navigate the complex cyber insurance market and select their coverage with confidence**. With a stronger understanding of how cyber insurance works, you can make informed decisions to help protect your businesses with greater peace of mind.

## About Coalition

Coalition is the world's first Active Insurance company, combining active cyber risk assessment, proactive protection, expert response, and comprehensive cyber coverage. Unlike traditional insurance, which can be passive and slow to respond only after the worst happens, Active Insurance allows Coalition to actively partner with organisations to help prevent digital risk before it strikes.

[1] Allianz, Allianz Risk Barometer 2024

# Understanding Cyber Risk

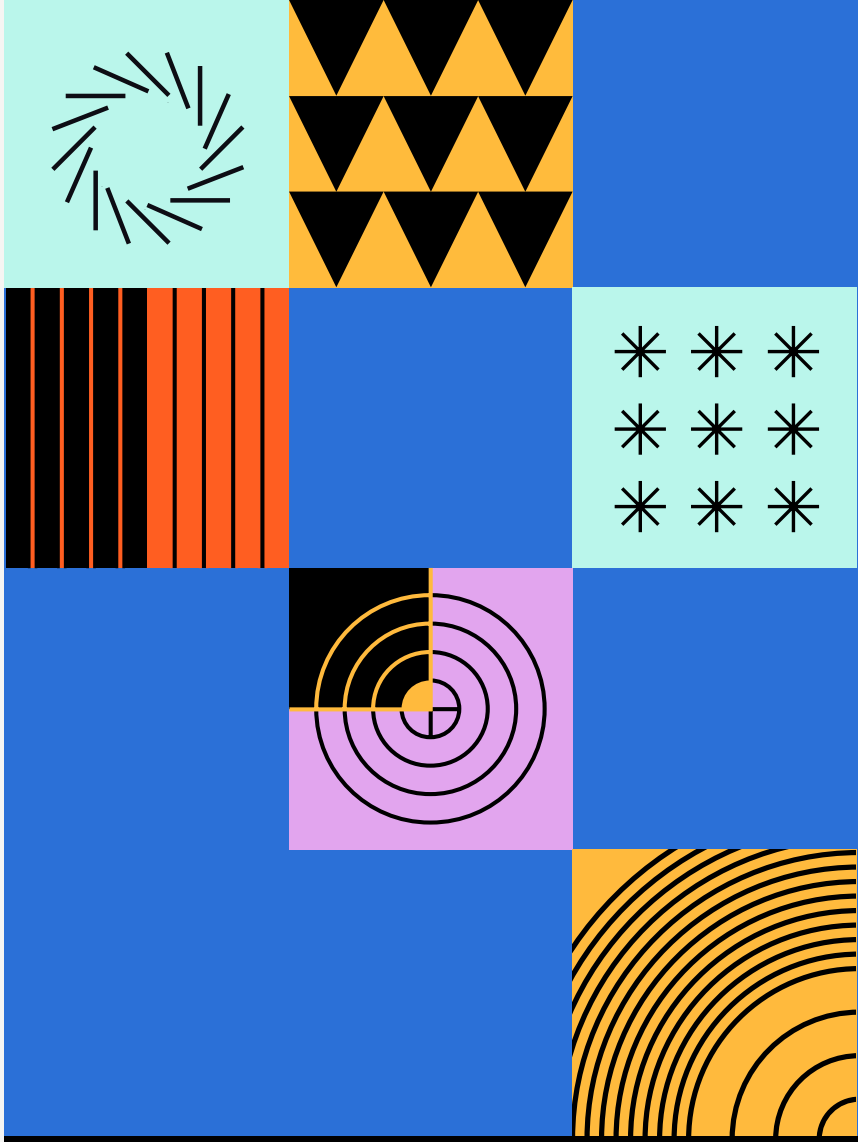
## Why cyber attacks are considered to be the biggest threat to your business

All technology your business uses comes with cyber risk: Email communications, websites, payment processors, even mobile phones are vulnerable to a cyber attack. These technologies can be essential to your business, and cybercriminals actively target weaknesses within these technologies for profit.

