CLOUDGUARD
Security Done Different

The Cybersecurity ROI Business Case

How to justify cybersecurity spending

2025

Table of contents

Introduction

Introduction

Effective cybersecurity is a core part of doing business. While investment priorities are always competing, smart businesses now recognise that cybersecurity is critical to protecting operations, preserving brand reputation, avoiding costly regulatory penalties and retaining customer trust.

But it is also a journey. It is a continual process of understanding changing risks and threats, reducing your business' security exposure, whilst improving security posture and readiness.

Here's the problem. IT budgets are under significant pressure. You may not have headroom for the security posture improvements that your business needs to make. Now you need to develop a business case for such an investment.

Why?

Because effective cybersecurity protects the operational integrity of your business, both now and in the future.

Think of cybersecurity like an insurance policy. It's there in the event that something untold goes wrong or happens. Investing in cybersecurity doesn't just reduce risks, it protects your business, strengthens trust and ensures long-term success.

This guide aims to walk you through the logic of building a business case with worked examples. Businesses typically consider three principal approaches to investing in improved cybersecurity.

Beyond doing nothing different from today, these are:

1. Internal deployed, developed and managed
2. Product solutions integrated and managed in partnership with providers
3. A complete security partnership and externally managed cybersecurity service

Introduction

Cyber-related attacks can bring businesses to the brink of financial ruin. Under attack, businesses find they cannot operate as designed, face considerable barriers to recovery and suffer significant reputational damage.

But what about cyber insurance?

Whilst cyber insurance may cover immediate costs, an increasing number of smaller businesses cannot secure cyber insurance. This places them at an even greater risk.

Businesses that invest in enhanced cybersecurity not only improve productivity — particularly as more employees work remotely — but also strengthen customer confidence and trust, while protecting shareholder investments. Investors now scrutinise companies' cybersecurity posture and policies as part of their due diligence processes.

50% of businesses and **32% of charities** suffered cyber-attacks in 2024, costing medium-sized businesses **£10,830 on average.**

Unfortunately, 50% of all businesses and 32% of charities reported suffering a cyber-attack in 2024. This cost medium-sized businesses an average of £10,830*.

The impact can be significantly higher in the longer-term, especially as any stolen data is resold on the dark web. There also may be regulatory fines.

On top of this, the threat of subsequent attacks increases by an average of approximately 4 times. Investing in enhanced cybersecurity needs to be prioritised for any business.

This document provides a structure to build the business case to do so.

*Source: GOV.UK, Cyber security breaches survey 2024

The cybersecurity business case

The cybersecurity business case

Whilst cybersecurity is an **integral** part of doing business today, it often requires significant and continual investment.

For small businesses facing today's high costs, cybersecurity risks are just as serious but determining the value of investing in protection is both important and complex.

It requires an in-depth understanding of the threats and risks to your business, as well as operational priorities and impact assessments. We help many of our customers understand and build successful cybersecurity business cases to continually improve their security posture.

Here, we share what we have learnt and how this will help you with your business case. If you need more help – we're happy to support you.

The most effective business cases create succinct focus on these key **RADAR** points:

1. **Risk:** The Threat Landscape and business risk
2. **Approach:** Cybersecurity roadmap and goals updates
3. **Develop:** Business readiness and cyber awareness
4. **Align:** Prioritising and schedule resources
5. **ROI:** Value and measurements

The cybersecurity business case

Initial consideration

Before we dive into the detail on each of these points, there are several elements you must keep in mind as you consider each of the **RADAR** points, as well as how they need to adapt to your business' needs.

- The investment profile is over a time period and requires **continual updates** and reviews to maximise effectiveness
- Unfortunately, cyber threats are **constant.** Your defences must also continually evolve and adapt to the risks to your business.
- There may be non-specific and specific company threats, as well as cybersecurity goals. Your cybersecurity strategy will need to adapt.
- No company is **immune.** Malicious actors are invariably using automated technology to identify targets. Anyone can become a target very quickly. It should be a leading business priority.
- Technology is only part of the story. User behaviours and awareness are a **significant** part of improving cybersecurity in all businesses.
- Automation is key to minimising exposure and risk. It also **reduces** the disruption and cost of any breach or attack.

The business case rationale

Your business case must explain the business benefits of cybersecurity and improving security posture, as well as how these outweigh the costs and risks if it is not approved.

The objective is to include:

1. Cybersecurity objectives
2. Costs - Initial, operational and variable
3. Benefits
4. Why the investment should be made
5. Timescales

When considering cybersecurity, it's important to highlight the risks of not investing.

Relying only on financial metrics may not fully justify the investment, as the potential consequences go beyond just costs.

This guide provides supporting information and calculations on the **Risk Assessment** inclusions.

82%

of cyber attacks are phising related

Only

22%

of UK businesses overall have formal incident response plans

89%

of Small and Medium UK business now work with Managed Security Service Providers.

The business case rationale

93% of UK boards and senior management teams see cybersecurity as a high priority. Despite this, cybersecurity investment levels in 2024 have remained largely stable compared to 2023.

This suggests that many organisations may be maintaining existing commitments rather than expanding them. At the same time, the proportion of businesses seeking external certification has continued to decline, as it did in 2023.

Businesses are reviewing and following the NCSC advice and guidance in the **10 Steps to cybersecurity,** they are just not seeking independent endorsement of these. Only 12% of all UK SME businesses are aware of the Cyber Essentials scheme which is unchanged from 2023.

There has been more focus and resources allocated to **Incident Response** planning. However, only 22% of UK businesses overall have formal incident response plans which is an increase over 2022 of 12%.

One other challenge to note is the timely external breach reporting as measured by the Information Commissioner's Office (ICO). Only 34% of businesses reported data breaches directly to the ICO in 2024 within the guidelines of 72 hours.

The most common cyber threat remains **phishing** related attacks at 82% of all attacks. It only takes **one** attack and one email to reach an unsuspecting individual to be successful.

The problem is...

67% of UK small businesses feel they do not have the in-house skills to manage cybersecurity issues or data breaches.

