Grant Thornton

Department for Science, Innovation & Technology

Insuring Resilience

Adoption of Cyber Insurance by UK small and medium sized enterprises

April 2025

Contents

Executive summary

This study explores small and medium sized enterprises' (SMEs) perceptions of cyber insurance, their adoption decisions, its role in risk management, and market gaps requiring potential government intervention. Using a mixed-methods research approach combining literature review, interviews, and a survey, it offers a thorough analysis of key challenges and opportunities.

Key findings

- **Growing threats and financial vulnerabilities:** Many SMEs have minimal cyber security budgets and potentially face severe financial impacts, such as lost revenue and extended recovery times, if they suffer a cyber-attack. This vulnerability is further compounded by interconnected supply chains, where a breach in one SME can affect larger networks.

- **Adoption challenges:** Despite high awareness of cyber insurance (62%), many SMEs struggle with understanding insurance policy details. Complex policy language and a lack of clear, accessible guidance impede adoption. SMEs also often overestimate their ability to self-insure, which can contribute to a disconnect between risk recognition and the implementation of effective safeguards.

- **Insurance coverage and cost:** 59% of SMEs report coverage limits up to £1 million, with a median cost of £11,500 focused on business interruption and crisis management. For more extensive coverage including business interruption insurance, crisis management/PR services, cyber extortion/ransomware coverage, and data breach coverage, the median cost rises to £55,000. Additionally, 65% had to meet specific security requirements, with half of those spending between £5,000 and £25,000 to comply.

- **Market dynamics and emerging innovations:** Innovations such as advanced risk assessments show promise in driving proactive risk management. These innovations are not yet widely integrated, but they signal a potential shift toward more sophisticated, data-driven approaches that could better align with the threat environment.

Recommendations

- **Elevate the role of cyber insurance in SME risk mitigation:** Position cyber insurance as a key component of SME risk management by providing clear, accessible information, targeted training, and simplified policy details, supported by real-life case studies. This approach helps demystify cyber insurance for SMEs, ensuring they recognise its practical benefits as part of a broader risk mitigation strategy rather than viewing it as an optional extra.

- **Accelerate adoption of innovative underwriting practices:** Encourage insurers to pilot advanced analytics and AI-driven risk modelling to shift from reactive to proactive risk management, with coordinated support from regulatory bodies and industry associations. Embracing innovative

underwriting practices could significantly improve risk assessment accuracy, reducing potential losses and aligning the insurance sector with rapidly evolving cyber threats.

- **Develop and promote specialist expertise in cyber insurance:** Integrate specialised cyber knowledge into underwriting and brokerage through standardised communication and comprehensive training delivered by reputable industry associations, such as the Chartered Insurance Institute (CII) and the British Insurance Brokers' Association (BIBA), in collaboration with cyber security experts and academic institutions. This would ensure industry professionals can effectively communicate complex risks and tailor policies to meet the evolving cyber threat landscape, providing SMEs with more reliable and relevant coverage.

1. Introduction

1.1. Background to the research

The Department for Science, Innovation and Technology (DSIT) commissioned this research to better understand the UK cyber insurance market for SMEs. Over the past two decades, digital transformation has reshaped the UK business landscape, intensifying the exposure to cyber threats across all sectors. Cyber insurance has emerged as a strategic tool aimed at mitigating the financial and operational impacts of cyber incidents, particularly for SMEs.

The cyber insurance market is dynamic and fragmented. This is characterised by challenges in risk quantification, policy complexity and accessibility for SMEs. This research will consider whether current market practices adequately support SME resilience in an evolving digital environment and highlight any market failures that could necessitate government intervention, thereby contributing to a more robust and sustainable cyber risk framework for the UK.

1.2. Research objectives

The primary objective of this research is to develop a comprehensive understanding of the UK cyber insurance market, with a particular focus on its effectiveness in addressing SME needs by:

- Examining how SMEs perceive cyber insurance.
- Investigating the rationale behind SMEs' decisions to adopt or forgo cyber insurance, providing insights on the factors that drive cyber security risk management practices.
- Exploring the broader role that cyber insurance plays in the risk management decision-making process among SMEs.
- Identifying market gaps and potential failures that may require targeted government intervention.

1.3. Overview of methodology

To achieve the objectives of this study, a mixed-methods approach was employed, combining both quantitative and qualitative research methods to provide a comprehensive understanding of the market dynamics and SMEs' perspectives. This included a systematic literature review, qualitative interviews, and a quantitative survey.

Literature Review

- A comprehensive systematic literature review was conducted to examine existing research and publications on cyber insurance and UK SMEs. The review aimed to identify key themes, trends, and gaps in the current understanding of SME engagement with cyber insurance.

The methodology for the literature review involved a combination of:

- Targeted searches using research databases and academic repositories, applying relevant keywords related to cyber insurance, SMEs, risk management, and insurance adoption barriers.

- Review of industry reports, including publications from trade bodies, insurance companies, and government sources.

- Existing knowledge and additional open-source searches to ensure relevant and recent materials were included.

Approximately 30 papers and reports were reviewed, ensuring a broad yet focused analysis of the topic. The selection process prioritised peer-reviewed academic studies, government publications, and industry white papers published post-2019.

Quantitative Survey

A quantitative survey was designed to explore SMEs' awareness, experiences, risk management decision processes, and use of cyber insurance as a risk transfer mechanism. Key aspects covered in the survey included:

- Understanding of the cyber insurance market
- How cyber insurance is procured and used
- Types and financial range of coverage purchased
- Security controls deployed to qualify for insurance
- Costs associated with cyber insurance
- Support provided by the insurance industry

The survey was sent to 9,000 SMEs, curated from a CRM database of businesses held by Grant Thornton (GT), and was conducted over a six-week period in February and March 2025. A total of 104 SMEs responded, providing both structured responses and free-text feedback to capture nuanced perspectives. Respondents were also given the option to volunteer for follow-up interviews, allowing for more detailed case studies on the cyber insurance buying process. Further details on the survey methodology can be found in Appendix B.

Qualitative Interviews

To complement the survey data, semi-structured qualitative interviews were conducted with key stakeholders, including:

- Six representatives from cyber insurers and brokers to gain insights into the practical application and challenges of cyber insurance.

- Two SME owners to understand first-hand experiences with cyber insurance decision-making.

The interviews took place in late January and throughout February 2025, arranged via introductions from DSIT and GT industry contacts. Interviewees were selected from those who volunteered after completing the survey. All interviews were conducted remotely and lasted approximately one hour. A topic guide outlining the key discussion areas can be found in Appendix C.

1.4. Limitations

- **Short Research Timeframe:** The study was conducted over a relatively brief period, which constrained both the data collection process and the depth of analysis. A longer study duration might have allowed for a more extensive survey distribution, follow-ups with non-respondents, and deeper qualitative insights. As a result, the findings offer a snapshot of the current landscape rather than a comprehensive perspective.

- **Small Sample Size:** Despite efforts to reach a broad audience by distributing the survey to 9,000 UK SMEs, the response rate was low, with only 104 completed surveys. This limited sample size reduces the statistical power of the study and may not fully represent the diverse experiences of SMEs across different sectors and sizes. While the results provide an indication of trends and concerns within the SME community, they should not be interpreted as universally applicable.

- **Survey Design:** The inclusion of numerous in-depth questions, while valuable for obtaining detailed insights, may have inadvertently reduced the overall response rate. Some SMEs may have found the survey too time-consuming or complex, leading to non-completion. A more concise or tiered survey approach, incorporating optional follow-ups, might have increased participation and improved the richness of responses.

Given these constraints, it is important to interpret the findings and insights as an indication of prevailing attitudes and barriers rather than definitive conclusions applicable to all UK SMEs. Further research could help validate and expand upon these findings. Additionally, studies conducted over a longer period with a higher response rate would be beneficial in ensuring more robust conclusions about SME engagement with cyber insurance.

1.5. Acknowledgements and feedback

DSIT and the report authors would like to thank those that participated in the survey research, including those SMEs and insurance firms who volunteered their time to provide valuable insights to enrich our analysis.

2. The UK SME threat landscape

Summary

- The UK cyber threat landscape is evolving rapidly, with attacks on SMEs increasing in both scale and sophistication.
- SMEs frequently serve as entry points into larger networks and supply chains, a single breach can have cascading effects on critical, high-value targets.
- Severe financial repercussions from breaches have led to cyber insurance emerging as a potential risk management tool to help mitigate these impacts.

The UK cyber threat landscape is evolving rapidly. Attackers are leveraging increasingly sophisticated techniques to exploit vulnerabilities. What was once the domain of highly skilled hackers is now bolstered by underground marketplaces - a thriving ecosystem where cybercriminals buy and sell hacking tools, stolen data, and exploit kits, making cyberattacks more accessible to a broader range of threat actors.

In these marketplaces there are commoditised services available, such as Ransomware-as-a-Service. This provides less experienced actors the capability to launch impactful attacks, effectively lowering the barrier to entry and intensifying overall risk. Small and medium-sized enterprises (SMEs) are particularly susceptible to these threats. With constrained budgets, many SMEs allocate minimal resources to cyber security, leaving them exposed to a fast-changing threat environment.

Cyber Threat Landscape

The cyber threat landscape refers to the ever-evolving environment of cybersecurity risks, including emerging threats, vulnerabilities, and attack methods that organisations and individuals may face. It encompasses the range of potential cyberattacks, threat actors, and tactics used to exploit digital systems and data.