Cyber attacks are becoming more common and more costly. Businesses of all sizes, and across various sectors, have become attractive targets leading to a surge in the frequency and complexity of attacks. Total losses due to cybercrime cost the UK economy an estimated £30.5 billion in 2023, hitting 1.5m organisations.[2] According to 2023 Coalition US data, the average cyber insurance claim across all business sizes was $100,000, while small and midsize businesses (SMBs) experienced an average claim amount of $71,000.[3]

A cyber attack can take many forms. Ransomware, funds transfer fraud (FTF), and business email compromise (BEC) are some of the more prominent and impactful cyber threats facing businesses today. Coalition regularly sees claims for each of these event types.

[2] 2023 Beaming study with Censuswide, Price of Insecurity, The Cost of Business Cybercrime in 2023
[3] Coalition Inc., 2024 US Cyber Claims Report



"Maintaining proper cyber hygiene may seem unexceptional, but it comes full circle: robust cyber security improves resilience, and with resilience comes not only stronger defences that deter cyber criminals, but also a much more effective response and recovery process."

**– Jonathon Ellison**
*NCSC Director for National Resilience & Future Technology (Dec 2023)*

# Common Cyber Events by the Numbers[4]

### Ransomware

Ransomware is an attack in which a cyber criminal uses malicious software to prevent access to your data or computer system until you pay a ransom demand. Ransomware can take days or weeks to remediate, often resulting in operational downtime and substantial financial losses.

- Accounted for **19%** of all cyber events experienced by policyholders
- Claims frequency **increased 15%** from previous year (2022)
- Policyholders experienced an average claim amount of **$263,000**
- Average ransom demand of **$1.4M**

### Business Email Compromise

Business Email Compromise (BEC) is a cyber attack in which a cybercriminal gains access to your email account through various means. Once your email account is compromised, the attacker may use the access to launch additional attacks, such as a data breach or funds transfer fraud. If your email account is compromised, it can require costly intervention to respond to the breach and determine if any data was stolen.

- Accounted for **28%** of all cyber events experienced by policyholders
- Claims frequency **increased 5%** from previous year (2022)
- Policyholders experienced an average claim amount of **$27,000**

### Funds Transfer Fraud

Funds Transfer Fraud (FTF) is a cyber attack in which a cybercriminal uses social engineering or other tactics to deceive you into sending money to an unintended recipient. FTF is often perpetrated after a BEC event, though the financial impacts of FTF are typically significantly greater.

- Accounted for **28%** of all cyber events experienced by policyholders
- Claims frequency **increased 15%** from previous year (2022)
- Policyholders experienced an average initial loss amount of **$278,000**

## Can your business survive a cyber attack?

As the impact of cyber attacks increases, the benefits of cyber insurance become more apparent. Businesses of all sizes should recognise the growing threat posed by cybercriminals and consider prioritising cybersecurity measures that can help to protect them from the potentially devastating consequences of cyber attacks.

If you're uncertain about your company's resilience in the face of mounting cyber threats, now is the time to consider a cyber insurance policy that can provide both comprehensive coverage and other tools and resources, including active cyber security monitoring, and an experienced incident response team, to help your business recover quickly after experiencing a cyber attack.

[4] Coalition, 2024 Cyber Claims Report

# Why Cyber Insurance?

## Take an active approach to digital risk management

Cyber insurance can be considered an essential part of risk management that not only helps businesses cover the financial losses resulting from a cyber attack, but also often includes tools and resources to help prevent cyber attacks before they occur. With cyber insurance that provides access to continuous digital risk monitoring and support from cybersecurity experts, organisations can protect themselves from the growth in cyber risks that are often not covered by traditional commercial insurance policies.