If that isn't enough, in 2022, there were over 474.2 million ransomware attacks globally. Even with increased cybersecurity investments, the volume of attacks and sophistication is increasing.

Since Russia's invasion of Ukraine, Russian-based phishing attacks against email addresses of European and US based businesses has increased almost 8x.

The problem is 67% of UK small businesses feel they do not have the in-house skills to manage cybersecurity issues or data breaches. That is why 89% of **Small and Medium** UK business now work with **Managed Security Service Providers** (MSSPs).

However, security vulnerabilities in one business can expose partners they are connected with via supply chains or group companies. In 2023, was a greater than 300% increase in supply chain related attacks. These are equally important considerations in your cybersecurity planning.

*Source: GOV.UK, Cyber security breaches survey 2024

The business case rationale

In 2024, only 19% of UK businesses checked the risks from their direct suppliers. Just 27% looked at risks from group companies the same way they do with supply chain partners.

Less than 23% of UK business have a formal Incident Response plan that they have tested within the last 12 months. One of the most important metrics here is the ability to respond and recover. Yet only a quarter of UK businesses have tested and updated a plan.

The Association of British Insurers (ABI) report on 29th January 2025 highlighted there are 5.6 Million SME's contributing £2.6Trn to the UK economy in 2024.

The ABI estimates that 50% of these UK SME's experienced a cyber breach or incident in 2024, yet 97% of these could have been prevented with improved cybersecurity.

The average business impact of downtime is estimated at £2,949 per day with an average cyber-attack recovery taking 12 days. That is an estimated economic impact of £35,388, excluding insurance premium increases and regulatory fines.

Only 57% of UK SME's have cyber insurance coverage, so this cost and impact would be significant to most UK SME businesses.

CloudGuard's 2024 research identified that those businesses with a recently (last 12 months) tested incident response plan recovered 45% faster than those businesses without one.

Stronger cybersecurity can prevent 97% of attacks. And even if a cyber attack does happen, you could recover in just 6 days and save around £17,694 in losses.

This excludes the consideration of any **customer experience** and **reputational impact.**

*Source: ABI, Cyber resilience for SMEs: The insurance gap explored 2025

The business case rationale

Given the supply chain cyber focus, many larger businesses are seeking assurances in the form of **ISO 27001:2022** as a minimum independently certified level of cyber maturity and controls.

SMEs should be considering working towards this standard, which includes many of the best practices included within the ABI cybersecurity improvements that could protect 97% of businesses from a breach.

There is an increasing gap between company board concerns and importance of cybersecurity and tangible actions.

As AI tool adoption rates increase, and business considerations for how this will impact cybersecurity and data controls have to be updated, this gap has the potential to increase further.

CloudGuard's 2024 research found that many of the gaps are relatively easy to fix, including:

- UK SMEs with a clear cybersecurity strategy in 2024 is estimated at 45%. Excellent free preparation tools and guidelines are available from many sources including the NCSC.
- A complete Starter/Leaver and Mover process for all staff – this must include all SaaS and external data sharing services. Over 23% of SMEs failed to remove all SaaS accounts for leavers in 2024.
- UK SMEs need to take into account increased supply chain risks and cyber posture improvements more seriously when operating in international markets.
- Understanding current cybersecurity risks in posture and external business exposure using free services from a variety of cybersecurity providers.
- Ensure externally managed services, such as public facing websites, are regularly updated and all critical and high severity issues are resolved to Service Levels of 14 days or less.
- Ensure all cyber insurance policy conditions are understood and actioned to prevent any challenges in the event of a business incident and subsequent claim.
- All employees receive cybersecurity awareness training at least every 6 months. Any serious weaknesses are followed up with extra support.
- UK SMEs should implement and test an incident response plan at least every 12 months.

*Sources: NCSC, Small business guide: Cyber security, 2025
NCSC, Annual review 2024


Risk

Understanding risk

Understanding the threat landscape and assessing your business risk are two difficult but essential early steps.

Firstly, lets define what cyber risks are.

Risks are defined as...

the potential for disruption, financial loss or reputational damage to your business resulting from a failure in digital systems caused by a direct or indirect cyber event.

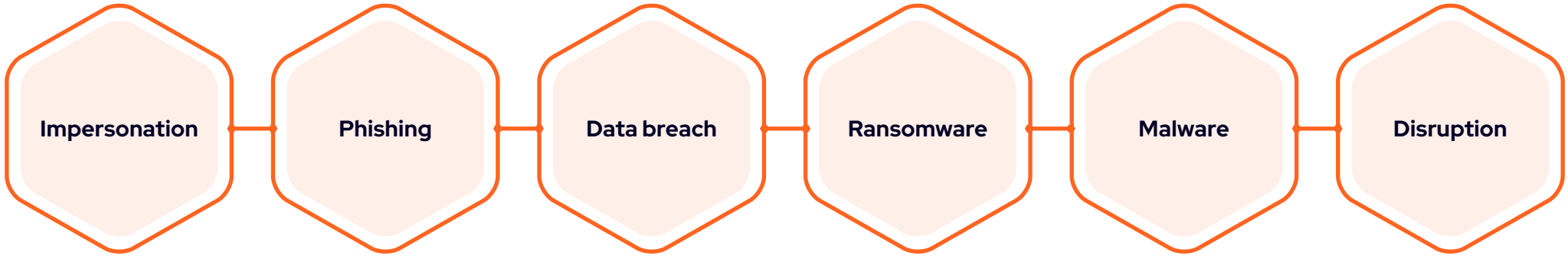
The threat landscape changes daily. **UNLESS** you act now, and keep reviewing your defences regularly, your business risks will grow.

Disruption is the hardest threat to measure because attacks can be slow and sophisticated.

Attackers often gather information, test weaknesses and explore vulnerabilities before escalating.

Most testing is done to determine if they have identified the most effective attack method. Larger, faster attacks are more immediately disruptive, usually targeting a specific weakness with a clear motive.

This graphic outlines the key threat landscape elements every business needs to consider.



Cyber risk types

Many organisations find it difficult to measure risk. To help with this, we've created a simple summary approach to make risk quantification easier. There are many risks to consider, so the best way to measure them is by grouping them into categories. This makes quantification easier.