The UK Government's Cyber Security Breaches Survey (2024) shows that many SMEs dedicate less than 5% of their IT budgets to security, even as they face increasing cyber incidents. In addition, research from Hiscox (2021) indicates that many SMEs lack dedicated cyber security teams and instead rely on ad-hoc solutions, further heightening their vulnerability.

SMEs are attractive targets not only because of their own vulnerabilities but also because they often serve as entry points into larger, more critical networks, especially within supply chains. A breach in an SME can provide access to interconnected systems, potentially compromising high-value targets and amplifying the impact of a single incident (Kapani, 2024).

The financial implications can be severe. Hidden costs such as lost revenue and reputational damage frequently exceed the immediate expenses of a breach (IBM, 2024). For SMEs, prolonged recovery periods can result in lasting competitive disadvantages, further challenging their survival in an increasingly competitive market.

It is important to recognise that up to 98% of cyberattacks can be prevented with basic cyber hygiene (Microsoft, 2022). Cyber hygiene involves everyday practices such as keeping software up to date, using strong, unique passwords, regularly backing up data, and installing reliable security tools. These simple steps form a robust first line of defence, significantly reducing vulnerabilities and the likelihood of a breach.

Ransomware as a Service (RaaS)

A criminal business model where threat actors sell or lease ransomware tools to affiliates, who then carry out attacks.

In exchange, the RaaS operators take a cut of the ransom payments, making it a highly profitable and scalable form of cyber extortion.

The RaaS kits are typically promoted and sold on the dark web using the same marketing and sales tactics that legitimate businesses use.

Given the current challenges, cyber insurance is emerging as a potential risk management tool. It offers financial support in the event of a breach, thereby mitigating the impact of cyberattacks and enhancing overall resilience. As MacColl, Nurse and Sullivan (2021) state, “cyber insurance policies aim to provide financial protection when all other cyber security measures have failed,” highlighting its function as a safety net for residual risks. Although it is not a universal remedy, cyber insurance remains a valuable component in the suite of strategies available to SMEs facing an evolving threat landscape.

Learning from the frontlines: Case studies of cyber incidents

Ransomware attack on a UK Retail SME

In 2021, an independent London-based retailer suffered a ransomware attack that resulted in the encryption of all sales and customer data records. The attackers demanded a ransom of £50,000. Due to an absence of adequate backup protocols, the business faced considerable downtime and ultimately remitted a partial ransom payment to regain access to critical systems. The incident led to a 20% decline in revenue over three months and a substantial loss of consumer confidence (Smith et al., 2022).

Phishing attack on a legal firm

In 2022, a Manchester-based legal practice was subjected to a phishing attack where an employee inadvertently provided login credentials in response to a fraudulent email. The attackers subsequently accessed confidential client files, resulting in potential legal and regulatory ramifications under the UK's General Data Protection Regulation (UK GDPR). The firm incurred fines imposed by the Information Commissioners Office (ICO) alongside additional legal expenses, reinforcing the necessity of comprehensive cyber security training (Johnson & White, 2021).

Ransomware attack on a UK Retail SME

A Midlands-based manufacturing SME experienced significant disruptions following a cyberattack that targeted its third-party software supplier. The attackers inserted malware into an update, affecting the SME's inventory management system. This led to production and delivery delays, resulting in contractual penalties from corporate clients. The incident underscored the importance of stringent third-party risk management practices (Brown & Patel, 2020).

3. Challenges to Cyber Insurance Adoption

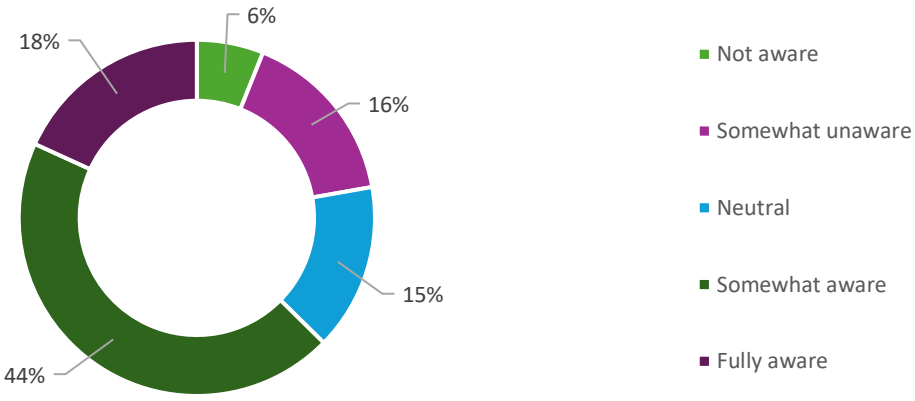
Summary

- Many SMEs underestimate the severity of cyber threats and dismiss cyber insurance as non-essential, largely due to a limited understanding of their actual risk exposure and the overly technical, opaque information available.
- Cost remains a critical barrier, with smaller enterprises finding current premium structures prohibitive given their constrained security budgets. This underscores the need for adaptable, scalable pricing models.
- Broker advice and the imperative for operational resilience drive adoption, especially when paired with clear, accessible communication that demystifies cyber risk and highlights the strategic benefits of comprehensive coverage.

3.1 Lack of awareness and perceived necessity

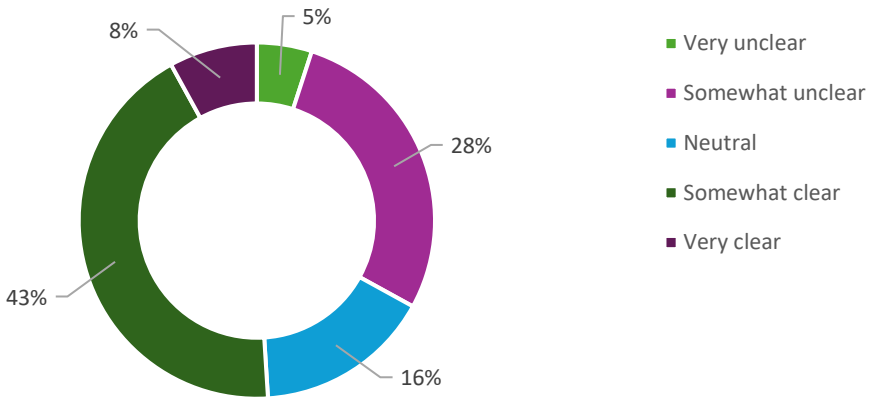
Our survey of 104 SMEs showed 62% of respondents (Figure 1) have an awareness of the different types of insurance policies available to them, yet there is a significant gap when it comes to truly understanding these products.

Figure 1: Survey question - How aware are you of the types of insurance policies available for SMEs?



Only 8% of respondents (Figure 2) felt that the information provided by insurers or brokers was “very clear”, suggesting that despite high awareness, many SMEs remain confused about the specifics of their coverage and what options are available to them.

Figure 2: Survey question - How clear is the information provided by insurers/brokers on cyber insurance?



3.2 Vulnerability and insurance uptake

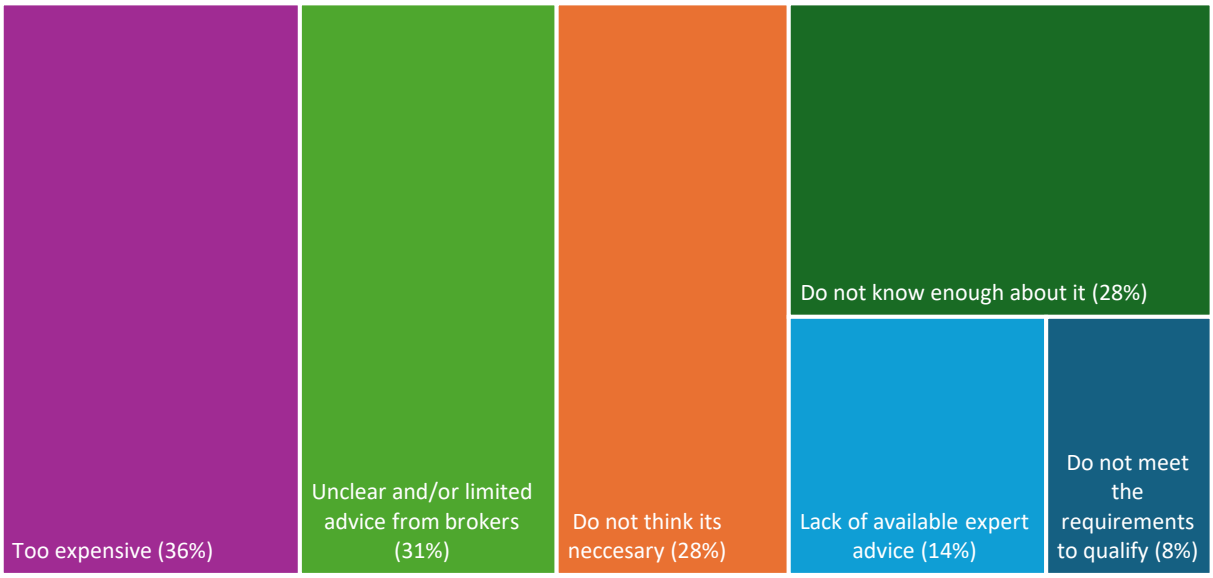
Survey results indicate that 69% of all respondents perceive their businesses as facing a moderate to high risk from cyber threats. This concern is reflected in their actions, as 65% of the 104 SMEs (n=68) surveyed have opted for cyber insurance, while 35% remain uninsured.