### Traditional insurance policies aren't enough

Most businesses take steps to ensure their physical operations are protected against damage and resulting general liabilities. However, traditional insurance policies weren't designed with digital risks in mind.

Traditional Commercial Combined insurance policies help protect your business from third-party claims of injury, property damage and negligence, and are typically limited to addressing physical damage of a tangible asset or to a person. Even professional liability coverages such as Professional Indemnity or Directors & Officers, don't protect from all types of cyber risks. None of these traditional business insurance covers provide adequate protection from the risks inherent in a digital-first world.

Businesses are now choosing to prioritise cyber insurance policies and other cybersecurity tools to protect themselves, as IT budgets are squeezed and skills shortages prevail.

**10%**

of UK businesses' IT budgets are dedicated to security[5]

**3x**

Global cyber insurance market growth in the last 5 years[6]

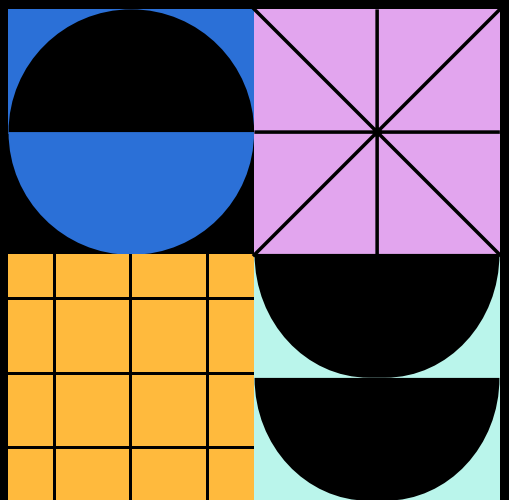
**51%**

of mid-size companies already have or are in the process of buying cyber insurance[7]

[5] Vanta, 2023 The State of Trust Report
[6] Swiss Re, What you need to know about the Cyber insurance market
[7] Coalition Risk Solutions Ltd, Mid-market IT Leaders Survey 2024

# Debunking Cyber Insurance Myths

Whether it's a lack of resources and funding or a misconception that cyber risks only impact large organisations, businesses delay purchasing cyber insurance for a few reasons:



### "My business is too small to be a target."

Many business owners mistakenly assume that small businesses with a low profile aren't targets for cybercrime. In fact, threat actors are increasingly targeting small businesses, which can often have fewer security controls and limited IT security personnel.

**PROOF POINT:** 46% of all breaches impact businesses with fewer than 1,000 employees[7]

### "We don't rely on technology."

Cybercrime doesn't just affect data-rich companies. Every business that relies on technology to operate — mobile phones, point-of-sale systems, payroll, etc. — may become a target of a cyber attack. In fact, email systems are commonly exploited by cyber criminals in phishing and similar attacks.

**PROOF POINT:** 3.4 billion emails containing a malicious link are sent every day[8]

### "We already have protection from cyber threats."

Cybersecurity tools are important in any cyber risk management strategy, but they're only one layer of protection. Systematic protections that businesses employ to combat cyber threats can fail and often don't mitigate human errors. In fact, many cybercrimes and security breaches against organisations are a result of human error.

**PROOF POINT:** 74% of all cyber breaches result from human error[9]

[8] Verizon, 2021 Data Breach Investigations Report
[8] Valimail, Email Fraud Landscape Spring 2021
[9] Verizon, 2023 Data Breach Investigations Report

### "We have coverage in our existing insurance."

Traditional business insurance isn't designed to cover cybercrimes. Most package policies only cover third-party costs, leaving significant coverage gaps that can be detrimental to a business, like loss of revenue due to operational downtime or covering the cost of a ransomware payment.

**PROOF POINT:** 90% of small business owners say cyber insurance is just as important, or more important, than other types of business insurance.[10]

### "Cyber insurance costs too much."

Cyber insurance is a small financial tradeoff for those that rely on digital technology to grow and expand their businesses — and the cost of a cyber incident far outweighs the cost of cyber insurance premiums.