Category	Type of cyber security risk						
Credential stealing	Email compromise	Social engineering	Service breach	3rd party breach	Malicious UR	Account takeover	Session hijacking
Phishing / Quishing	Email phishing	Smishing	Vishing	Whaling	Spear phishing	Angler phishing	Quishing
Impersonation	Deep fake	Whatsapp interception	Social engineering	Spear phishing	Email spoofing	Domain spoofing	Account takeover
Data exfiltration	Innappropriate access	Employee data theft	Incorrect transfer	Device theft	Data cleansing	Account takeover	Vulnerability exploitation
Malware	Bots	Malvertising	Adware	Rootkits	Keyloggers	Trojans	Spyare
Ransomware	Data encryption	Backup encryption	Device encryption	Storage encryption	RaaS	Leakware	Lockers
Deepfake	Audio messaging	Video messaging	Meeting AI agents	Social engineering	Voice requests	Face swaps	Email re-enactment
Business disruptions	Denial of service	Website defacing	Fake feedback reviews	Domainsquatting	Typosquatting	Impersonation	Social engineering
Misconfigurations	External services	IT systems	Cybersecurity systems	Attack evasion	3rd party breach	AI tools	API interfaces
Vulnerability exploitation	Critical vulnerabilities	High severity issues	Insecure services	No account MFA	Weak passwords	Quarantine override	Insider threat

But remember the risk definition. **Knowing the risk** and **reducing risk** through improved protection are two different things. Your cyber strategy must define **"how"** you will use your sources of threat intelligence to continually reduce risks.

There are many continually updated sources of threat intelligence available to your organisation. Several trusted free sources are listed below.

AlienVault

Spamhaus

SANS Institute

VirusTotal

Risk framework

Calculating cyber risk

Within the cyber industry, a commonly used calculation of business risk is as follows.

Risk = Likelihood x Business impact

We now have defined risk and the categorises of risk, so we can now move to assessing risks in more detail. A **risk assessment** framework is a very useful approach to assessing your risks.

A risk assessment framework

This framework has four categories of risk we allocate a business risk into:

- **Known Known Risks –** These are easily identifiable risks where the impact can be measured and the return on investment (ROI) for protection can be determined. For example, losing a major customer due to a data breach or service failure caused by cyber disruption.
- **Known Unknown Risks –** Risks that are recognised but difficult to quantify in terms of impact or likelihood. While regulatory fines may have predictable ranges, the probability of a data breach due to an employee or subcontractor is much harder to determine.
- **Unknown Unknown Risks –** The most dangerous risks. They are unforeseen or emerge suddenly. Since they are unknown, they cannot be quantified in advance. For example, zero-day cyber threats or unprecedented global events like the COVID-19 pandemic. Readiness and business continuity planning are key to managing such risks.
- **Unknown Known Risks –** Risks caused by negligence or process failures. Businesses may ignore these risks because they assume adverse events won't happen. These risks are often overlooked in continuity planning. For example, a bank knows that rumours could cause customers to take out their money but it's hard to predict how big the impact would be.

Risk focus areas

OK, so we have this framework to assess and categorise risks. Risks in your business will be spread across a number of areas. To help understand the key drivers of operational risk, the following 4 areas of focus can be used.

People

Employee integrity is a business responsibility, ensuring that all staff and agents follow established processes and report any failures. Governance is implemented to provide guardrails and guidelines to avoid the risk. Regular training and awareness sessions in cybersecurity are also an imperative here. Why? Many malicious actors attempt to exploit human weaknesses first.

Processess

Many businesses operate with defined workflows and processes, and invest in process improvement to close any identified gaps or changes. Unfortunately, impersonation is a significant threat in many cyber events, so processes need to be augmented to check and validate authenticity of the parties involved.

Systems

Data classification and sensitivity is an increasing challenge in terms of protecting data in all processes, and ensuring appropriate management. The responsibility, and risk, is wholly on the company to ensure appropriate data security at all times. The controls and governance need to extend to unauthorised data access management, as well as monitoring to detect and prevent data loss.

External events

Malicious actors repeatedly seek to disrupt the operations of any business externally. Relatively few companies have included cybersecurity readiness testing within business continuity plans should such events occur. As a result, when organisations are attacked, their response often falls short. This is something attackers notice. But when businesses respond quickly, they can greatly reduce the damage from an attack. This includes understanding what data or systems are affected and stepping in to stop data loss or impersonation.

The output of the risk section should be a table listing your risks, organised using the **risk assessment framework and categories**. You can revisit this table at any time to reassess and update your risks.

Risk approach

We now move on to the approach for **building a Business Case** and **calculating Return on Investment (ROI)**.

ROI is a well-established method used across many organisations, and there may already be a relevant template in place.

Effective risk management relies on a business' ability to identify, assess and mitigate risks.

Classification, therefore, is the first step in managing risk. However, there is no universal framework for classifying cyber risks.

One widely adopted method, popularised by former **US Secretary of Defence Donald Rumsfeld**, is the **Known and Unknown framework**.

This straightforward matrix categorises risks based on current knowledge, while acknowledging that some risks remain unknown, regardless of how much intelligence is available.

Before we examine this framework, it's worth briefly considering what it is you are aiming to protect.

Business case template

There are many good sources of templates available to support the approach. In our experience, a simple structure containing the following suggested sections provides an effective approach.

Cyber Business Case Section	Description
Project details	Provide a project name, owner, team, sponsor and duration to service benefits
Executive summary	1 page review summarising the risks, options and business need
Product/Service outline	Current state analysis, threat landscape, why it is being considered
Project definition and scope	Define goals, key metrics, interested parties, business requirement
Project timeline	Provide a high level timeline and deliverables
Commercial considerations	Summary of considered approaches
Cybersecurity strategy	Summary of strategy, objectives, feedback from references
Return on investment	Financial analysis of options versus business benefits with returns
Risk assessment	Explain risks and risk profile in order to support comparison and investment decision

What are you protecting?

As you create the executive summary, it is essential to have a view on business value and what you are protecting.