However, there is a gap in awareness. While 62% of all respondents were aware of the different types of cyber insurance available (Figure 1), data suggests 24% of SMEs who purchased an insurance policy may have done so without being aware of all their options. This indicates that certain businesses may have acquired coverage without a clear grasp of the available alternatives.

Of the 104 SMEs surveyed, the 35% (n=36) who did not purchase cyber insurance were asked to select all the factors they believed contributed to their decision (Figure 3). The results revealed that 28% do not think cyber insurance is necessary, while 31% are deterred by unclear or limited advice from brokers, and another 36% cite cost as a prohibitive factor.

Additionally, 28% stated they did not know enough about cyber insurance to form an opinion. Separately, over half (58%) of uninsured SMEs expressed concern about the potential impact of a cyber incident on their business, highlighting a misalignment between perceived risk and the decision not to insure.

Figure 3: Why has your company not purchased cyber insurance?



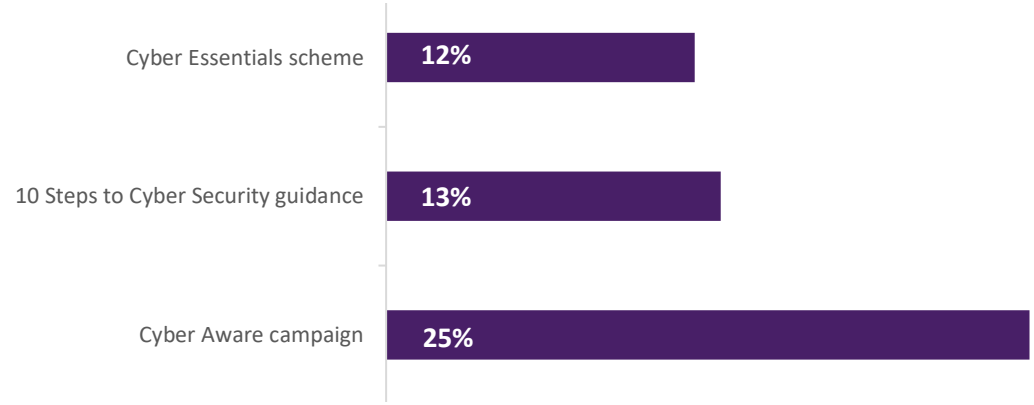
When asked about risk management, 47% of respondents who do not have cyber insurance choose to “self-insure”. This means they rely on their own financial reserves to cover losses from a cyber breach instead of purchasing an external insurance policy. This approach can seem practical, especially when budgets are tight, but it carries the risk that a major attack could result in costs far beyond what the business can afford.

In contrast, 47% of respondents who do not have cyber insurance noted that they have no formal approach to cyber risk management. Risk management involves proactively identifying potential cyber threats, implementing robust security measures, and developing clear response plans. The first stage in this process is identifying what is most critical to the organisation's operations and going concern, ensuring that efforts are focused on protecting key assets. This structured method minimises the likelihood of an attack but also provides resilience should an incident occur.

A key factor contributing to this lack of formal risk management may be limited awareness of available cyber security guidance. Findings from the UK Cyber Security Breaches Survey (2024) indicate that many organisations remain unaware of government initiatives, such as the Cyber Aware campaign and the Cyber Essentials scheme which are designed to help businesses improve their cyber resilience (Figure 4).

Without knowledge of these resources, or other available resources, organisations may struggle to implement effective risk management practices, leaving them more vulnerable to cyber threats. Raising awareness and encouraging adoption of such frameworks could help bridge this gap, ensuring businesses are better equipped to mitigate risks and respond to cyber incidents.

Figure 4: Percentage of organisations aware of the following government guidance, initiatives, or communication campaigns



Source: Cyber Security Breaches Survey 2024

Survey comments from SMEs who did not have cyber insurance suggest that many would like more case studies or real-world examples showing how cyber insurance 'pays off in practice'. Some called for an industry led "central publication of loss ratios" (the cost of cyber losses versus premiums paid), hoping to see clearer value for money. Others cited the need for "a consistent approach from insurers highlighting the benefits versus costs" and "clearer guidelines" on what policies cover and what the requirements entail.

Of those SMEs who do carry cyber insurance (n=68), 76% of respondents stated they received their insurance advice through a broker (Figure 5). The main reasons for obtaining coverage include protecting against potential financial losses (71%) and ensuring business continuity or peace of mind (62%), with board-level directives and broker recommendations also influencing decisions (Figure 6).

Figure 5: Survey question - Where did you receive your cyber insurance advice?

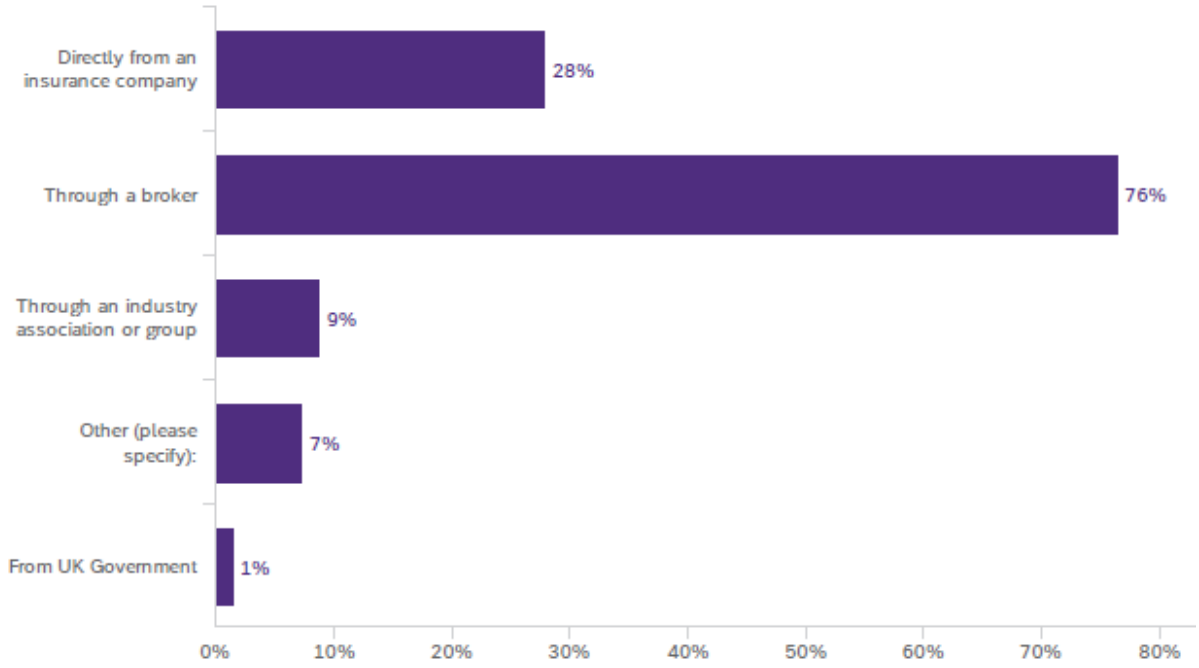


Figure 6: Survey question - Why did you choose to purchase cyber insurance?