**PROOF POINT:** The average cyber insurance claim for businesses of any size is $100,000[11]

## Assessing digital risks

Faced with a growing list of cyber threats and vulnerabilities, it can be hard to determine where to start. Fortunately, certain cyber insurance providers can help you assess your digital risks prior to purchasing a policy. Coalition provides a Cyber Risk Assessment along with your insurance quote that can help identify vulnerabilities based on your company's digital footprint and the types of hardware and software used in your operations.

[10] Coalition, SMB Decision-Maker Survey on Cyber Insurance, 2023
[11] Coalition, 2024 Cyber Claims Report

# Selecting the Right Coverage

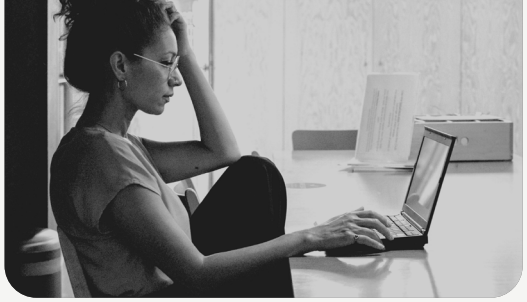
**Prioritise coverage that is designed to protect against dynamic cyber risks**

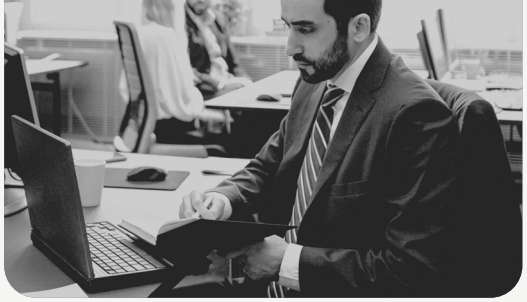
### What to look for in a cyber insurance policy

A cyber event can result in significant financial losses for your business, including damage to technology, loss of data, money directly lost through a FTF or ransom payment, third-party claims brought by customers and vendors, or lost revenue due to downtime and public perception.

However, not all cyber insurance policies are created equal. When shopping for a policy, businesses should consider policies that offer comprehensive coverage by providing protection from dynamic cyber risks and the most pervasive types of cyber events. A comprehensive cyber insurance policy provides crucial coverage across five important areas outlined on the next few pages.

# 5 Important Areas of Coverage





## 1. Direct costs to respond

Responding to a cyber event typically requires numerous direct costs, also known as “first-party expenses.” If your business experiences a cyber attack, you may require incident response, legal services, forensic investigation, help facilitating a ransom payment, and breach notification to comply with regulatory requirements. Simple breach incidents can cost tens of thousands of pounds, while complex matters can increase costs exponentially. When evaluating a policy, you should consider:

**Breach Response →** This covers the costs to respond to a failure of computer security or a data breach, including incident response services, customer notification, credit monitoring, and legal costs.

**Crisis Management →** This covers the costs to respond to a cyber incident, including public relations experts, media purchases, and voluntary notification costs.

**Ransomware and Cyber Extortion →** This covers the costs to respond to an extortion incident, as well as a payment to a cyber threat actor.

## 2. Liability to others

Navigating the patchwork of laws and regulations after a company sustains a security incident or data breach can be difficult for any organisation, especially if you operate in a highly regulated industry across multiple jurisdictions. A ransomware attack or data breach can trigger liability to third parties and cause bodily harm or injury, quickly increasing a company’s losses. When considering a policy, you should consider:

**Network & Information Security Liability →** This covers the liability and legal costs arising from a loss by a third party due to a data breach or a breach in your company’s network security, such as unauthorised access, transmission of a virus, blocked access, or failure to provide notice of a security breach..

