Digital Security
Progress. Protected.

THE TRUE COST OF CYBER ATTACKS:

Balancing business protection and risk

Executive Summary

This report explores the extent of cybersecurity measures, the prevalence and costs of cyber attacks and the impact of cybersecurity investments on business performance.

CYBERSECURITY MEASURES AND PREPAREDNESS

Nearly half (45%) of surveyed UK businesses manage cybersecurity fully in-house, while 42% adopt a hybrid model combining in-house and outsourced functions and only 12% fully outsource their cybersecurity functions. Cybersecurity readiness and certification levels are high, with 59% certified under Cyber Essentials or Cyber Essentials Plus and 46% meeting ISO cybersecurity standards; 85% of businesses also report a dedicated cybersecurity budget. Most surveyed UK businesses (77%) planned to increase their budget in the upcoming year. The primary drivers behind these increases included growing cyber risk concerns (69%), greater financial resources (46%) and recent cyber attacks (16%) influencing budget decisions.

PREVALENCE OF CYBER ATTACKS

Cyber attacks remain a significant challenge for surveyed UK businesses, with 53% of UK businesses reporting an attack in the past three years. Looking ahead, 43% of respondents believe their organisation is likely to experience a cyber attack within the next year.

COST OF CYBER ATTACKS

Cyber attacks cost UK businesses an estimated £64 billion annually, with £37.3 billion in direct costs and £26.7 billion in indirect costs. Consumer-facing services[1] face the second-highest absolute costs (£18.5 billion). On a regional basis, South England bears the highest financial burden (£35.7 billion), while the Midlands experiences the lowest (£7.2 billion). The most significant direct cost was the time spent by staff on dealing with such attacks, whereas the most significant indirect cost was the subsequent increase in cybersecurity budgets. Despite the cost, 93% of businesses experiencing attacks reported having sufficient reserves to cover the costs of the attack, with financial and insurance firms being the most prepared.

IMPACT OF CYBERSECURITY ON TURNOVER

The majority of surveyed businesses (53%) note that cybersecurity has a positive impact on turnover beyond just improving security. Cybersecurity investment boosts UK companies' revenue by 0.5%, which translates to £27 billion a year. Key channels through which cybersecurity investment positively impacts growth included winning clients (70%) and IT system improvements (68%). The information and communication sector saw the highest positive impact, with an average impact on turnover amounting to 1.2%.

[1]Consumer-facing services, as tracked by Cebr, include the following industries: wholesale & retail, transportation & storage, accommodation & food services, real estate, administrative & support activities and Arts, entertainment, and recreation.

Introduction

As businesses become increasingly reliant on digital infrastructure, the risk from cyber attacks only grows. The threats, ranging from ransomware to data breaches, can severely disrupt operations, leading to reputational damage and increased regulatory scrutiny. However, one of the biggest costs to businesses is the financial losses they incur following an attack. Earlier this year, **Southern Water revealed it had incurred costs of £4.5 million** as a result of a ransomware attack in 2024. Just one company name added to the ever-growing list of businesses that are not only falling victim to data breaches and cyber attacks but suffering potentially devastating financial consequences as a result. It has also been reported that banks are **being forced to pay out millions to their customers after months' worth of IT outages.** While many of these outages haven't been reported to have direct links to cyber attacks, outages and the consequences for customers, is one of the biggest risks for businesses when falling victim to an attack.

More recently, an **NHS software provider was fined £3m** by the Information Commissioner's Office due to security failings that led to a ransomware attack on the health service.

In the UK, cybercrime poses a significant challenge to businesses of all sizes, impacting not only individual companies but the broader economy. The rise of AI has further amplified these risks, enabling cybercriminals to launch more sophisticated and automated attacks, such as AI-driven phishing scams and adaptive malware. The financial strain and lost revenue, rising recovery costs and need for stronger measures highlight the urgent need for cybersecurity investment.

Matt Knell, UK Managing Director, ESET, says,

> **"With over 50% of UK businesses experiencing a cyber attack in the past three years, it's clear that no organisation is immune. Businesses must shift from a reactive to a proactive cybersecurity strategy to stay ahead of evolving threats. At ESET, we've found that organisations forced to make a reactive investment can spend more than 10 times as much as they would have spent on proactive measures when recovering from an attack. This highlights the immense financial and operational benefits of early investment.**
>
> **Strengthening cyber resilience is essential not just for business continuity but also for safeguarding the UK's economy stability and growth in an increasingly digital world."**