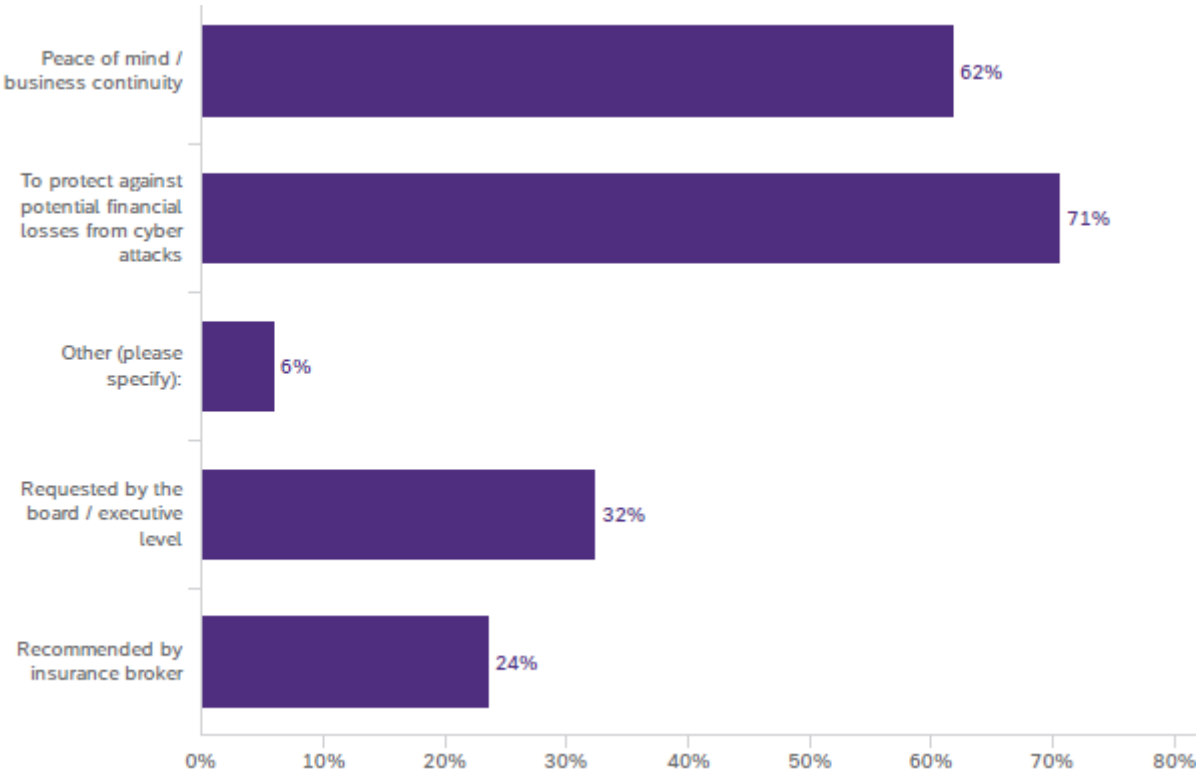
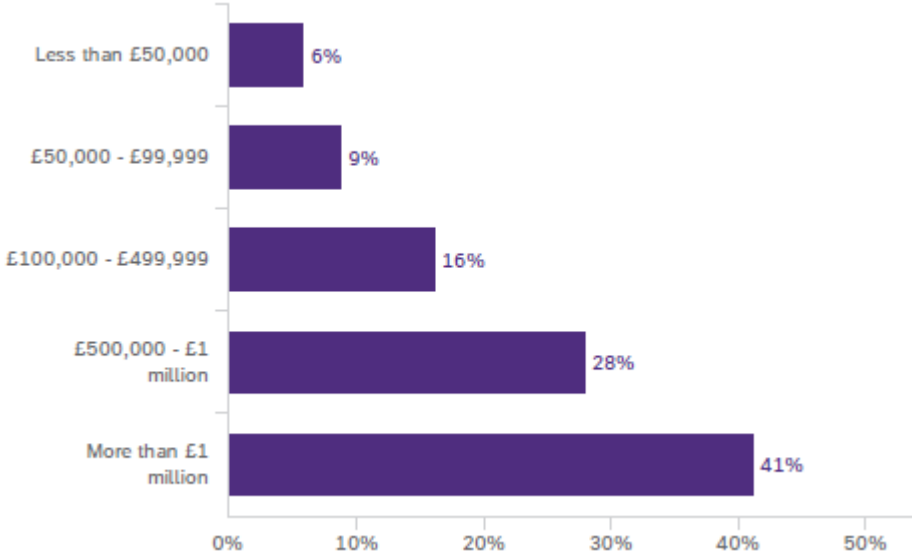


Figure 7 shows that 59% of our respondents from insured SMEs (n=68) opt for coverage amounts of up to £1 million, primarily focusing on business interruption and crisis management. These policies come with a median cost of £11,500, indicating that many SMEs see these risks as central to their operations but prefer to keep coverage limits relatively modest.

It is unclear if there is a sliding scale, but businesses seeking coverage above £1 million, which often includes business interruption insurance, crisis management/PR services, cyber extortion/ransomware coverage, and data breach coverage, face a higher median cost of £55,000. This increase in cost highlights the added expense of more extensive protection and higher liability limits.

Interestingly, when SMEs specifically target cyber risks and legal issues, such as cyber extortion, ransomware, data breaches, and regulatory fines, the median cost is £26,000. The data suggests a tiered approach to cyber insurance where SMEs have the option of either a basic, cost-effective coverage or invest in more robust, specialised policies depending on their respective risk profiles and finances.

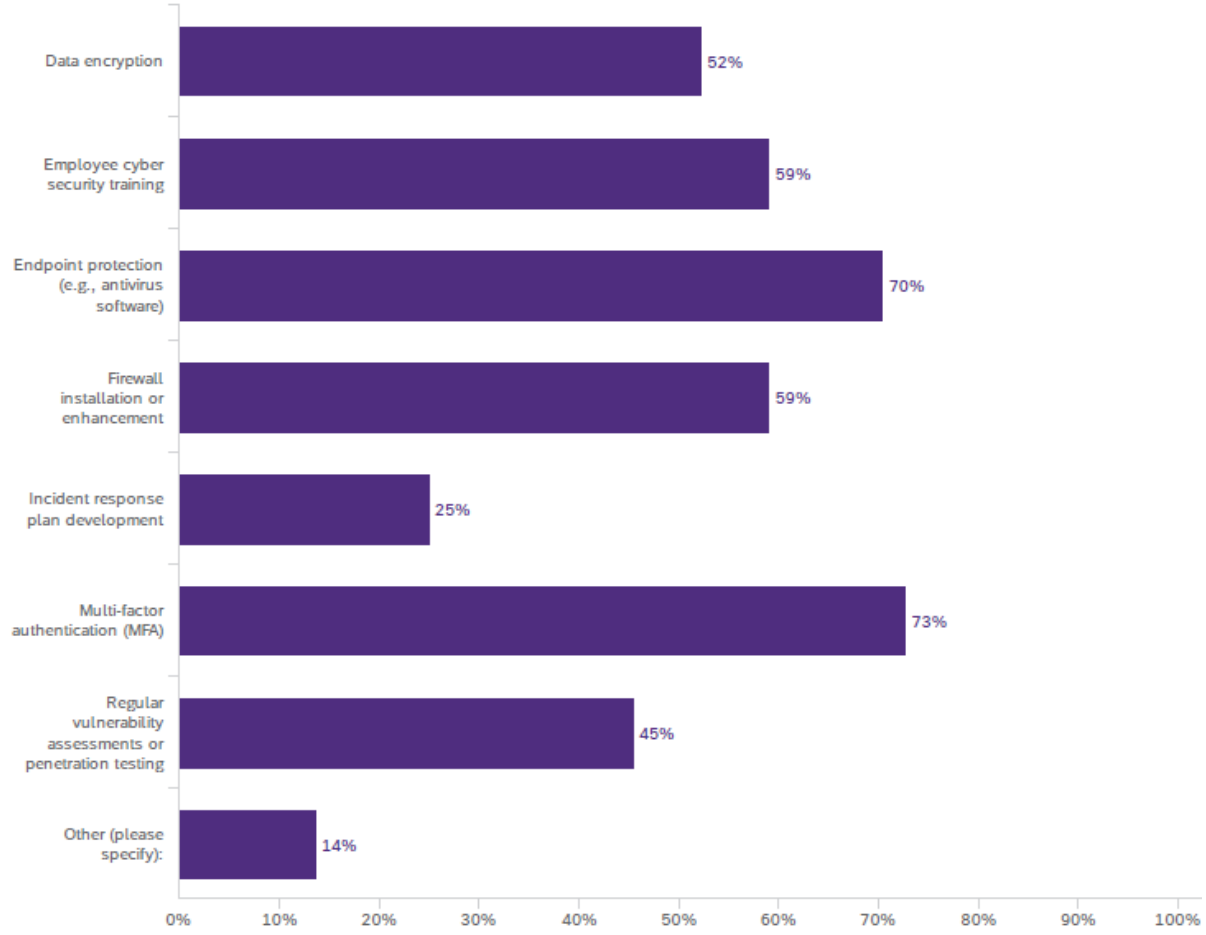
Figure 7: Survey question - What is the total coverage amount of your cyber insurance policy?



However, securing this coverage is not without challenges as 65% reported that their companies had to meet specific security requirements to qualify. While this can be demanding, it also contributes to building resilience by ensuring that SMEs enhance their security posture to meet these necessary standards.

Our survey showed 50% spent between £5,000 and £25,000 to meet the criteria. Respondents noted difficulties in “assessing whether outsourced IT meet technical requirements” and asked for “better education for boards on best practices.”

Figure 8: Survey question - What cyber security measures did your company implement to meet insurance requirements?



Looking at the broader picture, when SMEs factor in all cyber security expenses (including insurance and staff salaries), 30% spend less than £10,000 annually, and another 15% fall within the £10,000-£24,999 range. Just over half (51%) reported that these investments in cyber security have positively impacted their overall business.

3.3 The challenges faced

When asked to rank the limitations or challenges encountered with cyber insurance, 29% of all survey respondents highlighted the difficulty in meeting cyber security requirements as a major limitation: according to SMEs a further 21% cited high premiums and 14% pointed to the complexity of navigating policy documents. Half (48%) of respondents say their insurance provider offered any assistance in meeting these requirements.

Top three key benefits of having cyber insurance.

1. Business continuity during a cyber event (42%)
2. Financial protection against cyber-crime (24%)
3. Access to cyber security experts and resources (22%)

Free-text responses to our survey did provide some further insight on what SMEs require. Respondents frequently called for plain-language explanations of coverage terms and exclusions, regular engagement from insurers or brokers (e.g., webinars, annual training updates), and transparent cost-benefit data, including how specific security measures might reduce premiums.

This lack of clear, accessible information also extended to awareness of existing resources. Others emphasised the importance of board-level education, noting that executive teams often drive the decision to purchase cyber insurance. Some even advocated for government involvement in creating public resources or incentives that could help smaller businesses overcome cost barriers and adopt best practices.

Overall, while SMEs recognise the risks posed by cyber threats and are aware of cyber insurance options, there is a clear need for more cost-effective solutions, transparent information, better advisory support, and to encourage broader adoption and more effective risk management.