**Regulatory Defense and Penalties →** This coverage can reimburse you for claims, expenses, fines and penalties that your company becomes legally obligated to pay because of a regulatory proceeding resulting from a failure in your security or data breach.*

**to the extent insurable under applicable law*

## 3. Business interruption and reputation damage

A cyber event that impacts essential technology can have a significant impact on your ability to operate, which can be highly visible to customers and other stakeholders. Even short periods of disruption due to ransomware or cyber extortion can lead to direct loss of revenue and inhibit your company's ability to operate, negatively impacting customers, employees, and delivery of products and/or services. When evaluating coverages, you should consider:

**Business Interruption & Extra Expenses →** This coverage reimburses your business for your lost net profit, or increased net loss resulting from a failure in your network security or a network systems failure, as well as certain additional expenses your business incurs to resume operations.

**Reputational Harm Loss →** This coverage reimburses your business for your lost net profit, or increased net loss, resulting from negative media exposure after your company experiences a cyber incident.

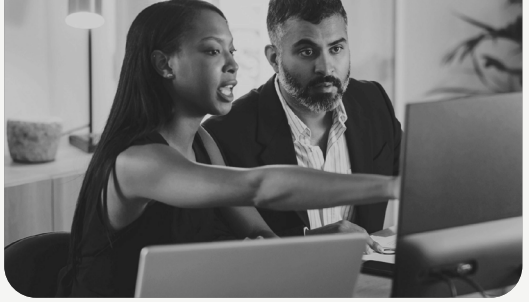
## 4. Cybercrime

Beyond ransomware attacks and data breaches, cyber events can result in financial losses. For example, funds transfer fraud can lead to losing thousands of pounds almost instantly. Attackers can also gain access to email accounts through social engineering techniques, like phishing or business email compromise (BEC), and use credentials to send fraudulent invoices or payment instructions to your customers, vendors, and other third parties. Consider the following coverages when shopping for a policy:

**Funds Transfer Fraud →** This covers funds transfer losses your business incurs from a failure in your security or social engineering.

**Invoice Manipulation →** This covers the net cost of receivables you cannot collect as a result of your customer being tricked into sending payment to fraudsters due to a security failure in your company's network.

**Impersonation Fraud →** This covers your costs to respond to a phishing attack impersonating you, including public relations, reimbursing your customers, and costs related to preventing and mitigating future incidents.



## 5. Recovery and restoration

After a cyber event, resuming operations may prove challenging. If malware damages or destroys essential technology, data, or physical equipment, you may need to bring in external support or purchase new equipment to re-secure systems. Full remediation, restoration, and recovery of your business operations following a cyber event, when possible, can take a significant amount of time and may require purchasing new software, systems, and consultants to rebuild the network. Consider the following coverages in a cyber insurance policy:

**Computer Replacement →** This covers the costs to replace computer systems whose integrity has been permanently altered by malware.

**Digital Asset Restoration →** This covers the costs to replace, restore, or rebuild your digital assets that are damaged or lost following a security failure or network systems failure.

# Understanding your cyber insurance policy

Before you buy a cyber insurance policy, it's important to ensure you understand what is covered and what isn't and how that might impact your business in the event of a cyber attack.

Cyber policies can be tailored to the needs of each individual organisation, and your insurance broker should work with you to include the right coverage, adjust limits and excess, and explain what that means in the context of a cyber event.

# Added Protections and Policyholder Benefits

Some cyber insurance policies go above and beyond industry standards to include additional coverages and policyholder benefits that may not be available elsewhere. Here are additional features to look for in a policy that can give you a distinct advantage in mitigating cyber risks:

### Proactive Monitoring and Security Alerts

Knowing if your business is at risk is a key component of cybersecurity. Coalition[12] continuously monitors policyholders for new and emerging threats in real-time and sends actionable security alerts to help businesses resolve vulnerabilities before they result in financial loss.