Most metrics are based on revenue metrics, and correlate to the cost of disruption, but you may also want to consider other potential costs.

These include but are not limited to:

- Brand reputational impact
- Customer confidence loss
- Investor confidence loss
- Customer churn or loss
- Compliance and legislative fines
- Uninsured recovery costs
- Employee burn out
- Opportunity cost of investment (in terms of maintaining inferior cybersecurity posture)

Examples of risk

Examples

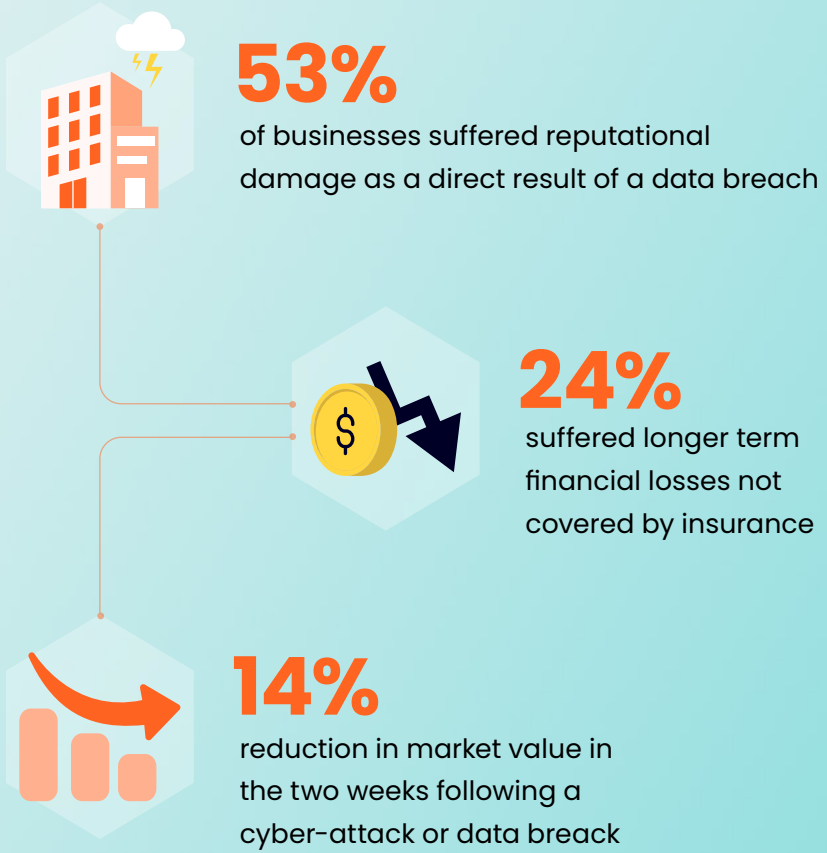
Where an organisation is targeted by malicious actors, all categories of cybersecurity risk may be automatically scanned to identify weaknesses. This is a relatively low-cost exercise for the perpetrators, so it has a **high likelihood.**

If this identifies weaknesses, the perpetrators will assess the organisational properties to prioritise how they could **exploit** a targeted attack. This will cross reference this to what will provide the **highest likelihood** of a ransom or disruption.

They approach it in the same way looking at organisational revenue, profitability, service lines, supply chains, identified protections, hosting arrangements and industry legislation.

Attackers usually focus on quick, short-term gains or the immediate impact on a business. This means they most often **targeting revenue.**

Many organisations have worked tremendously hard for many years. Unfortunately, reputational damage or loss of customer confidence can happen quickly. Recovery can be even more difficult.



53%
of businesses suffered reputational damage as a direct result of a data breach

24%
suffered longer term financial losses not covered by insurance

14%
reduction in market value in the two weeks following a cyber-attack or data breack

*Source: ABI, Cyber resilience for SMEs: The insurance gap explored 2025

The cost of risks

The cost of risk is more difficult to assess.

An ABI report in January 2025 found that 53% of businesses suffered reputational damage as a direct result of a data breach, whilst 24% suffered longer-term financial losses not covered by insurance following a security breach.

The insurers Aon and Pentland Analytics estimated in 2024 that larger organisations can experience a fall of an average 14% in market value in the two weeks following a cyber attack or data breach. This value can increase further dependent on the response and recovery of an organisation.

To understand more about how these risks can affect your business and how to **calculate your business risk,** CloudGuard has further tools to complete a rapid high level impact assessment.

It is important to **understand what you are protecting** to calculate the best investment and **value** of this investment. This helps to ensure that it is proportional in the same way you would estimate the value of insurance coverage for business continuity.

*Source: ABI, Cyber resilience for SMEs: The insurance gap explored 2025

Planning for cyber investment

Planning for cyber investment

Save point! We now have:

- A framework to categorise risks and have identified
- An approach to assess operational risks

How does this inform our overall strategy and actions?

As part of CloudGuard's CISO Advisory Services, we work with clients to identify a simple and effective 8-step process to create and continually review your cybersecurity strategy.

We guide clients through this 8-step strategy, which is rooted in **Secure by Design principles**. It ensures systems are architected for security from the start and delivered with **Secure by Default configurations.**

Why Secure by Design?

- **AI & open source risks:**
  - No universal standards for AI training source validation.
  - Open-source tools lack consistent SLAs for vulnerability management, potentially impacting cyber insurance compliance.
- **AI tool maintenance:**
  - Frequent updates required due to evolving algorithms and usage policies.
  - Use private LLMs only, aligning with Secure by Design/Default principles.
- **Application security:**
  - Regular hardening (e.g., CIS standards), reviewed quarterly.
  - Enforced MFA and strict privileged access controls.
- **Secure software supply chain:**
  - Vendors must follow Secure SDLC and prove Secure by Default capabilities, eliminating the need for add-on security.
- **Monitoring & integration:**
  - Solutions should natively support SIEM/SOAR integration with standardised logs and syntax.
- **Secure APIs:**
  - APIs must be Secure by Default, independently tested, and certified.

Developing a cyber investment plan

Great progress!

You should now have a clearer understanding of risk and a structured approach to building an effective, continuously reviewed cybersecurity strategy.