4. Qualitative industry insights

This section summarises in-depth conversations we had with industry experts, including both brokers and insurers. These interviews were conducted on the condition that all comments remained anonymous.

Summary

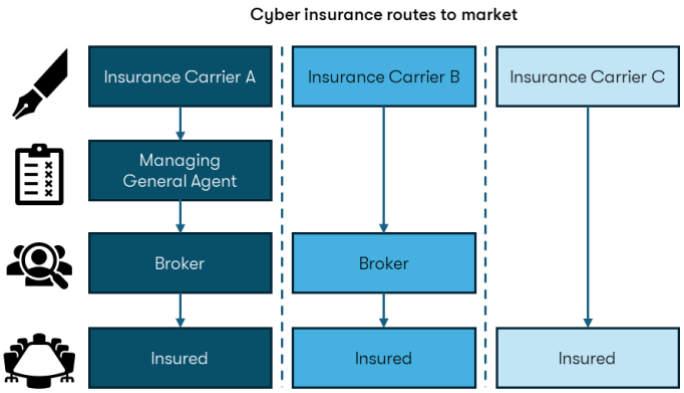
- Cyber insurance has evolved from early risk quantification challenges into a specialised market, spurred by disruptive attack methods, such as ransomware that have reshaped underwriting and risk management.
- Brokers and managing general agents are vital in bridging the gap between legacy underwriting practices based on historical data and a rapidly evolving threat landscape, underscoring the urgent need for specialised expertise and innovation.
- A dynamic regulatory environment is set to recalibrate risk models, while the emergence of comprehensive, bundled coverage is establishing cyber insurance as a cornerstone of integrated, proactive risk management.

Several industry experts commented that during the COVID-19 pandemic, a surge in ransomware attacks underscored the urgent need for innovation in cyber insurance. As attacks increased and remote work widened vulnerabilities, insurers tightened underwriting standards, raised premiums, and enforced stricter policy rules. This turbulent period forced the industry to rethink its risk management practices and paved the way for a stronger, data-driven market.

Cyber insurance is no longer just a financial safety net. It has become a key driver in enhancing cyber security practices. Many insurers now bundle traditional coverage with proactive services such as ongoing scans, tailored incident response plans, and direct access to cyber security experts. However, there was a consensus amongst most interviewees that SMEs do not understand the value of cyber insurance and brokers do not spend enough time explaining those benefits.

Industry experts described the cyber insurance landscape as a balancing act among insurers, managing general agents (MGAs), and brokers. Insurers are beginning to use tools like vulnerability scans to underwrite policies, though it was noted by some experts that there is still some dependence on using historical data, a method that may struggle to keep pace with ever-changing cyber threats.

MGAs act as specialised intermediaries who work closely with insurers to design and distribute tailored cyber insurance products. They are emerging as agile operators, using advanced data analytics to streamline product distribution, especially for SMEs. At the same time, brokers remain essential by translating complex cyber risks into understandable terms for their clients. However, there is debate about whether SMEs are mature enough to fully leverage these innovations.



Some industry stakeholders have raised concerns that clients could be locked in with one insurer for several years, limiting their access to more competitive offerings. While innovation is driving efficiencies in distribution, questions remain about how flexible these arrangements are and whether SMEs have the knowledge and confidence to assess alternative options.

In response, specialised brokers have emerged, offering flexible bundled services that allow SMEs to tailor their coverage without being confined to a single insurer's ecosystem.

Cyber Essentials

The UK government's Cyber Essentials scheme is a certification program designed to help organisations protect themselves against common cyber threats by implementing fundamental cybersecurity measures.

It provides guidance on securing networks, devices, and data, and demonstrates an organisation's commitment to cybersecurity best practices.

At the same time, the growth potential in the cyber insurance market has attracted new insurance generalists. These entrants often focus on price competition, use different terminology for threats, and sometimes bypass detailed technical assessments in search of better deals. Their presence is seen by some/most as diluting the pool of cyber expertise and hinder clear risk communication, which may prevent SMEs from adopting proactive cyber security measures before a breach occurs.

One industry expert commented that SMEs, and their brokers, do not understand and cannot articulate their risks due to a lack of skilled cybersecurity resources. Their perception was that brokers spend more time on trying to drive down the price for an opportunity they have rather than

going out and finding new business. This, in their view, is driving a disconnect between the brokers and the needs of the customers.

It is acknowledged that government initiatives, like the Cyber Essentials (CE) scheme, have established baseline cyber security standards that some insurers consider during underwriting. However, obtaining CE certification or adhering to standards such as ISO27001 does not automatically lower premiums. These benchmarks signal a basic level of insurability, while insurers continue to apply their own criteria to assess individual controls.

It is widely recognised that government-led forums designed to share threat intelligence and non-competitive data hold great promise for improving cyber security across the industry. In principle, these forums, such as NCSC Industry 100, could foster a collaborative environment where participants benefit from a shared understanding of emerging threats and effective mitigation strategies. A few experts commented that some insurers are reluctant to participate, as they are cautious about disclosing sensitive information, which they view as a competitive asset. The experts also acknowledged the fact that this reluctance limits the free flow of critical data and undermines the potential benefits of such initiatives.

ISO/IEC 27000 series standards

The ISO/IEC 27000 series of standards is a collection of internationally recognised frameworks designed to help organisations manage and protect their information assets.

These standards provide best practices for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS), with ISO/IEC 27001 being the most widely adopted for certification.

5. Horizon scanning

Summary

- Rapidly evolving cyber threats, driven by new tools, artificial intelligence, and quantum computing, are outpacing traditional risk models, necessitating innovative underwriting and risk pricing strategies.
- Emerging risk transfer solutions like parametric insurance and capital market cap bonds offer rapid liquidity and streamlined claims, though their success hinges on improved risk quantification and regulatory acceptance.
- Blockchain technology is being explored to enhance transparency and efficiency in claims processing, complementing these innovative insurance products by providing a secure, automated framework.

5.1 Emerging cyber threats and their impact on insurance

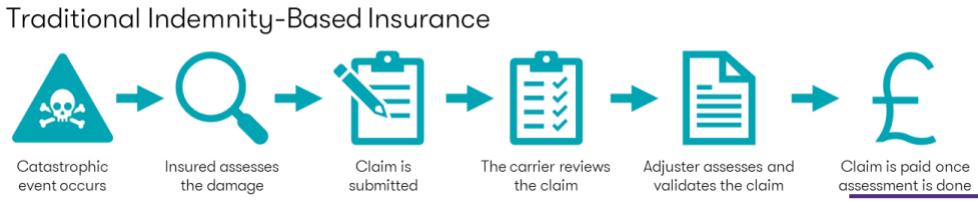
The rapid adoption of new tools, techniques, and procedures by threat actors is outpacing traditional risk assessment models (Europol, 2023). For instance, while conventional models might evaluate risks based on historical data and static threat landscapes, cybercriminals are now using sophisticated methods such as AI-driven phishing, automated ransomware deployment, and real-time dark web monitoring to quickly adapt and launch attacks. These dynamic tactics have rendered many existing models inadequate for predicting emerging risks.

The increasing frequency and sophistication of cyber threats underscore the need for innovative approaches within the insurance industry to refine underwriting and risk assessments. Currently, risk transfer mechanisms such as parametric insurance are being trialled by the wider insurance industry (Munich Re, 2024). While the concept of parametric insurance is not new—having been successfully used in sectors like agriculture, where payouts are triggered by measurable factors such as rainfall — the adaptation of this model to cyber risk is considered innovative.

Parametric insurance operates by automatically triggering payouts when predefined and measurable events occur, providing rapid liquidity and streamlining claims processing. However, its application to cyber risk remains in the early stages of development due to challenges in quantifying cyber threats and setting objective trigger criteria.

A real-world example of parametric insurance in the agricultural sector is the collaboration between NFU Mutual, Skyline Partners, Gallagher, and Markel, which launched the UK's first parametric heat-stress insurance for dairy farmers in May 2023. This innovative product provides predetermined payouts when specific temperature and humidity thresholds are exceeded, offering timely financial support to mitigate losses in milk production and invest in infrastructure improvements to combat heat stress (NFU Mutual, 2023).

Parametric cyber insurance can similarly assist SMEs by accelerating the receipt of funds following a cyber incident. Instead of enduring a lengthy and complex claims process, payouts are automatically triggered when specific, measurable events occur. This enables businesses to access funds rapidly to cover immediate recovery costs, while also benefiting from clear and predictable terms and conditions that simplify planning and risk management (Intangic MGA, 2023).



In addition, blockchain technology is being explored to enhance transparency in claims processing. Unlike parametric insurance, blockchain is a technology platform. It enables secure, immutable record-keeping and the use of smart contracts that can also automatically execute payouts once predetermined conditions are met.

While both approaches facilitate automation in claims processing, parametric insurance focuses on product innovation and risk transfer, whereas blockchain provides the technological infrastructure to support transparency, security, and efficiency in those processes (Deloitte, 2022).

Alternative insurance mechanisms such as capital market cap bonds are also emerging. Often discussed alongside insurance-linked securities and catastrophe bonds, these leverage capital market funding to absorb extreme losses (The Geneva Association, 2024).

In cyber insurance, these bonds can be designed to trigger payouts based on defined events. For example, a breach affecting a predetermined number of records. By transferring portions of risk to investors, these bonds have the potential to diversify the risk pool and provide rapid liquidity after major cyber events.