### Separate Limit for Breach Response Costs

Having separate limits for breach response allows you to preserve your limits for other coverages, like extortion and business interruption. Included in most Coalition policies[14], this benefit can provide a boost of confidence that your business will have sufficient limits to respond in case of an incident.

### Pre-Claims Assistance

Expertise is critical when dealing with a cyber incident. Policyholders have access to Coalition Incident Response (CIR)[13] for technical digital forensic and incident response services when dealing with a cyber incident if they select CIR from Coalition's panel of vendors.

### "Pay on Behalf" Language

Breach response costs, ransom payments, and other first-party expenses can add up fast. Many cyber insurance providers require you to pay these fees directly and then seek reimbursement. But as a Coalition policyholder, you get the benefit of upfront costs handled on your behalf, so you don't have to wait for reimbursement.

### Access to Expert Incident Responders

Expertise is critical when dealing with a cyber incident. Policyholders have access to Coalition Incident Response (CIR)[13] for technical digital forensic and incident response services when dealing with a cyber incident and benefit from a £0 retention if they select CIR from Coalition's panel of vendors.

[12] Services may be provided by Coalition, Inc.

[13] Coalition Incident Response (CIR) services are available to a policyholder pre-claim or after a claim has been filed. CIR is one of several vendors that Coalition policyholders may engage at the time a claim is filed. CIR is an affiliate of Coalition Risk Solutions Limited. To see a full range of vendors available to Coalition policyholders click here.

[14] Standard for all companies below £100M in revenue, but may be removed upon underwriter review

# Cyber Insurance Buyer's Checklist

## What to look for in a cyber insurance policy

Not all cyber insurance policies are created equal. Ask these questions to see if a provider or policy includes the essential coverage and added benefits necessary to help protect your business from cyber risk.

### Assessment

Does the cyber insurance provider include any of the following to identify the right risks and coverage for your business?

- [ ] Real-time cyber threat analysis
- [ ] Customised business risk assessments
- [ ] Actionable security recommendations

### Protection

What added benefits are provided to help keep your business safe throughout the duration of your policy?

- [ ] Proactive monitoring and security alerts
- [ ] Expert guidance on fixing vulnerabilities
- [ ] Pre-claims assistance

### Coverage

Does the policy include comprehensive coverage that reflects the most common cyber incidents?

**Direct Costs to Respond**

- [ ] Breach Response
- [ ] Crisis Management
- [ ] Ransomware and Cyber Extortion

**Cybercrime**

- [ ] Funds Transfer Fraud
- [ ] Invoice Manipulation
- [ ] Impersonation Fraud

**Business Interruption and Reputation Damage**

- [ ] Business Interruption and Extra Expenses
- [ ] Reputational Harm Loss

**Liability to Others**

- [ ] Network and Information Security Liability
- [ ] Regulatory Defense and Penalties*

**Recovery and Restoration**

- [ ] Computer Replacement
- [ ] Digital Asset Restoration

**Additional Coverage Benefits**

- [ ] Separate Limit for Breach Response Costs
- [ ] "Pay on Behalf" Language

Want to learn more about Coalition's comprehensive coverage? For comparisons and details, visit coalitioninc.com/en-gb/coverages

### Response

Does the product come with added benefits to support your business in the event of an incident?

- [ ] Access to expert incident responders
- [ ] 24/7 claims and incident hotline
- [ ] Proven track record of recovering stolen funds
- [ ] Seamless security service add-ons like MDR (managed detection & response)

**to the extent insurable under applicable law*

Case Study

## Coalition helps manufacturer decrypt data without paying ransomware demands

A manufacturer with no data backups was rendered inoperable after getting hit by a ransomware attack. Locked out of its systems and projecting $1 million losses per day, the manufacturer worked with Coalition Incident Response[16] (CIR) to identify alternative options. Within one day, CIR was able to locate a decryption key for the ransomware variant and unlocked the systems, which allowed the manufacturer to promptly resume operations and avoid a seven-figure ransom payment.[17]

### Ransomware negotiation

No business ever wants to pay a ransom demand. However, when reasonable and necessary, Coalition will help guide your business through the process of negotiating and paying a ransom. In 2023, 36% of Coalition policyholders opted to pay a ransomware demand, and the average demand was $1.4 million.[17] **Through successful negotiation, CIR was able to reduce the amount paid down to an average of 64% of the initial demand.** When shopping for a policy, look for a cyber insurance provider that works with a panel of expert incident responders.