The next step in our business case is to define detailed objectives that will support our strategy.

Just a word of caution: there are many other excellent frameworks and sources of security best practices available. It can become harder to measure both success and return on investment when you start **blending** approaches.

NIST is a commonly adopted framework, as is **CIS**, but smaller customers can find the level of detail involved in NIST very time intensive and not as relevant for them.

CIS is more adaptable to smaller organisations, but mixing the frameworks can have **implications** for measurements.

Zero Trust Security for many businesses is another framework and cyber strategy but this can involve significant changes. Whilst it should be a longer-term goal, it can involve significant changes to business processes, workflows and security policies.

If not managed appropriately, this can cause unintended consequences of individuals unable to complete processes and affecting business performance.

As you improve cybersecurity **processes** and **maturity,** malicious actors often **shift their focus** to supply chain disruption, software code controls and impersonation attacks.

Forecasting time allocation for cyber investment

With more businesses operating remotely or in hybrid models, maintaining visibility into security issues and ensuring effective awareness training has become more challenging. A strong cybersecurity strategy **must** include continuous updates to user awareness programs and training.

Additionally, security workflows and processes must be regularly adapted to keep pace with digital transformation.

To develop an initial plan, simply follow the 8 steps from page 23 of this guide. The table below provides an idea of the time investment for a **typical SME with 100 to 150 employees.** This includes manages standard cybersecurity risks and non-sensitive data in-house.

Cybersecurity plan	Estimated effort (days)	Support
Security risk assessment	3	External services recommended to review and analyse any issues
Business goals	4	Internal and key stakeholders alignment and approvals
Solution evalutaion	8	Evaluate options to optimise protection with continual improvements over time
Framework adoption	4	Ensure all key business teams are aligned, communicated and supporting
Security policies & controls	10	Ensure all key business teams are aligned, communicated and supporting
Risk management plan	11	Ensure all key business teams are aligned, communicated and supporting
Implement security strategy	7	Ensure all key business teams are aligned, communicated and supporting
Test incident response plan	2	Ensure Board, Business and IT teams are involved, communicated and updated
Security review	3	Review and measure KPI's for continual improvement & risk identification
Total effort days	**52**	

Total effort days

52

Aligning the plan to your business

People often take on multiple roles in SMEs. Cybersecurity responsibilities become shared across multiple roles. It can be really challenging to prioritise the resources needed to successfully implement and continually review optimal cybersecurity practices.

To help understand **best practices** and accelerate implementation, external expertise is often crucial in several areas. It's highly recommended to **identify a partner** who will help you achieve this.

There is substantive information available on security controls, governance and best practices. The downside? Reading all the relevant documents and updates can be a time intensive task.

It is best to align business resources on where that investment of time will be **most effective for you.** It is equally important to align the different business areas, owners and board members to the agreed goals, as well as policies.

This **maximises buy-in** and maintains awareness. This is absolutely fundamental to continually improving security posture.

Ensuring **continual alignment** to the principal risks and preparation activities should be important to any organisation wishing to maintain optimal levels of **cybersecurity effectiveness,** as well as identifying areas of change in risk and impact.

Many organisations choose to implement **Cyber Essentials,** a government backed initiative to guard their organisation against cyber-attacks.

This certainly encourages organisations to think about cybersecurity levels and align plans to the most common types of cyber risks.

Risks constantly evolve. They require continuous review and optimisation, just like regular security testing. Ongoing alignment and investment are essential to adapting to new threats effectively.

Most international companies will recognise **ISO 27001:2022,** so it is recommended to carefully consider the needs of your customers and suppliers in terms security certifications over the next 12 months before selection.

Return on investment

Return on investment

Most businesses compare the **gain or loss** from an investment relative to the cost of the investment over a given time period. Whilst you can estimate the likely **cost of a given cybersecurity incident** and multiply this by the expected frequency based on industry data, this remains a somewhat abstract or **high-level approach.**

For a **successful business** case, we attempt to walk through various scenarios to improve the cost risk analysis for the ROI calculations.

Given there are so many variables to consider, just **how do we improve the accuracy** of an ROI cyber investment calculation?

Let's use industry data to help inform us on key inputs.

Over 50% of UK organisations

experienced a successful cyberattack in 2024. However, with added cost pressures and inflation, this doesn't necessarily mean that every business is able to increase its investment in security.

13% of businesses

had a negative outcome such as loss of money or data.

In 2024, AON estimated that the average data breach cost an enterprise business **£1.24 Million.**

This is significantly above alternative UK specific estimates from the Department of Culture, Media and Sport. They looked specifically at data breaches from business of all sizes and stated the **average costs was £32,388,** a reduction of 38% over 2022.

This estimated value clearly depends on organisational size, data sensitivity and the type of security incident. The point is, with such a range, **where do you position a ROI calculation?**

*Source: UK Data Breach Survey 2024

Investment context

Security budgets remained flat in investment growth terms at 12%. The key difference was **83% of organisations** moved to products that incorporated more AI, automation and machine learning.

As a result...