UK business cybersecurity measures and preparedness

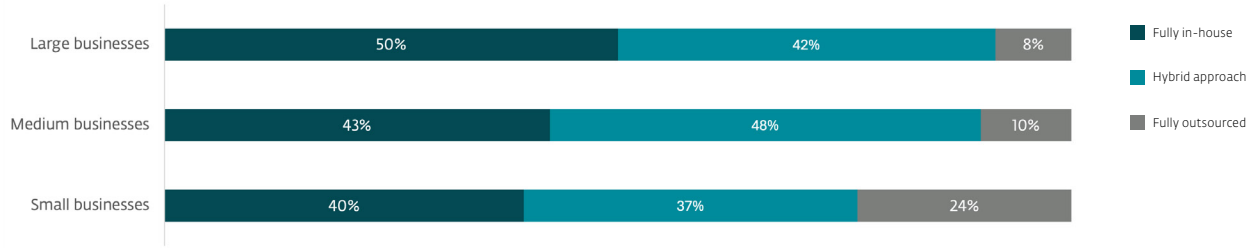
→ CYBERSECURITY STRATEGIES

The landscape of cybersecurity strategies among UK businesses reflects the increasing complexity of digital threats and regulatory pressures. While most respondents (45%) manage cybersecurity functions in-house, and 42% adopt a hybrid approach, combining in-house and outsourced cybersecurity functions, only 12% of businesses fully outsource their cybersecurity functions. However, with the evolving nature of cyber threats and the growing sophistication of attacks, businesses should reconsider their reliance on in-house teams, which may lack the specialised expertise and resources necessary to keep up with emerging risks.

Larger businesses[2] are more likely to fully manage their cybersecurity operations in-house, as they have better access to and greater budgets to support resources for this approach. Meanwhile, small businesses are almost 3 times more likely to fully outsource their cybersecurity management. Even among those with fully in-house cybersecurity operations, 32% report occasional challenges in maintaining adequate resources, indicating a potential gap in security coverage that outsourcing to partners like ESET could address.

We examined the prevalence of industry-recognised credentials to measure cybersecurity maturity. Most (59%) surveyed businesses hold Cyber Essentials or Cyber Essentials Plus certification, reflecting adherence to the UK government's cybersecurity resilience

Cyber security management methods by business size
(As a share of all respondents)



*Business sizes were defined as: Large businesses = more than 250 employees | Medium businesses = 50-249 employees | Small businesses = 1-49 employees

framework. Additionally, nearly half (46%) of businesses meet international standards (e.g. ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 9001). However, 11% of respondents either lack cybersecurity credentials or are uncertain of their certification status, which suggests a gap in awareness or compliance. Outsourcing cybersecurity to a trusted provider like ESET can help businesses achieve and maintain these essential certifications more efficiently.

[2] Large businesses = more than 250 employees | Medium businesses = 50-249 employees | Small businesses = 1-49 employees

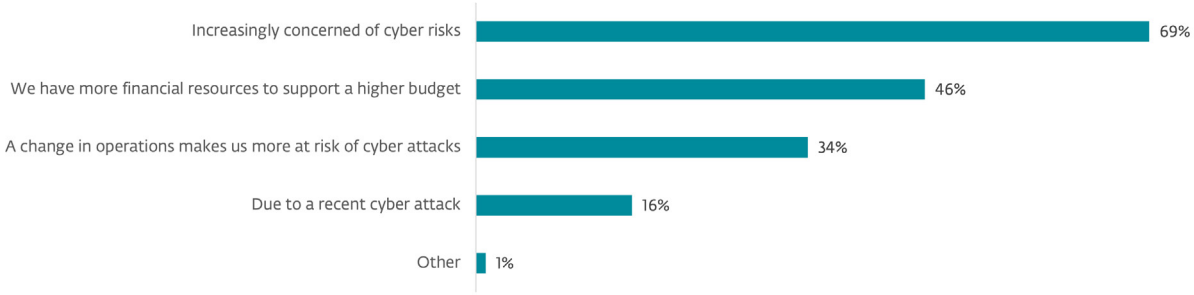
→ CYBERSECURITY BUDGETS

Investment in cybersecurity is increasingly recognised as a strategic priority, with 85% of surveyed businesses reporting an allocated cybersecurity budget. Perhaps unsurprisingly, large businesses are more likely to have a cybersecurity budget (96%) than small businesses (58%). However, simply having a budget does not guarantee effective protection.

Recent **government research** suggests that 43% of businesses have some form of cyber insurance – only 8% have a specific cyber insurance policy, while 35% are covered through a wider policy. While this insurance uptake is encouraging, it still leaves over half of organisations without cover. Cyber insurance should be considered a key element of any business.

Looking ahead, 77% of surveyed businesses plan to increase their cybersecurity budget in the coming year, with an average increase of 12%. The primary drivers for this rise include heightened concerns over cyber risks (69%), greater financial capacity (46%) and recent cyber attacks (16%). While increased budgets are a positive step, businesses must also ensure their spending translates into truly improved security outcomes. Outsourcing cybersecurity to ESET provides access to industry-leading security expertise, advanced threat detection and proactive risk mitigation strategies, ensuring businesses get the most out of their cybersecurity investments.