**$1.4 million**

Average initial ransomware demand in 2023[17]

**64%**

Average payment decrease from initial demand via successful negotiation[17]

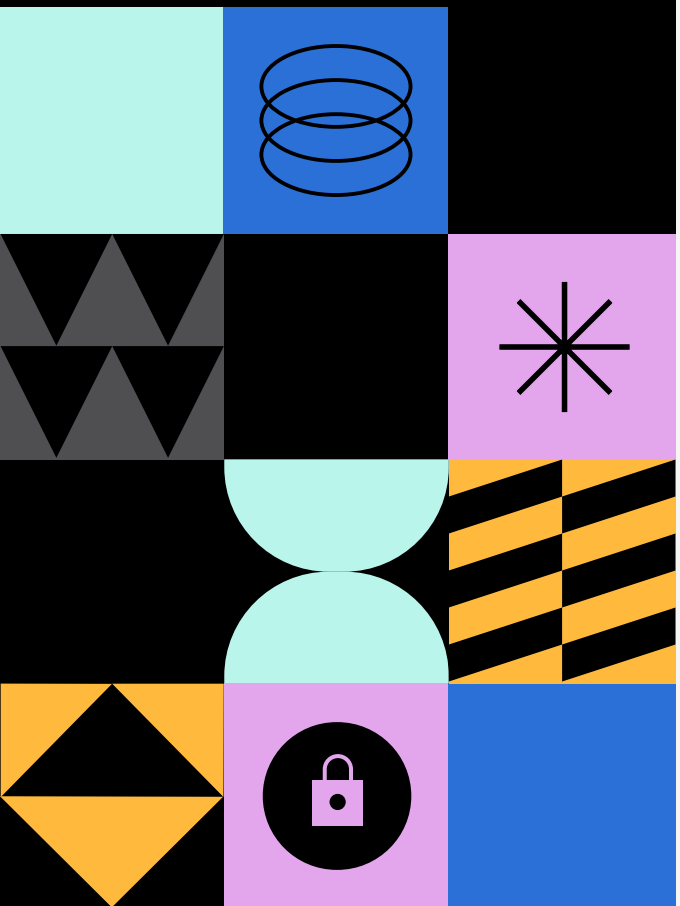
[15] Coalition Incident Response (CIR) services are available to a policyholder pre-claim or after a claim has been filed. CIR is one of several vendors that Coalition policyholders may engage at the time a claim is filed. CIR is an affiliate of Coalition Risk Solutions Limited.

[16] Case study based on a Coalition, Inc. policyholder claim

[17] Coalition, 2024 Cyber Claims Report

*The claim scenarios described here are intended to show the types of situations that may result in claims. These scenarios should not be compared to any other claim. Whether or to what extent a particular loss is covered depends on the facts and circumstances of the loss, the terms and conditions of the policy as issued and applicable law. Facts may have been changed to protect privacy of the parties involved.*

# How Much Does Cyber Insurance Cost?



In today's dynamic market, the cost of cyber insurance can vary widely. Factors that can impact the price of a cyber insurance policy include:

**Technology infrastructure:** More insurance companies are using scanning technology as part of their application process to assess potential vulnerabilities in an organisation's technology and apply it to pricing. Thinking like a cybercriminal allows insurers to gain better insight into potential risk exposures.

**Business industry:** Cybercriminals often target some industries more than others due to perceived weaknesses in their technology or potential for a greater payday.