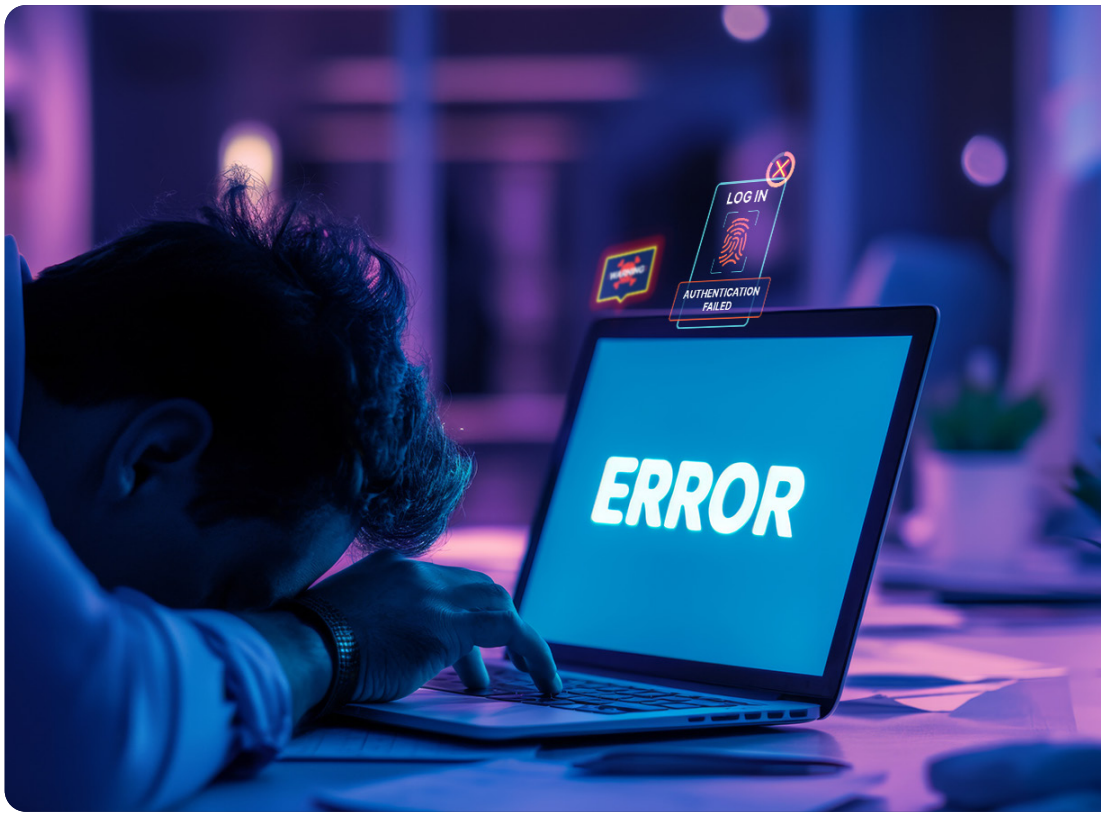
57% of ransomware attacks

were intercepted and prevented from encrypting data.

Only 57% of UK organisations

are operating **with cyber insurance** in 2024. This is down from 67% in 2023.

As claims increase, many organisations are experiencing renewal issues. Most must now demonstrate that they have **Security by Design** embedded to minimise security exposure.



*Source: ABI, Cyber resilience for SMEs: The insurance gap explored 2025

Calculating cybersecurity cost exposure

At a basic level, any business could look at a risk calculation for cybersecurity investment based on the following approach.

Caution: **risks vary by industry sector** and are noted to increase with protected categories of information held. So, simply applying a general number may not be supportive of your business case.

However, to assess ROI for a small business, we first need a **baseline understanding of risk**. Using the previous industry sources, we can extract the following metrics to build a costed risk profile.

2024 cybersecurity exposure	Probability	Cost impact	Frequency	Risk profile
Data breach	42%	£2,949	52	£64,406.16
Phishing emails	83%	£1,032	52	£44,541.12
Ransomware	57%	£471,385	1	£268,689.45
Malware	75%	£2,949	52	£115,011.00
Insider threat	12%	£112,741	1	£13,528.92
Average total annual cybersecurity cost exposure				**£506,176.65**

Cost of internal implementation

Cyber security solution 150 employee business	2024 Annual cost	Cost per user Annual	 Monthly
Software & maintenance	£36,114.00	£240.76	£20.06
Management & updates	£9,316.18	£62.11	£5.18
Governance and review	£6,600.00	£44.00	£3.67
Total	**£52,030.18**	**£346.87**	**£28.91**
Cybersecurity strategy	**Average IT salary**	**Day rate**	**Total cost**
52 days	£46,086.00	£209.48	£10,893.05
Total investment	**£62,923.23**	**£419.49**	**£34.96**

We already worked out that it would take approximately **52 days** to implement and maintain an effective cybersecurity strategy in a business environment. This makes assumptions about cybersecurity posture maturity and existing controls, so this estimate is subject to variation.

For calculation purposes, as internal costs vary significantly, we have adopted a managed approach for the costings. You may need to adjust your own calculation to reflect your specific circumstances.

As you will see, we have arrived at an average UK day rate cost of **£209.48.** We now have an average cybersecurity solution and governance cost for a 150 employee business, as well as a risk profile

The proposed ROI calculation is based on this formula.

ROI
return on investment
=

$$\frac{\text{Net return on investment}}{\text{Cost of investment}} \times 100\%$$

Return on investment

Before we proceed to the calculations, there are **a few considerations** to cybersecurity assessment of ROI we need to **keep in mind.**

ROI is usually expressed as a percentage because ratios are **relatively meaningless** when risk is measured in percentage likelihood.

The ROI calculation uses the net return as the starting point, since the impact of a cybersecurity solution can be positive or negative depending on your business' current state, past cyber incidents and defence maturity.

An ROI calculation should factor in the **time-to-value component**. Using external expertise can accelerate this, offering faster results compared to the time it would take to build skills and develop optimisations internally.

ROI is an **approximate measure** of an investment's profitability. The net return element involves subtracting the initial investment costs from a final value. The time dimension has to be set to define a final value, which is recommended as 2 years.

Resourcing ROI scenario modelling

A frequently asked question is...

how do you compare the ROI of **internal versus external cybersecurity services?**

The answer? There is no single approach. ROI modelling will vary depending on whether you choose to implement and manage the solution internally or bring in expert external support.

We therefore need to model both scenarios.

Cost scenario 1 – Internal implementation & management

In this scenario, your IT team is responsible for deploying and managing the cybersecurity solution. Given the complexity and specialised skills required, including out-of-hours monitoring and response, it may be necessary to augment internal capabilities if there are no dedicated security professionals in place.

For example, if your organisation requires 24/7 coverage, additional staff and expertise will be needed to sustain that level of service.

However, for many SMBs of around 150 employees, full 24/7 support may not be essential. In such cases, critical incidents can be escalated according to a defined SLA (Service Level Agreement). Lower-priority issues may be managed by an on-call staff member outside of regular business hours.