Reasons for increasing cyber security budget
(As a share of all respondents)



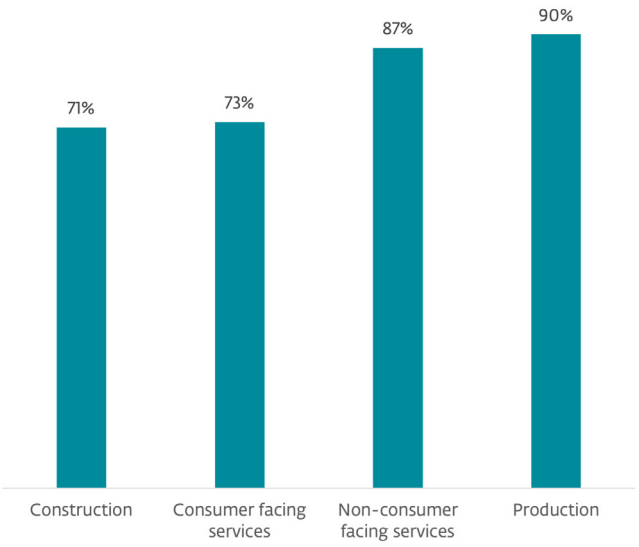
➔ INDUSTRY BREAKDOWN

Cybersecurity budgeting varies across industries and is influenced by sector-specific threats, regulatory requirements and technological dependencies. Across all major sector groupings, over 70% of businesses have a cybersecurity budget, at least, in each grouping. The production sector leads the way, with 90% of businesses allocating funds to cybersecurity, followed by non-consumer services (87%). Within non-consumer services, the information and communication sector reports the highest budget adoption rate at 93%, reflecting the high-value data and intellectual property at risk. The financial and insurance sector also maintains strong cybersecurity investment, with 86% of businesses allocating a dedicated budget, aligning with stringent regulatory requirements like the General Data Protection Regulation (GDPR) and Network and Information Systems (NIS) Regulations.

Investment growth trends also reveal industry-specific priorities. Most businesses (81%) in the production sector plan to increase their cybersecurity budgets by an average of 12%, perhaps driven by increasing digitisation and automation. Non-consumer services firms expect a 13% increase. In comparison, the construction sector reports the highest planned average increase at 15%, likely due to the sector's rising reliance on connected technologies and smart infrastructure.

In contrast, consumer-facing services show a lower appetite for budget expansion, with an average increase of just 7%, possibly due to tighter profit margins and perceived lower cyber risk. However, within non-consumer services financial and insurance services, 89% of businesses plan to increase their budgets, with an average increase of 14%. Similarly, 83% of information and communication businesses intend to expand their cybersecurity budgets, averaging a 15% rise, reflecting the sector's critical role in digital infrastructure and the need to counter increasingly sophisticated threats.

Businesses with cyber security budget by industry
(As a share of respondents in each industry)



Across all major sector groupings,

over 70%

of businesses have a cybersecurity budget.

[3] Production sector includes manufacturing, utilities and waste management

[4] Non-consumer services encompass a wide range of activities and industries that provide services to businesses, organisations, or governments, rather than to individual consumers. These include sectors like industrial services, commercial services, distribution services, technology services, health services, and retail trade, among others. Essentially, non-consumer services cater to the needs of other businesses or entities, rather than directly to individuals.

The findings highlight that UK businesses are taking cybersecurity seriously, with increasing investments, strategic in-house capabilities, and adherence to government-backed and international standards. However, industry-specific differences underscore varying levels of preparedness and investment. The UK government's emphasis on cybersecurity resilience, tighter regulations and the growing adoption of AI-driven solutions will continue to influence how businesses shape their cybersecurity strategies in the coming years.

While in-house cybersecurity teams remain a popular choice, the complexity and rapid evolution of cyber threats demand a more specialised approach. Outsourcing cybersecurity to a trusted provider like ESET not only ensures businesses can stay ahead of emerging threats and achieve compliance with evolving regulations, but can offer sector specific expertise that enables companies to manage their unique threat landscape to a much more sophisticated level.

Prevalence of cyber attacks

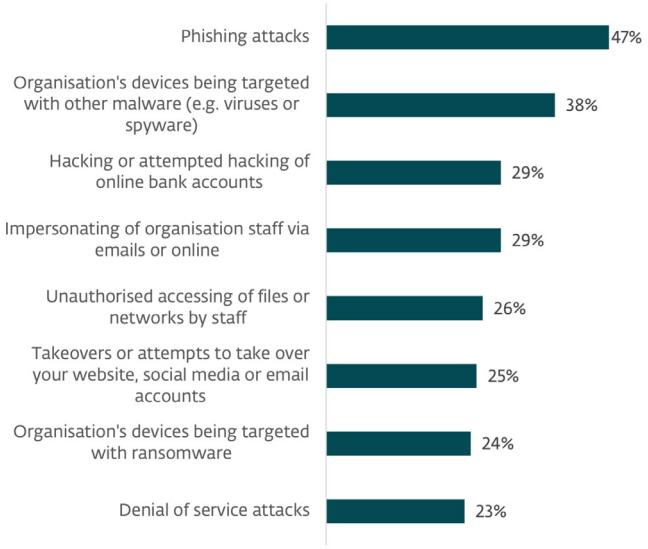
Fuelled by the rise of AI, the growing threat of attack methods like ransomware, phishing and supply chain attacks continues to impact businesses of all sizes, alongside increased exposure to international threats and the rise of Cybercrime-as-a-Service (CaaS). In the past three years, 53% of respondents reported that their organisation experienced a cyber attack or breach at least once. Of these, 26% experienced it once, 16% twice and 12% at least three times. Larger businesses were more likely to experience cyber attacks, with 63% reporting at least one attack in the past three years compared to only 25% of small businesses. While larger, more well-known businesses that have access to more funds and sensitive information are undoubtedly a greater target for attackers, these findings could also reflect larger businesses choosing to manage more of their cybersecurity operations in-house rather than working more closely with external partners with the right expertise.