**Company size and revenue:** While businesses of all sizes are at risk of cyber attacks, larger businesses typically require larger limits and, thus, pay higher premiums.

**Protected data:** The more sensitive data a company transacts or stores, the more likely cybercriminals will be interested in stealing it, reselling it, or using it as leverage in a ransomware attack.

**Coverage amount:** Like other forms of insurance, cyber insurance costs are directly tied to how much coverage is purchased. For example, a £1 million policy limit will be more affordable than a policy that provides up to £10 million in coverage.

Other factors that can influence cyber insurance costs include: increasing demands in coverage, increasing costs associated with cyber incident remediation, and growing sophistication of cyber threats and attack methods.

If a business has recently experienced a cyber attack, its cyber insurance premiums may also become more expensive upon renewal — similar to annual car insurance premiums increasing after a claim is made for an automobile accident. Businesses can improve their insurability and keep their premiums lower by choosing a cyber insurance provider that helps businesses proactively remediate risks and avoid claims.

# Why Modern Businesses Choose Coalition

## Prevent risk before it strikes with Active Insurance

### The Coalition Advantage

Hundreds of thousands of organisations around the globe help protect their businesses with Active Insurance. While many other cyber insurance providers wait for a claim to engage, we use data and security insights to partner with you and help mitigate digital risks throughout the life of your policy. Comprehensive cyber coverage, innovative security tools, and proactive claims handling allows Coalition policyholders to focus on growing their business with protection and greater peace of mind.

HOW WE PERFORM:

**64% fewer**

Coalition claims compared to cyber insurance industry average[18]

**52%**

Reported matters handled without any out-of-pocket payments by the policyholder[19]

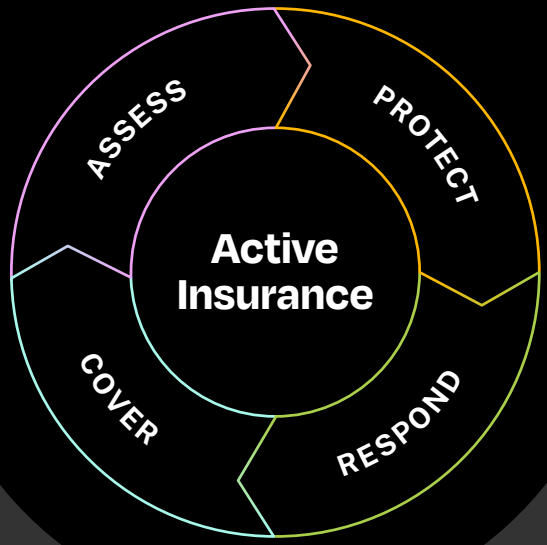
[15] Coalition, 2023 Cyber Claims Report: Mid-year Update
[16] Coalition, 2024 Cyber Claims Report

**ASSESS**
Real-time, external view of cyber risk with customised recommendations

**PROTECT**
Identify and prevent new threats with tailored remediation guidance and support

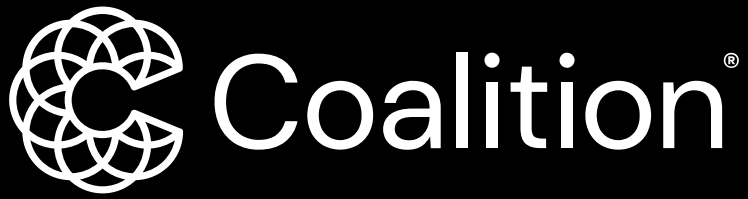
**RESPOND**
Immediate expert support to minimise impact and speed up recovery

**COVER**
Comprehensive coverage to give peace of mind following an attack




**Working with a broker?**
Ask your broker for a quote from Coalition

**Curious about your risk?**
Get your free risk assessment



coalitioninc.com/en-gb

34-36 LIME STREET
LONDON, EC3M 7AT