There are two main options to resource this capability: **train existing staff** or **hire experienced professionals**. While it might be assumed that a single resource could suffice, business continuity must be considered. This includes cover for holidays, sick leave and training periods.

Please note: Some cyber insurance providers may not accept this setup as incident management typically requires a minimum of two dedicated individuals. If this isn't feasible, you may need to build additional capability by rotating other staff to support more complex scenarios or prolonged incident response efforts.

If you are required to meet strict SLAs, especially out-of-hours, it is recommended to recruit at least two dedicated security personnel to ensure consistent coverage.

If you're considering building and running your own internal Security Operations Centre (SOC), the following model can help you estimate the potential costs.

£56,086
National average salary for UK SOC employee

1x SOC Manager	2x Security Analysts	2x Incident Responders

SOC Personnel costs	**£374,974**
Total costs with software annually	**£469,054**

Cost scenario 1 – Internal implementation & management

Where building a full SOC isn't possible, hiring a single cybersecurity role is a common alternative. This typically requires a more experienced individual to cover all aspects of the role as it evolves. However, without external support, there is exposure around 24x7x365 monitoring and response. This table compares internal and external recruitment options for smaller businesses.

	Cost description	Cost estimate	Total
Internal recruitment - existing resource with training	External training and support tools	£15,000.00	**£63,073.50**
	75% of time allocated to cyber support (165 days) 13.75 days per month	£48,073.50	
External recruitment - skilled SIEM candidate	Resource oncost	£83,327.40	**£95,927.40**
	Resource recruitment	£9,000.00 (15%)	
	On-call	£3,600.00	

We need to present **a range of cost options** to model different ROI scenarios. One scenario may involve no further investment but this would increase risk, making it more of a risk assessment than a traditional investment analysis.

Where investment is made, the spectrum ranges from businesses choosing to use internal resources (where available) to those recruiting more experienced professionals. Implementing a cybersecurity solution will reduce risk in all cases.

The outcomes fall somewhere between a reduction in cyber incidents, supported by evidence showing that well-managed cybersecurity solutions reduce successful ransomware attacks by 37%, and multiple cyber events occurring at the average 2024 frequency and associated response costs.

Cost scenario 2 – Outsourcing to a managed service

In this second scenario, your business has chosen to outsource its security operations to a **managed security service provider (MSP)**. For simplicity, we've excluded software costs from this comparison to align directly with Scenario 1 (hiring one staff member).

MSPs deploy skilled professionals across multiple customers and a tend to offer a variety of solution models.

At its core, the service focuses on monitoring and responding to identify and manage threats. This is typically delivered through a combination of reactive and proactive measures.

The scope and complexity of the service will depend on several factors: existing security maturity, onboarding needs, the number and type of connectors, application support requirements, compliance obligations and any relevant legislative demands.

Role	Cost description	Cost estimate
SIEM - SOC managed service monitoring	24x7x365 security monitoring	£22,016.00
	24x7x365 detect & monitoring	
SIEM - SOC managed service response	24x7x365 ThreatOps expertise	£18,933.00
	24x7x365 Response	
Average annual service cost (150 users)		**£40,949.00**
Average cost per user per month (May 25)		£22.75

Cost comparisons

Even in a smaller organisation, it is evident that an external managed service can be **more cost-effective** than internal or external recruitment.

The cost modelling shows a **35% improvement** over internal recruitment (excluding the benefits of immediate service commencement over training and recruitment timescales).

35%

Cost reduction for managed service vs internal recruitment

57%

Cost reduction for managed service vs external recruitment

Involving the wider risk assessment in ROI calculations

The percentage of risk reduction is not always proportional to the level of investment. It's important to prioritise the most critical risks and, for any given investment, assess both the likelihood of those risks occurring and the potential impact on your business.

For most organisations, you need to understand **revenue impact** and **service disruption.** This can be profiled at least at a high level reasonably quickly. For the most part, compromises, data breaches and disruption do not work in a uniform way though.

Phishing is still one of the most common cybersecurity threats. Most targeted attacks exploit human interaction, such as deceptive emails or social engineering.

By focusing on the cybersecurity categories related to human engagement (as shown in the earlier table on page 15), your business can better prioritise solutions and estimate the risk reduction each one offers.

We can assess risk by looking at the number of identified attacks and estimating their likelihood with a given cybersecurity solution. This includes factoring in the chance that the chosen solution won't fully prevent an attack.

For example, a phishing email still reaching an employee, who then clicks on a suspicious link. Even with security solutions in place and ongoing policy improvements, phishing remains the most common threat.

Despite investment, it is still the **most likely** to succeed and require further business intervention to manage the risk.

Calculating risk reduction

When considering the business case **risk reduction,** cybersecurity solutions absolutely reduce risk but cannot **eliminate risk completely.**

For example, as phishing related data breaches and attacks represent the **highest percentage** of both business risk and likelihood, it still involves a greater percentage of human engagement and behaviours.

As a result, there **remains risk from likelihood** that behaviour, particularly in very sophisticated attacks, regardless of technology, may result in a breach.

You must carefully consider various factors when assessing the ROI of a cybersecurity solution. **No solution can provide 100% protection** against all threats, whether existing, modified, new, or emerging. However, with proper management, most solutions can significantly reduce business risk through prevention.

The key factor in minimising disruption, loss, and overall risk is **time.** Fast detection, mitigation, intervention, response and resolution depend on **automation-driven** strategies.

Cybercriminals are **using automation** at scale, and the only effective defence is a similarly automated approach.

Business priorities	Identified attacks	Likelihood with investment
1 Phishing	83%	16%
2 Data breach	34%	11%
3 Ransomwre	24%	9%
4 Disruption	18%	5%
5 Impersonation	31%	4%
6 Malware	35%	3%

Calculating your risk-based return on investment

For this ROI calclation, we are looking beyond a single threat type to model the average likelihood of an attack across common vectors including phishing, data breach, ransomware, disruption, impersonation and malware.

Without additional investment, the average likelihood of an attack is estimated at 38%. With investment in any of the three protection options, this reduces to an 8% average, giving a 30% risk reduction. This was outlined on the previous page.