The top three most common cyber attacks or breaches were phishing attacks (e.g. staff recognising fraudulent emails) (47%), organisation devices being targeted with malware (e.g. viruses or spyware) (38%) and hacking or attempted hacking of online bank accounts (29%). These attack vectors highlight the need for continuous monitoring, advanced threat detection, and employee cybersecurity awareness.

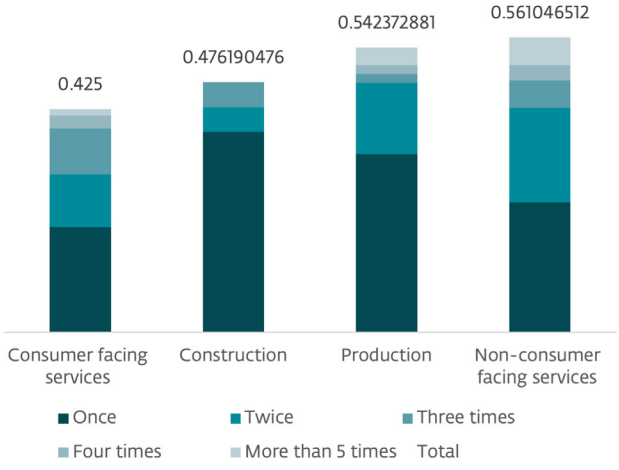
When asked about expectations for future cyber attacks, 43% of respondents believed their organisation would likely experience a cyber attack or breach in the next 12 months. Larger businesses (51%) were more likely to expect cyber attacks than smaller businesses (39%).

Across the main sector groupings, non-consumer services had the highest share of respondents experiencing cyber attacks (54%). Within this category, the information and communication sector had the highest share, with 69% of respondents reporting at least one attack in the past three years.

Types of cyber attacks experienced in the past three years
(As a share of those experiencing a cyber-attack or cyber breach)



Businesses experiencing a cyber-attack/breach in the past three years
(As a share of all respondents)



Cost of cyber attacks

Cyber attacks continue to impose a significant financial burden on UK businesses, with total costs amounting to £64 billion annually. Despite this staggering figure, many businesses remain underprepared to mitigate these risks, reinforcing the need for expert-managed cybersecurity services.

On average, direct costs account for 0.7% of business turnover across the UK, while indirect costs represent 0.5% of turnover – or in monetary terms £37.3 billion 13.1 billion in GVA terms) and £26.7 billion (£9.0 billion in GVA terms) respectively. These figures highlight the need for businesses to invest in robust cybersecurity solutions proactively rather than being forced to deal with costly repercussions after an attack has happened.

total costs amounting to

£64 billion annually

the most frequently cited

direct cost

was staff time spent dealing with an attack

→ REGIONAL BREAKDOWN

South England bears the highest cyber attack costs, totalling £35.7 billion, reflecting the region's concentration of high-value industries such as finance and technology. This cost is split into £20.2 billion in direct costs and £15.5 billion in indirect costs. Meanwhile, the Midlands experiences the lowest total cost, amounting to £7.2 billion annually, with £4.6 billion in direct costs and £2.6 billion in indirect costs. But no region is immune to threats.

→ DIRECT COSTS

The direct costs of cyber attacks include ransom payments, stolen/lost funds, legal and regulatory costs, direct costs of disruption to operations, staff time spent dealing with the attack, costs of third-party expertise, and higher cyber insurance premiums. Among these, the most frequently cited direct cost was staff time spent dealing with an attack, with 63% of respondents identifying this as a major factor. The smaller the business, the more significant staff time spent appears to be, with 74% of small businesses reporting it as a significant issue compared to 60% of large enterprises.

Notably, disruptions to operations (26%) and increased cyber insurance premiums (25%) were the most commonly cited as extremely significant costs. The cost of third-party expertise was identified as significant by 57% of businesses with fully in-house cybersecurity operations and 57% of those with hybrid cybersecurity management.

Interestingly, despite 24% of respondents being targeted by ransomware, ransom payments and lost funds were the least frequently considered significant costs in proportion to the overall direct costs of cyber attacks.