For SMEs this means that if a major cyber incident occurs, the risk is spread, making it more likely that you'll receive full coverage even in worst-case scenarios. It provides stronger, more reliable protection and peace of mind to SMEs knowing that extreme losses are less likely to leave them underinsured.

Artificial intelligence (AI) will play a key role in strengthening risk modelling and enabling dynamic pricing for cyber insurance. This would lead to a more effective approach to combine multiple data sources to build a complete view of an SME’s cyber resilience (McKinsey, 2024).

6. Conclusion

Our survey found that while cyber insurance holds significant promise as a tool for mitigating financial and operational risks, its current adoption among UK SMEs remains limited by several interrelated challenges. The evidence indicates that many SMEs, constrained by tight budgets and basic cyber security measures, often resort to self-insuring. This approach, although seemingly practical in the short term, exposes them to potentially catastrophic financial impacts when a major incident occurs.

Furthermore, the market itself is fragmented. Insurance industry interviews suggest traditional underwriting models lean heavily on historical data. These policy limitations, combined with complex coverage language, create a disconnect between the intended benefits of cyber insurance and the realities faced by SMEs.

Simplifying policy terms, offering tailored and affordable solutions and boosting industry collaboration are essential for cyber insurance to shift from a reactive safety net to a proactive risk management tool, ultimately strengthening the security and competitiveness of UK SMEs.

The literary review shows how recent industry innovations, including parametric insurance and blockchain-enabled claims processing, point toward a potential shift by promising faster claims handling and improved liquidity for insurers. However, their impact remains modest if challenges like cost barriers, limited advisory support, and unclear policy terms persist.

Insights from the UK Government's Cyber Security Breaches Survey and Cyber Security Longitudinal survey, underline that while SMEs are increasingly aware of cyber risks, they require clearer guidance and more accessible solutions. Government has taken action to address this issue by developing initiatives like Cyber Essentials and the Cyber Governance Code of Practice, to provide industry with clear instructions, to help them elevate baseline organisational security.

7. Recommendations

Recommendation 1: Elevate the role of cyber insurance in SME risk mitigation

Stakeholders could better communicate the role of cyber insurance to ensure SMEs recognise it as a component of their overall risk mitigation strategy rather than an optional extra. To facilitate this shift, targeted training programs and clear, accessible information could be deployed to dispel common misconceptions about risk and self-insurance. Additionally, insurers could work to simplify policy language and clarify coverage details, making it easier for SMEs to understand their options. Leveraging real-life case studies can further demonstrate the tangible benefits of integrated cyber insurance services, thereby strengthening the overall value proposition.

Recommendation 2: Accelerate adoption of innovative underwriting practices

Although some large insurers and emerging technology firms are already investing in advanced analytics and AI-driven risk modelling, widespread adoption across the industry remains in its early stages. Many thought leaders and consultancies argue that traditional underwriting models must evolve to better reflect today's cyber risks.

Insurers could pilot these innovative technologies to transition from reactive to proactive risk management. A coordinated effort, backed by regulatory bodies and industry associations, with transparent reporting on loss ratios and performance metrics, will drive broader investment and accelerate sector-wide innovation. This will not only enhance risk assessment accuracy and reduce potential losses. It also aligns the industry with the rapidly evolving cyber threat landscape, ensuring more effective and forward-looking risk management strategies.

Recommendation 3: Promote specialist expertise in cyber insurance

Foster the integration of specialised cyber expertise throughout the underwriting and distribution process. Insurers and brokers could adopt a common language and business-focused risk communication strategies to avoid technical confusion and effectively articulate risk profiles to SMEs. Comprehensive training for brokers is essential to bridge the knowledge gap, ensuring that they can guide SMEs through the complexities of cyber insurance and help them select policies that are aligned with their evolving risk exposures. This training could be provided by established industry associations, such as the Chartered Insurance Institute (CII) or the British Insurance Brokers' Association (BIBA), in collaboration with specialised cyber security training providers and academic institutions.

Annex A: Understanding cyber insurance for SMEs

Cyber insurance policies vary in scope, but most offerings can be broadly classified into first-party and third-party coverage:

- First-party coverage protects businesses against direct financial losses resulting from cyber incidents, such as business interruption, data recovery, extortion payments, and incident response costs (Marsh, 2022). This type of cover is particularly relevant for SMEs, as they often lack the financial resilience to absorb the costs of a prolonged cyberattack.

- Third-party coverage addresses liabilities arising from cyber incidents affecting external stakeholders. This includes legal costs, regulatory fines, and damages resulting from data breaches affecting customers or supply chain partners. Given SMEs' increasing integration into larger corporate ecosystems, third-party coverage is particularly important, as breaches within smaller firms can have cascading effects across supply chains, amplifying financial and reputational risks (NCSC, 2023).

Bundled insurance and standalone insurance

Bundled cyber security services can help SMEs identify and remediate vulnerabilities before incidents occur. They can even result in lower premiums by promoting robust cyber security practices. However, some SMEs may view these added requirements as an extra burden. For businesses with limited resources, the expectation to immediately address every identified issue can, potentially deter them from fully embracing these enhanced solutions.

ENISA (2021) notes that bundled services not only reduce claim frequency but also drive broader improvements in cyber security hygiene across the market. The convergence of cyber insurance with cyber security services signifies a strategic shift toward preventive risk management, highlighting that effective cyber defence hinges on both minimising incident likelihood and mitigating financial fallout when breaches occur.

Although these services can enhance protection there is debate on whether SMEs are sufficiently mature to fully leverage these innovations. Brown and Patel (2020) argue that clarity and flexibility in these offerings are key to increasing SME uptake, particularly in a market where price competition is intensifying.

Notwithstanding this, the fact these services exist is encouraging and reaffirms how the true value of cyber insurance lies in its capacity to drive continuous improvements in cyber security practices, bridging the gap between risk transfer and risk reduction. Cyber insurance can play an integral part of an integrated, proactive, broader risk management strategy rather than as a standalone remedy.

The role of brokers and managing general agents

The evolution of cyber insurance reflects a rapid adaptation to an increasingly volatile digital threat landscape. Emerging in the early 2000s, cyber insurance initially struggled with quantifying risk due to scarce historical data and the dynamic nature of cyber incidents (Biener, Eling, and Wirfs, 2015). Over time, as empirical methodologies matured, the UK market evolved into a specialised segment with structured policies and defined risk mitigation frameworks (Marsh, 2022).

The cyber insurance ecosystem is shaped by a complex interplay among insurers, managing general agents (MGAs), and brokers. MGAs have emerged as agile intermediaries who leverage advanced data analytics and streamlined underwriting tools to distribute insurer products. Their capacity to aggregate and interpret claim data strengthens their position in SME cyber insurance.

Brokers, meanwhile, remain pivotal in educating clients**.** Their role has traditionally involved translating complex cyber security issues into comprehensible risk profiles. According to recent industry analysis (Insurance Times, 2023), brokers are increasingly seen as essential catalysts in bridging the knowledge gap between technical cyber risk and client understanding.

Market sustainability hinges on integrating specialised cyber expertise into all facets of the distribution chain (Marsh, 2022). Better collaboration between insurers, MGAs, and brokers could lead to more sophisticated risk assessment models, enhanced client education, and ultimately, more resilient underwriting practices. In an industry where rapid cyber threats confront traditional insurance models with limited adaptability, fostering such collaboration is essential for mitigating risk and ensuring market stability.

Government and regulation

Cyber insurance functions within a comprehensive regulatory framework administered by the Financial Conduct Authority (FCA). Organisations are not legally compelled to procure cyber insurance, but the FCA does mandate that insurers adhere to rigorous risk management and capital adequacy standards, often derived from frameworks such as Solvency II, to promote market stability and ensure precise risk pricing.

While cyber insurance is not mandatory in the UK, certain jurisdictions have introduced requirements for specific sectors. For example, in the United States, healthcare organisations covered under the Health Insurance Portability and Accountability Act (HIPAA) are effectively required to maintain cyber insurance as part of their broader risk management obligations. Similarly, in India, the Insurance Regulatory and Development Authority (IRDAI) has encouraged critical infrastructure sectors to adopt cyber insurance.

Annex B: Survey Questions

DSIT - Understanding SME Engagement with Cyber Insurance (2025)

Q1. This survey, on behalf of the UK Government Department of Science, Industry and Technology (DSIT), is designed to gather insights specifically from small and medium-sized enterprises (SMEs) in the UK regarding their interaction with cyber insurance products.

It aims to understand how UK-based SMEs approach cyber insurance and the potential challenges they encounter.

Your responses will play a crucial role in shaping a more tailored and effective approach to addressing the needs of SMEs in this domain.

Individual responses will be used for internal purposes only and will only be shared between Grant Thornton and DSIT. Published data will be anonymous and in aggregated form only. Further details can be found on our respective data privacy page for Grant Thornton.

Thank you in advance for your participation.

Q2. As you have accessed this survey via an online link, the questions below will help us better understand stakeholder demographics. Could you please provide the following information: *This question is not mandatory, but by providing this information you will help us with research analysis. These details will not be shared with DSIT.*

- ○ Your name: _____
- ○ The name of your company: _____
- ○ Your email address: _____
- ○ Your job title: _____

Q3. What is the size of your company?

- ○ 1-9 employees
- ○ 10-49 employees
- ○ 50-249 employees
- ○ 250+ employees

Q4. What industry does your business primarily operate in?