To quantify return on investment, we apply this 30% reduction to an estimated annual incident exposure cost of £506,000, resulting in a risk reduction value of £151,800. This value is then compared to the cost of each solution to calculate a risk-based ROI. This is focused on avoided losses rather than revenue generation.

The table below outlines the key inputs and outcomes for each option.

As the table shows, while all three options deliver a positive return through reduced risk exposure, the managed service model offers the most cost-efficient ROI.

Internal recruitment delivers value but at a 46% lower return compared to managed services, while external hiring sees ROI fall by nearly 78%.

These differences highlight the importance of aligning investment with both risk and operational efficiency. This is especially for smaller businesses managing tight budgets and evolving threat landscapes.

Investment option	Solution cost (£)	Risk cost (£)	Risk reduction (%)	Risk reduction value (£)	ROI (%)	ROI % lower vs managed
Managed service	41,949	506,000	30	151,800	261.8	-
Internal recruitment	63,073	506,000	30	151,800	140.5	46% lower ROI
External recruitment	95,927	506,000	30	151,800	58.2	78% lower ROI

Note: ROI here reflects the value of avoided risk, not revenue gain. This a key distinction when evaluating cybersecurity investments.

Methodology and calculations

Risk-based ROI formula

Return on investment

=

$$\frac{\text{Risk deduction value - Cost of solution}}{\text{Cost of investment}} \times 100\%$$

Risk reduction value formula

Risk reduction value

=

Risk cost × (Likelihood before - Likelihood after)

Input values used

- Risk cost (average incident exposure): £506,000
- Likelihood without investment: 38%
- Likelihood with investment: 8%
- Risk reduction percentage: 30%
- **Risk reduction value:**
  506,000 × 0.30 = £151,800

Solution costs

- Managed service: £41,949
- Internal recruitment: £63,073
- External recruitment: £95,927

ROI calculations

- Managed service:
  (151,800 - 41,949) / 41,949 × 100 = 261.8%
- Internal recruitment:
  151,800 - 63,073 / 63,073 × 100 = 140.5%
- External recruitment:
  (151,800 - 95,927) / 95,927 × 100 = 58.2%

ROI reduction compared to managed service

- Internal recruitment:
  (261.8 - 140.5) / 261.8 × 100 = 46.3% lower
- External recruitment:
  (261.8 - 58.2) / 261.8 × 100 = 77.8% lower

And finally

Making the cyber case stick

Building a business case for cybersecurity investments requires focus on **key metrics** that will be used to support the investment return.

These key metrics are:

- Continually reducing security exposure and vulnerabilities
- Continually increasing security posture

Where there are incidents, the key metric is **mean time to resolve (MTTRe).**

Many investors have a sound appreciation of the increased business risk and disruption caused by cyber events. It can be more difficult to understand specific business risks, but we have hopefully provided an approach to enable any business to assess this in the framework.

We have also provided **ROI analysis** based on different approaches to enhancing cybersecurity, including internal vs external resourcing.

The basis of any solid business case is a **clear problem definition** with the measurement of success and return. The first perspective you need to understand is your business value as measured by assets, people, customers and shareholders.

You are investing to **protect this value** from risk and threats in a similar way that businesses protect with insurance coverage, security and safety measures from physical threats. Once you have this value, you can readily update this on a **monthly or quarterly** basis as risks and threats evolve with your new cybersecurity service.

Making the cyber case stick

On very **rare** occasions, some businesses wrestle with the prioritisation of cybersecurity investments vs other business needs. This may **challenge** you on the basis the return is unclear or lower than alternative investments.

If you do not invest in cybersecurity, the majority of businesses **will** experience a cyber event of some description.

This is not fear, uncertainty or doubt. This is a **regrettable reality** of the digital economy we all work in. The cost to a business is indeterminate.

If a board makes such a decision, it is the responsibility of the board to report this to shareholders, investors and customers in terms of previous considerations and rationale for not investing in improved cybersecurity posture.

According to the UK SME Chamber of Commerce, 61% of UK SME businesses **fail within 6 months** after a large cyber incident.

On one final note, we want all businesses to continually improve their cyber security posture. If you need help at any time, please feel free to reach out to our Guardians at CloudGuard.ai

Meet the author

Matt Lovell

Co-founder and CEO of CloudGuard

Matt, co-founder and CEO of CloudGuard, is an IT industry veteran with 35 years of senior experience. He has held pivotal roles at major organisations including Microsoft, Severn Trent Plc, Perot Systems, Computacenter, Digica, Pulsant, BCN, SmarterMed and SoftwareONE. He has been a Microsoft Certified Technical Architect since 2003 and was honoured as a CIO100 member in 2015, 2018, 2020, and 2021.

Since 2008, Matt has led advancements in AI and automation. Under his guidance, his team pioneered the use of machine learning to analyse extensive datasets across industries such as cybersecurity and utilities. His deep understanding of these technologies has driven innovation and positioned him as a thought leader on their ethical implications. He has shared his expertise at global conferences, discussing the transformative potential and ethical considerations of AI and automation.

Beyond his IT career, Matt has been a significant investor in renewable energy since 2010, reflecting his commitment to sustainable development.

Affordable 24/7 security for SMEs without adding to your IT budget

Security shouldn't drain your time or your resources. **CloudGuard's PROTECT Managed XDR Service** gives SME IT teams full 24/7 threat detection and response at a fraction of the cost of building your own SOC.

Our UK-based Security Operations Centre and advanced automation keep your business secure. No need to hire or manage extra staff.

- Seamless integration across your whole environment
- Fully automated deployment for faster onboarding
- Quarterly CISO-led reviews for continuous improvement
- UK-based Security Operations Centre for real-time response
- Backed by advanced automation and hands-on expertise

Why choose CloudGuard PROTECT MXDR?

One intuitive dashboard for complete visibility

Rapid deployment, zero downtime, zero disruption

Enterprise-level protection, SME-friendly pricing

24/7 threat monitoring by expert SOC analysts

Cut operational complexity, reclaim IT hours


CLOUDGUARD
Security Done Different

That's your lot for now!

Complete the form to access the full version of this white paper.