Matt Knell says,

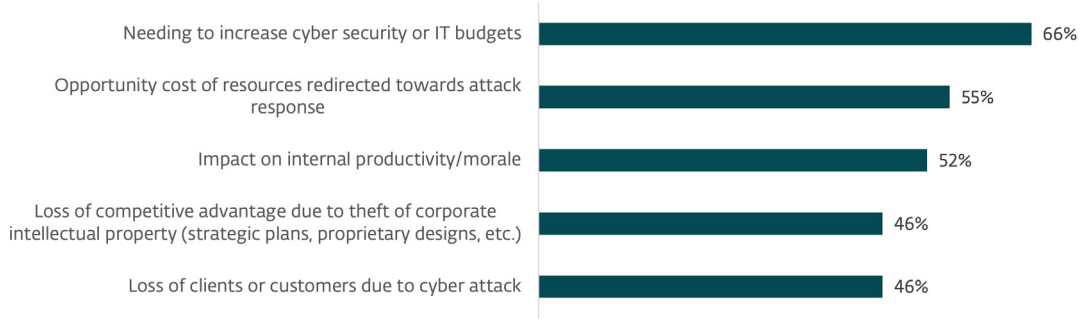
> **"We've seen firsthand how strong cybersecurity measures and a trusted security partner can reduce a business's direct costs. Cyber insurance premiums are skyrocketing, posing a major financial challenge, but they're a necessary investment in today's threat landscape. ESET recently worked with a UK-based mid-sized law firm that was initially quoted £60,000 for its annual cyber insurance. After our consultants reviewed the insurer's requirements, which included an XDR platform, multi-factor authentication, and vulnerability scanning, we helped the firm implement the necessary measures. As a result, their insurer reduced the premium by 75% to £15,000, allowing them to achieve a higher level of protection at a fraction of the cost."**

→ INDIRECT COSTS

Indirect costs include loss of clients or customers, opportunity cost of resources redirected towards attack response, loss of competitive advantage due to theft of corporate intellectual property (strategic plans, proprietary designs, etc.), impact on internal productivity/morale and subsequent need to increase cybersecurity or I budgets. The most significant indirect cost was the need to increase cybersecurity budgets, with two-thirds (66%) of respondents identifying it as a major financial burden and over a quarter (28%) identifying it as extremely significant.

Interestingly, the loss of customers or competitive edge was perceived as less significant. However, businesses should not underestimate the reputational damage of a cyber attack – particularly given the increasing public scrutiny on data protection and cybersecurity preparedness.

Significance of share of indirect cost of cyber attacks
(Share of respondents that identified the following as significant)



Average cost of cyber attacks for firms

SMEs

Production
£48,306

Financial & Insurance Activities
£721,454

Information & Communication
£83,812

Public sector
£2,868

Professional, Scientific & Technical Activities
£14,118

LARGE BUSINESSES

Financial & Insurance Activities
£64.3 million

Information and Communication
£12.8 million

Public sector
£3.4 million

*Business sizes were defined as: Large businesses = more than 250 employees | Medium businesses = 50-249 employees | Small businesses = 1-49 employees

➔ FINANCIAL PREPAREDNESS

Encouragingly, the vast majority (93%) of surveyed businesses confirmed they had sufficient cash reserves or access to finance to cover the associated costs of a cyber attack. However, while most industries demonstrated high levels of financial resilience, consumer-facing services and production had the lowest proportion of financially prepared firms (88%). In contrast, the financial and insurance sector was the most prepared (98%), followed by information and communication firms (92%).

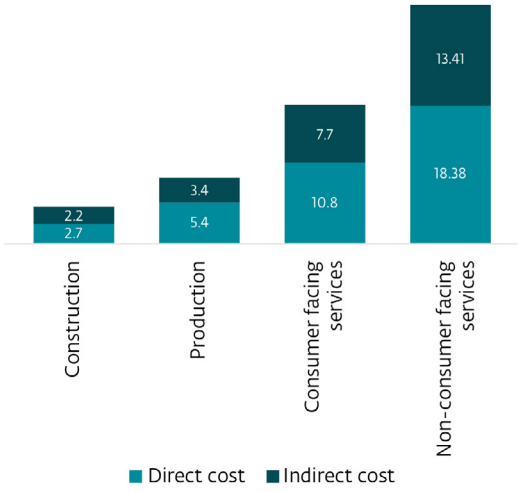
> While most businesses (93%) have sufficient cash reserves or access to finance to cover the costs of an attack, they should not underestimate the potential reputational damage that can be avoided with the right protection.

➔ FINANCIAL IMPLICATIONS

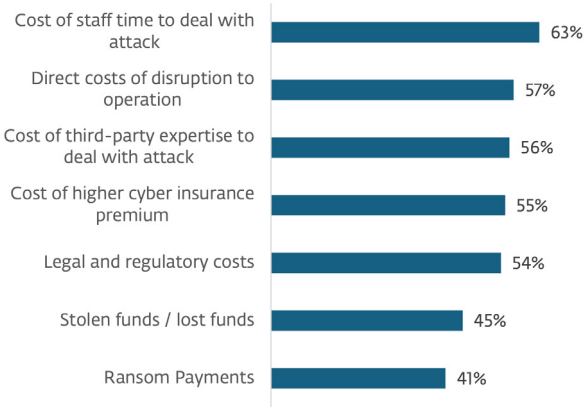
Beyond immediate costs, cyber attacks can have long-term financial consequences for businesses. The most commonly reported financial implication for those who experienced an attack was restricted business growth (43%), followed by the need to secure additional finance or funding (41%). Less frequently reported but still significant consequences included downsizing (14%), entering administration (15%) and undergoing mergers or acquisitions (16%).

