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


CLOUDGUARD
Security Done Different