- ○ Administration or real estate
- ○ Agriculture, forestry or fishing
- ○ Construction
- ○ Education
- ○ Entertainment, service or membership organisations
- ○ Finance or insurance
- ○ Food or hospitality
- ○ Health, social care or social work
- ○ Information or communications
- ○ Professional, scientific or technical
- ○ Retail or wholesale (including vehicle sales and repairs)
- ○ Transport or storage
- ○ Utilities or production (including manufacturing)
- ○ Other (please specify): _____

Q5. On a scale from 1 to 5, how aware are you of the types of cyber insurance policies available for SMEs?

Q6. On a scale from 1 to 5, how vulnerable is your business to a cyber-attack?

Q7. On a scale from 1 to 5, how clear is the information provided by insurers/brokers on cyber insurance?

Q8. Does your business currently have cyber insurance?

- ○ Yes
- ○ No

Skip To: Q13 If Q8 = Yes

Q9. Why has your company not purchased cyber insurance? *Select all that apply*

- ☐ Too expensive
- ☐ Lack of available expert advice
- ☐ Unclear and/or limited advice from brokers
- ☐ Do not think it is necessary
- ☐ Do not know enough about it
- ☐ Do not meet the requirements to qualify
- ☐ Other (please specify): _____

Q10. Please rank the following potential incentives for adopting cyber insurance in order of importance to you: *Drag and drop your options to rank, where 1 is 'most important' and 5 is 'least important'.*

_____ Clearer understanding of policy terms
_____ Demonstrated value of coverage
_____ Lower premium costs
_____ Support for meeting cyber security requirements
_____ Other (please specify):

Q11. How concerned are you about the potential impact of a cyber incident on your business?

Q12. How do you currently manage the financial risk of a cyber incident?

- ○ Self-insured (absorb the cost directly)
- ○ No specific risk management approach
- ○ Other (please specify): _____

Display This Question: If Q8 = Yes

Q13. Where did you receive your cyber insurance advice? *Select all that apply*

- ☐ Directly from an insurance company
- ☐ From UK Government
- ☐ Through a broker
- ☐ Through an industry association or group
- ☐ Other (please specify): _____

Display This Question: If Q8 = Yes

Q14. Why did you choose to purchase cyber insurance? *Select all that apply*

- ☐ Peace of mind / business continuity
- ☐ Recommended by insurance broker
- ☐ Requested by the board / executive level
- ☐ To protect against potential financial losses from cyber attacks
- ☐ Other (please specify): _____

Display This Question: If Q8 = Yes

Q15. What types of cyber insurance coverage does your business have? *Select all that apply*

- ☐ Business interruption insurance
- ☐ Crisis management / PR services
- ☐ Cyber extortion / ransomware coverage
- ☐ Data breach coverage
- ☐ Insurance being part of a business insurance package
- ☐ Legal fees and regulatory fines
- ☐ Other (please specify): _____

Display This Question: If Q8 = Yes

Q16. What is the total coverage amount of your cyber insurance policy?

- ○ Less than £50,000
- ○ £50,000 - £99,999
- ○ £100,000 - £499,999
- ○ £500,000 - £1 million
- ○ More than £1 million

Display This Question: If Q8 = Yes

Q17. What is the annual cost of your cyber insurance premium? *Please provide your best estimate and specify currency.*

Display This Question: If Q8 = Yes

Q18. To qualify for your cyber insurance, were there specific cyber security requirements that your company needed to meet?

- ○ Yes
- ○ No

Display This Question: If Q8 = Yes And Q18 = Yes

Q19. What specific cyber security measures did your company implement to meet these requirements? *Select all that apply*

- ☐ Data encryption
- ☐ Employee cyber security training
- ☐ Endpoint protection (e.g., antivirus software)
- ☐ Firewall installation or enhancement
- ☐ Incident response plan development
- ☐ Multi-factor authentication (MFA)
- ☐ Regular vulnerability assessments or penetration testing
- ☐ Other (please specify):

_____

Display This Question: If Q8 = Yes And Q18 = Yes

Q20. How much did your company invest in cyber security measures to meet the requirements for cyber insurance?

- ○ Less than £1,000
- ○ £1,000 - £4,999
- ○ £5,000 - £9,999
- ○ £10,000 - £25,000
- ○ More than £25,000

Q21 What is your company's overall cyber security budget (including the cost of insurance, if applicable, and security staff salaries)?

- ○ Less than £10,000
- ○ £10,000–£24,999
- ○ £25,000–£49,999
- ○ £50,000–£99,999

- ○ £100,000–£250,000
- ○ Over £250,000

Q22. How have these investments in cyber security measures impacted your overall business?

Q23. Could you please expand on your response above? _____

Display This Question: If Q8 = Yes

Q24. Please rank the below key benefits of having cyber insurance based on order of preference for your business: *Drag and drop your options to rank, where 1 is 'most preferred' and 6 is 'least preferred'.*

_____ Access to cyber security experts and resources
_____ Access to incident response team
_____ Business continuity during a cyber event
_____ Coverage for legal liabilities and regulatory fines
_____ Financial protection against cybercrime
_____ Other (please specify):

Q25. Please rank the below limitations or challenges your company has encountered with cyber insurance: *Drag and drop your options to rank, where 1 is 'most limiting/challenging' and 9 is 'least limiting/challenging'.*

_____ Challenges in meeting cyber security requirements
_____ Complicated claims process
_____ Difficulty in understanding or navigating policy terms
_____ Difficulty understanding the value of the coverage
_____ Excessive or unclear requirements to qualify
_____ High premium costs
_____ Limited coverage for certain types of attacks (e.g., ransomware)
_____ Low levels of business interruption coverage
_____ Other (please specify):

Display This Question: If Q8 = Yes

Q26. Has your insurance provider offered any assistance in helping your company meet cyber security requirements?

○ Yes
○ No

Display This Question: If Q26 = Yes

Q27. Please describe the support provided:_____

Q28. Please rank the following types of resources/support based on how important they would be for helping your business to better understand and utilise cyber insurance: *Drag and drop your options to rank, where 1 is 'most important' and 5 is 'least important'.*

_____ Case studies or examples of how cyber insurance has supported businesses
_____ Education and training on cyber insurance basics
_____ Guidance on integrating cyber insurance into overall risk management
_____ Recommendations for cyber security best practices
_____ Other (please specify):

Q29. Please rank the following factors in order of importance for encouraging your company to purchase or upgrade its cyber insurance policy: *Drag and drop your options to rank, where 1 is 'most important' and 6 is 'least important'.*

_____ Clearer policy terms
_____ Easier qualification process
_____ Higher percentage coverage of risk
_____ Lower premiums
_____ Support for cyber security improvements
_____ Other (please specify):

Q30. What do you think would improve your understanding of cyber insurance?

Q31. Do you have any additional comments, concerns, or experiences with cyber insurance that you would like to share?

Q32. Would you be interested in participating in a follow-up interview to share more about your experiences and insights?

- ○ Yes
- ○ No

Display This Question: If Q32 = Yes

Q33. As you selected 'yes', please provide the email address you would like us to reach out to:

_____

Annex C: Industry questions

1. Introduction (5–10 minutes)

- **Purpose of the Interview**:
  We explain the objective of the study and that this discussion aims to understand their perspective on the cyber insurance landscape, challenges, opportunities, and insights into how SMEs engage with cyber insurance.

- **Participant Background**:
  Ask the interviewee to share:

    - Their professional role, responsibilities, and years of experience in the cyber insurance sector.
    - The types of clients they primarily serve (e.g., industry focus, business size).
    - Their perception of the SME segment as a target market for cyber insurance.

2. Current Landscape of Cyber Insurance (10–15 minutes)

Survey Connection

Survey sections exploring SME awareness, adoption rates, and perceptions of cyber insurance are directly tied to this part of the discussion. For instance, if the survey shows low awareness among SMEs, this section digs into why insurers think that is the case and how they're addressing it.

Insight

While the survey identifies adoption trends quantitatively (e.g., X% of SMEs lack insurance due to cost), the interviews uncover qualitative nuances, such as specific market dynamics, underserved industries, or insurer efforts to educate SMEs.

Questions

- **Market Trends and Demand**:
    - How has the cyber insurance market evolved in recent years, particularly for SMEs?
    - Do you think SMEs are aware or interested in cyber insurance?
    - Has awareness changed in recent years?
    - Is there a particular industry or region that is showing more interest?
    - Is there an industry/region that is showing less interest? Why

- **Policy Coverage**:

- What are the most common types of coverage included in SME-focused policies?
- Are there any notable gaps in coverage that SMEs frequently raise concerns about?
- How do exclusions and limitations impact policy adoption?

- **Claims and Incidents**:
  - What types of claims are most common from SME clients?
  - Are there emerging trends in the types of cyber incidents affecting SMEs?
  - How does the claims process for SMEs differ from that of larger enterprises?

3. Challenges and Barriers (15–20 minutes)

Survey Connection

The survey gathers data on barriers SMEs face, such as cost, complexity, or meeting requirements. This section asks insurers to share their perspective on these challenges and the efforts made to address them.

Insight

By comparing survey responses about challenges (e.g., "high premiums" or "limited coverage") with insurers' explanations (e.g., cost drivers or underwriting complexities), the discussion uncovers gaps between SME perceptions and insurer realities.