For SMEs, growth restrictions were particularly pronounced (45%), while large enterprises were more likely to require additional financing (46%) to recover from attacks. Among businesses that identified the subsequent need to increase cybersecurity/IT budgets as a significant share of the cost of cyber attacks, nearly half (49%) required additional funding, slightly higher than the overall average of 41%. This indicates that the financial burden of strengthening cybersecurity post-attack is a major challenge for many businesses, underscoring the substantial financial burden of reactive cybersecurity measures. Meanwhile, businesses with a hybrid approach to cybersecurity management found raising finance or funding to be a lesser concern (35%) than those with fully in-house cybersecurity management, where this issue was more prevalent (46%). It's clear then that proactively outsourcing cybersecurity can help businesses avoid such financial strain by providing scalable, cost-effective protection.

Annual cost of cyber attacks in GBP millions - by main sector groupings



Significance of share of direct cost of cyber attacks (As a of respondents that experienced cyber attacks)

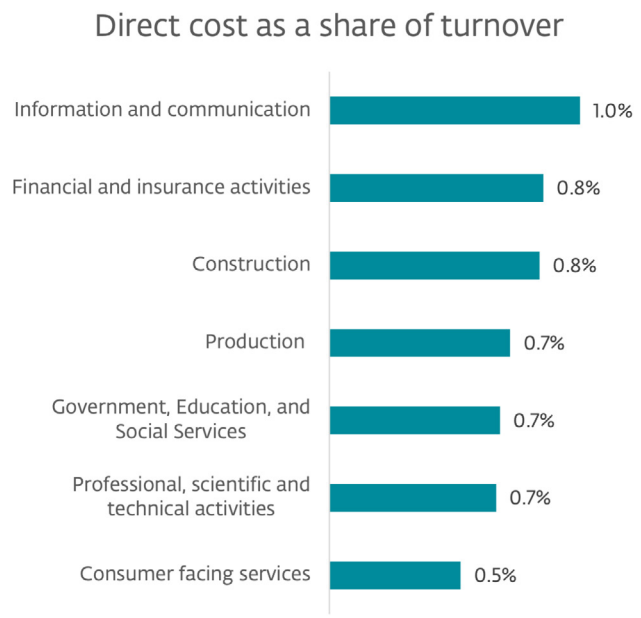


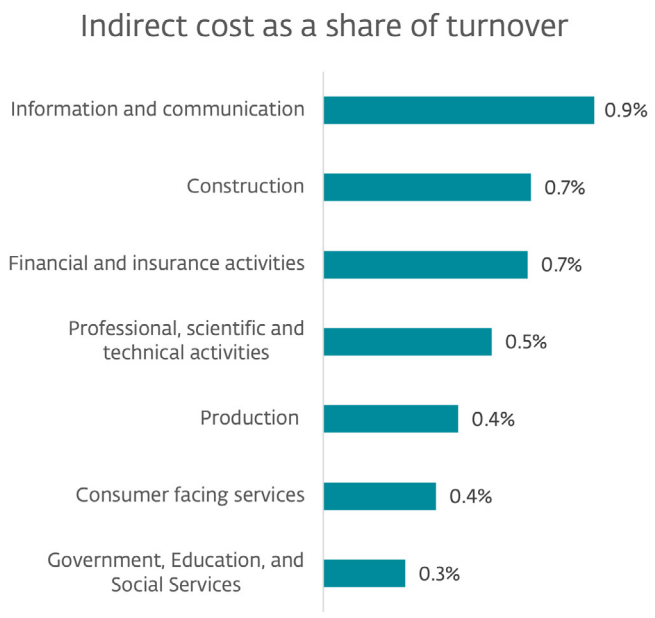
→INDUSTRY BREAKDOWN

Non-consumer services bore the highest financial impact by absolute cost, incurring £31.8 billion in cyber attack-related expenses annually. Within this category, financial and insurance activities reported the highest costs at £16.5 billion, reflecting the industry's attractiveness to cyber criminals. Consumer-facing services followed, with £18.5 billion in annual losses. The production sector had an annual cost of £8.8 billion, and the construction sector had a cost of £4.9 billion. The average cost of a cyber attack for a production SME organisation is £48,308; meanwhile, for large businesses in the finance sector, businesses report an average cost of £64.3 million and £4.3 million for large public sector organisations.

When considering cyber attack costs as a share of industry turnover, the information and communication sector experienced the highest impact, at 1.0% in direct costs and 0.9% in indirect costs. Given the sector's reliance on digital infrastructure, it remains a prime target for cyber threats. The sector also reported the highest impact on cybersecurity budgets, with three quarters reporting this as a significant share of the indirect costs incurred following a cyber attack. However, its absolute costs at £5.9 billion remain lower than those of consumer-facing and financial services, which have much larger total revenues, though the impact on productivity loss and reduced employee morale was particularly pronounced in financial services, with 59% identifying it as a significant share of indirect costs.

Since direct and indirect costs can be significant, businesses must prioritise comprehensive protection, continuous monitoring, and rapid response capabilities.





MDR costs just

1p per hour

per employee

Jake Moore, Global Cybersecurity Advisor at ESET, says, "For essential employee endpoint protection and MDR, businesses can expect to pay around £94 per employee, per year – that's £2805 annually for a 30-person team, £8080 for 100 employees, and £34,300 for a 500-strong workforce. This equates to 1p per hour, per employee.

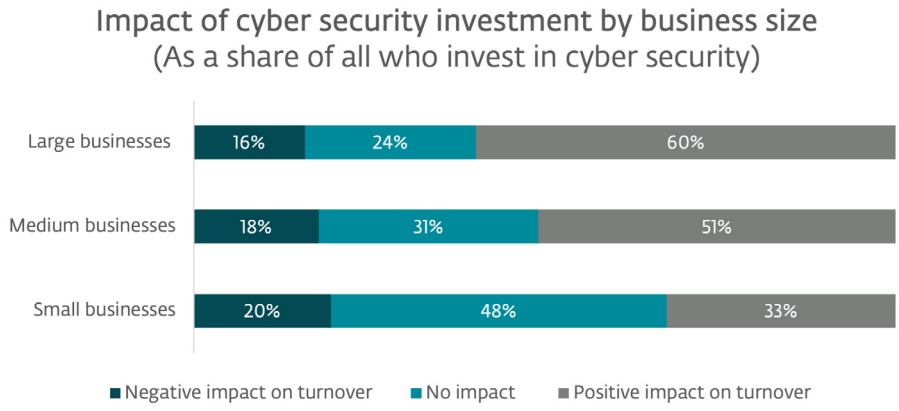
> **"While these costs may appear steep for a business with stretched budgets and multiple priorities to juggle, they pale in comparison to the potential fallout of a cyber attack, which can reach £721,000 for SMEs and run into the millions for large businesses. With the rising cost of cyber threats, no business can afford to overlook cybersecurity. Investing in expert-managed protection can significantly reduce long-term financial and operational risks."**

Impact of cybersecurity on turnover

➔ ECONOMIC BENEFITS OF CYBERSECURITY INVESTMENT

Investment in cybersecurity delivers tangible economic benefits beyond protection, with 53% of surveyed UK businesses reporting a positive impact on turnover. This underscores the importance of cybersecurity as a defensive measure and a strategic enabler of business growth.

While 30% of businesses reported no impact on turnover, only 17% noted a negative effect, highlighting that cybersecurity investments contribute positively to financial performance in most cases. Larger businesses, which often have greater resources to invest in security, were more likely to perceive higher returns. However, nearly one-third (33%) of small businesses also recognised cybersecurity as a growth driver.



*Business sizes were defined as: Large businesses = more than 250 employees | Medium businesses = 50-249 employees | Small businesses = 1-49 employees

On average, cybersecurity investment had a net positive impact of 0.5% on turnover, translating to £27.3 billion across the whole economy (£10. 3 billion in GVA terms). This demonstrates that, far from a cost burden, strategic cybersecurity investments contribute to economic performance.

➔ INDUSTRY BREAKDOWN

The financial and insurance sector saw the highest absolute value of net impact at £6.4 billion. In contrast, the information and communication sector recorded the highest average net impact relative to turnover, at 1.0% (£3.4 billion).

PRIMARY BENEFITS OF CYBERSECURITY INVESTMENT

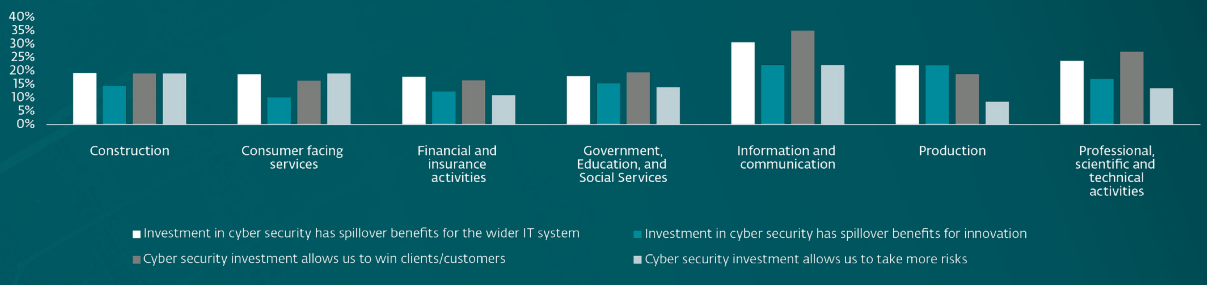
The main ways that cybersecurity investment contributed to business growth included:

- **Winning new clients and customers (70%)** – Businesses with strong cybersecurity credentials are more likely to secure contracts, especially with companies prioritising security in their supply chain.
- **Spillover benefits for IT systems (68%)** – Investments in cybersecurity often lead to improved IT efficiency, better system performance and reduced downtime.
- **Driving innovation (50%)** – Secure digital environments allow businesses to develop and launch new products and services confidently.
- **Enabling risk taking (44%)** – Companies with robust cybersecurity frameworks feel more secure in taking risks, for example expanding operations and adopting new technologies.

For larger enterprises, the spillover effects on wider IT systems (70%) and client acquisition (73%) were the most prominent growth drivers, followed by spillover benefits for innovation (50%) and risk-taking (43%). For SMEs, winning more clients (65%) was broadly as beneficial as spill-over impacts for the wider IT system, reinforcing the argument that businesses of all sizes should prioritise outsourced cybersecurity solutions to maximise return on investment.