Questions

- **Adoption Barriers**:
  - What are the main challenges insurers face in selling cyber insurance to SMEs? (Probe for cost, complexity, perceived lack of value, etc.)
  - How do factors like premium costs, policy complexity, and coverage limitations influence adoption?
  - Are SMEs aware of the potential value of cyber insurance, or is there a knowledge gap relating to awareness and risk of a cyber-attack?

- **Underwriting Challenges**:
  - What challenges exist in assessing and underwriting risks for SMEs?
  - Do insurers require SMEs to meet specific cyber security standards before issuing policies? If so, what are the standards?
  - How do insurers handle the variance in cyber security maturity among SMEs?
  - Does the insurance industry utilise government tools/guidance?

- **Brokers' and Insurers' Challenges:**

- What difficulties do brokers face in educating and selling cyber insurance to SMEs?
- Are there particular pain points in maintaining relationships with SME clients?
- What feedback or complaints do SMEs commonly provide about cyber insurance policies?
- Are brokers appropriately equipped with the right tools/knowledge?

4. Pricing, Accessibility and Incentives (10–15 minutes)

Survey Connection

The survey explores SME budget constraints, willingness to pay, and what incentives might encourage adoption. This section examines how insurers set premiums, design policies, and consider incentives.

Insight

While SMEs may cite "high costs" as a barrier, the interviews may clarify why premiums are priced as they are (e.g., claims trends, reinsurance costs). It also sheds light on how insurers assess affordability and design financial incentives.

Questions

- **Premium Costs**:
  - How are premiums typically determined for SME clients?
  - Are current pricing models perceived as accessible for SMEs?
  - Are there any efforts to make cyber insurance more affordable for smaller businesses?

- **Incentives**:
  - Are there any incentives offered to SMEs for implementing robust cyber security measures (e.g., premium discounts)?
  - What further support do you think can be provided in encouraging cyber insurance adoption?

5. Role of Brokers and Insurers (10–15 minutes)

Survey Connection

Survey questions related to SMEs' understanding of cyber insurance and their need for education or support align with this section. This part explores the roles insurers and brokers play in bridging knowledge gaps.

Insight

SMEs may indicate they don't fully understand policies or their value. This section seeks to uncover how insurers educate their clients, what tools they use, and whether they recognise these gaps as significant obstacles.

Questions

- **Support and Education**:
    - What resources or support do brokers/insurers provide to help SMEs understand cyber insurance?
    - How effective are these resources in addressing knowledge gaps or misconceptions?
    - What challenges do you face in communicating the value and limitations of policies?

- **Policy Development**:
    - How are policies designed to meet the unique needs of SMEs?
    - Is there a demand for more tailored or modular policies?

- **Collaboration and Partnerships**:
    - Are insurers working with cyber security providers to enhance the value of policies (e.g., bundled services)?
    - Are there opportunities for greater collaboration with industry groups or government bodies to promote cyber insurance?

6. Future of Cyber Insurance (10–15 minutes)

Survey Connection

The survey might gather SME perspectives on what would make cyber insurance more appealing or valuable. This section aligns by exploring insurers' plans to innovate and adapt to emerging risks and needs.

Insight

Insurers provide a forward-looking view, offering ideas about market trends, technologies, or regulatory changes that could transform the SME landscape. This contrasts with SMEs' current challenges and aspirations, creating a roadmap for progress**.**

Questions

- **Emerging Trends**:
    - What trends do you foresee shaping the future of the cyber insurance market?

- How are emerging threats (e.g., AI-enabled attacks, supply chain vulnerabilities) affecting the demand for cyber insurance?
- Are there technologies, such as AI or machine learning, being used to improve underwriting or claims processing?

- **Market Opportunities**:
  - What untapped opportunities exist in the SME segment?
  - How can insurers and brokers better serve SMEs?
  - Are there specific sectors within the SME market that are particularly underserved?

- **Regulatory Landscape**:
  - How do current regulations impact the cyber insurance market?
  - What role could the government play to help SMEs understand the market. For example, through guidance?
  - What role should regulators play in ensuring clarity, fairness, and accessibility in cyber insurance policies?

7. Final Thoughts (5–10 minutes)

Survey Connection

Open-ended survey questions about SME concerns or suggestions for improvement align with this section, as it seeks actionable recommendations from insurers.

Insight

This closing section ensures a wider understanding by capturing any additional insights or perspectives that may not directly correlate with specific survey questions.

Questions

- **Closing**:
  - Is there anything else you would like to share about your experience or perspective on cyber insurance for SMEs?
  - Do you have any recommendations for improving SME access to and adoption of cyber insurance?

References

- Biener, C., Eling, M. and Wirfs, J.H. (2015). ‘Insurability of Cyber Risk: An Empirical Analysis’, The Geneva Papers on Risk and Insurance – Issues and Practice, 40(1), pp. 131–158.

- Brown, J. and Patel, S. (2020). Cyber Security and Data Protection Regulations in the UK. Oxford: Oxford University Press.

- Deloitte (2022). Blockchain in Insurance: Driving Transparency and Efficiency in Claims Processing. Available at: https://www2.deloitte.com/ca/en/pages/financial-services/articles/blockchain-in-insurance.html (Accessed: 04 March 2025).

- Descartes Underwriting (2024). Cyber Shutdown Parametric Solution for a Manufacturing Company. Available at: https://descartesunderwriting.com/case-studies/cyber-parametric-solution-manufacturing-company [Accessed 06 March 2025].

- ENISA (2021). Cyber Security Guide for SMEs. Available at: https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes? [Accessed 11 March 2025].

- Europol (2023). 'Internet Organised Crime Threat Assessment', Europol. Available at: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023 (Accessed: 19 March 2025).

- Hiscox (2021). Cyber Readiness Report 2021. Hiscox. Available at: https://www.hiscox.co.uk/broker/about-hiscox/news/cyber-readiness-report-2021 (Accessed: 2 March 2025).

- IBM (2024) Cost of a Data Breach Report 2024. IBM Security. Available at: https://www.ibm.com/security/data-breach (Accessed: 14 March 2025).

- Insurance Times (2023). Brokers to take a more proactive approach to cyber risk education, CyberCube. Available at: https://www.insurancetimes.co.uk/news/brokers-to-take-a-more-proactive-approach-to-cyber-risk-education-cybercube/1445479.article? [Accessed 11 March 2025].

- Intangic MGA (2023). Intangic MGA announces cyber parametric policy. Available at: https://www.insurancebusinessmag.com/uk/news/cyber/intangic-mga-announces-cyber-parametric-policy-439765.aspx [Accessed 21 March 2025].

- Johnson, P. and White, R. (2021). 'Phishing Attack on a Legal Firm: Implications for GDPR Compliance', Legal Cyber Security Review.

- Kapani, C. (2024). Businesses at risk from SME partners with weaker cyber defences. Strategic Risk. Available at: https://www.strategic-risk-global.com/cyber-/-technology-risks/businesses-at-risk-from-sme-partners-with-weaker-cyber-defences/1451860.article (Accessed: 25 March 2025).

- Marsh (2022). UK Cyber Insurance Trends Report 2022. Available at: https://www.marsh.com/en/services/cyber-risk/insights/uk-cyber-insurance-trends-report-2022.html [Accessed 12 March 2025].

- MacColl, J., Nurse, J.R.C. and Sullivan, J. (2021). 'Cyber Insurance and the Cyber Security Challenge', Occasional Papers. Royal United Services Institute, June. Available at: https://rusi.org/explore-our-research/publications/occasional-papers/cyber-insurance-and-cyber-security-challenge (Accessed: 01 March 2025).

- McKinsey & Company (2024). The cybersecurity provider's next opportunity: Making AI safer. [online] Available at: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cybersecurity-providers-next-opportunity-making-ai-safer? [Accessed 15 March 2025].

- Microsoft (2022). Microsoft Digital Defense Report 2022. Available at: https://www.microsoft.com/en-gb/security/business/microsoft-digital-defense-report-2022-cyber-resilience (Accessed: 10 March 2025).

- Munich Re (2024). Cyber Insurance: Risks and Trends 2024. Available at: https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html [Accessed 26 March 2025].

- National Cyber Security Centre (2023). Supply chain security guidance. [online] Available at: https://www.ncsc.gov.uk/collection/supply-chain-security [Accessed 1 April 2025].

- NFU Mutual (2023). NFU Mutual, Skyline Partners, Gallagher, and Markel Pioneer New Parametric Insurance to Protect Dairy Farmers from Heat Stress Losses. Available at: https://www.nfumutual.co.uk/media-centre/nfu-mutual-skyline-partners-gallagher-and-markel-pioneer-new-parametric-insurance-to-protect-dairy-farmers-from-heat-stress-losses/ [Accessed 26 March 2025].

- UK Government (2024). Cyber Security Breaches Survey 2024. Available at: https://www.gov.uk/government/collections/cyber-security-breaches-survey (Accessed: 01 March 2025).

- Smith, A., et al. (2022). 'Ransomware Attack on UK Retail SME: A Case Study', Journal of Cyber Incident Response.

- The Geneva Association (2024). Catalysing Cyber Risk Transfer to Capital Markets: Catastrophe bonds and beyond. [online] Available at: https://www.genevaassociation.org/publication/cyber/catalysing-cyber-risk-transfer-capital-markets-catastrophe-bonds-and-beyond [Accessed 19 March 2025].