The information and communication sector reported the highest positive impact across all categories, particularly in securing new clients (35%) and IT system improvements (31%). In contrast, other industries reported lower but still notable spillover effects. Risk-taking is the least cited benefit across most industries, with the lowest percentage in the production sector (8%), suggesting that while cybersecurity investments drive growth, their impact on business risk appetite varies.

Reasons cyber security investment positively impacts growth beyond protection, by industry
(As a share of total respondents in each industry)

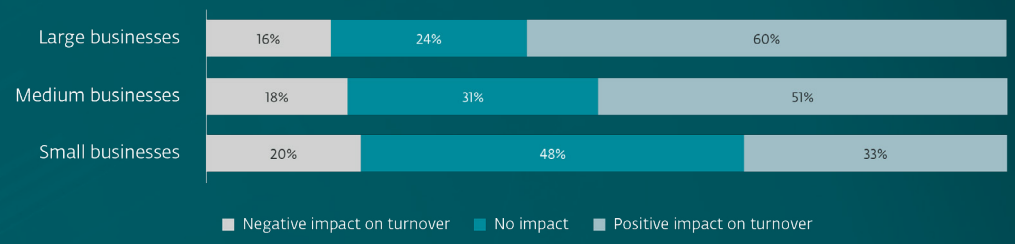


ADDRESSING PERCEIVED NEGATIVE IMPACTS

Among the 17% of businesses that reported a negative impact on turnover, the primary reasons cited included:

- **Cybersecurity investment diverting funds from other business initiatives (62%)** – This suggests that businesses need to integrate cybersecurity into their overall business strategy rather than viewing it as an isolated expense.
- **Making businesses more risk-averse (47%)** – While security is essential, companies should ensure it does not stifle agility and innovation.
- **Operational restrictions due to cybersecurity policies (40%)** – Overly rigid security controls can impact productivity if not implemented effectively.
- **Compliance burdens (38%)** – Businesses struggling with regulatory requirements may benefit from expert-managed security solutions to ease the compliance process.

Impact of cyber security investment by business size
(As a share of who invest in cyber security)



*Business sizes were defined as: Large businesses = more than 250 employees | Medium businesses = 50-249 employees | Small businesses = 1-49 employees

Cybersecurity investment is no longer just about risk mitigation; it is a critical driver of business success. With businesses reporting a net positive financial impact, investing in expert cybersecurity management is a strategic decision that ensures both security and long-term growth.

> **"Businesses that integrate cybersecurity into their growth strategies are not just protecting themselves; they're also enhancing their reputation, winning more clients, and building a more resilient future. By outsourcing cybersecurity to ESET, businesses can maximise efficiency, enhance customer trust, and position themselves for sustained competitive advantage in an increasingly digital economy."**

concludes **Matt Knell.**

Conclusion

The findings of this report make one thing clear: cyber threats are imposing a growing financial burden on UK businesses, with annual costs reaching a staggering £64 billion. While some industries bear higher absolute costs than others, no sector or business size is immune. Beyond direct financial losses, the ripple effects of cyber attacks – ranging from operational disruption to stunted business growth – underscore the urgent need for a more strategic and proactive approach to cybersecurity.

For businesses, cybersecurity should no longer be viewed as just a defensive measure but as a critical investment in resilience and long-term success. The evidence shows that businesses prioritising cybersecurity not only protect themselves from costly breaches but also unlock tangible economic benefits, such as improved client trust, enhanced innovation and a stronger competitive position. However, the cost and complexity of maintaining robust in-house security measures can be overwhelming, making outsourcing to expert-managed cybersecurity providers like ESET a smart, cost-effective solution.

Beyond individual business action, addressing the escalating cyber threat landscape requires collaborative efforts across industries, government bodies, and cybersecurity providers. Policymakers must continue supporting businesses through regulatory guidance, financial incentives, and initiatives encouraging cybersecurity best practices. At the same time, cybersecurity providers must play a crucial role in helping businesses stay ahead of emerging threats, offering scalable solutions tailored to evolving risks.

Jake Moore states,

> **"The cyber threat landscape is evolving rapidly, and businesses cannot face it alone. A coordinated effort between the private sector, government, and cybersecurity experts is essential to securing the UK's digital economy."**

By taking a proactive, partnership-driven approach to cybersecurity, businesses can reduce their financial exposure, enhance resilience and turn cybersecurity into a growth driver rather than a cost burden. The organisations that recognise and act on this today will be the ones best positioned for success in an increasingly digital and threat-prone world.

Methodology

This report is based on the findings of a survey of 504 IT and finance decision-makers across UK businesses. The survey was run by Potentia Insight and was in field 3-8 January 2025. Most findings in this report are based on unweighted results, the exception being the findings that refer to a total UK GVA or turnover impact. The economic impact figures were weighted by business size on a non-interlocked basis, then by industry and region on an interlocked basis, based on official statistics.

Business sizes were defined as: Large businesses = more than 250 employees | Medium businesses = 50-249 employees | Small businesses = 1-49 employees