Cyber Resilience for SMEs: The Insurance Gap Explored

January 2025

Contents

The UK insurance and long-term savings market and the ABI

The ABI is the voice of the UK's world-leading insurance and long-term savings industry, which is the largest sector in Europe and the third largest in the world. We represent more than 300 firms within our membership, including most household names and specialist providers, providing peace of mind to customers across the UK.

We are a purpose-led organisation: Together, driving change to protect and build a thriving society. On behalf of our members, we work closely with the UK's governments, HM Treasury, regulators, consumer organisations and NGOs, to help ensure that our industry is trusted by customers, is invested in people and planet, and can drive growth and innovation through an effective market.

A productive and inclusive sector, our industry supports towns and cities across Britain in building a balanced and innovative economy, employing over 300,000 individuals in high-skilled, lifelong careers, two-thirds of whom are outside of London. Our members manage investments of £1.4 trillion, contribute £18.5 billion in taxes to the Government and support communities and businesses across the UK.

Association of British Insurers
One America Square, 17 Crosswall, London EC3N 2LBT:
+44 (0) 207 600 3333 I **abi.org.uk**

Foreword

Small and medium-sized enterprises (SMEs) are the lifeblood of the UK economy, accounting for 99.9% of all businesses and generating over £2.6 trillion in turnover. These businesses drive innovation, create jobs and sustain communities across the country. Yet, despite their importance, SMEs are increasingly at risk to cyberattacks—an evolving threat that many are ill-equipped to handle.

The reality is stark. In 2024, half of all UK businesses fell victim to a cyber breach or attack. For SMEs, the consequences can be devastating. With limited resources to allocate to cyber security, many are left exposed, easy targets for cyber-criminals who exploit weaknesses in their systems. The fallout is often catastrophic: financial loss, reputational damage, and disruption that can cripple operations and impact employees, customers and communities.

This is where the insurance industry plays a vital role. As cyber threats evolve with unprecedented speed and sophistication, we must offer innovative solutions and proactive measures that enable SMEs to protect themselves. The stakes are high, and the need for accessible, comprehensive coverage has never been greater.

In this report, the Association of British Insurers (ABI), in collaboration with Grant Thornton UK LLP, examines the state of the cyber insurance market for SMEs. Our findings shed light on the challenges that leave many businesses vulnerable. More importantly, we offer actionable insights and practical recommendations for insurers, brokers, and policymakers to bolster cyber resilience across the economy.

The challenges are significant, but so too are the opportunities. By equipping SMEs with the right tools, knowledge and support, we can help them secure their digital future and continue to thrive in a rapidly changing world. The insurance industry is committed to playing a pivotal role in this effort, ensuring that businesses - large and small - have the protection they need to succeed in the face of growing technological risks.

Hannah Gurga
Director General, Association of British Insurers (ABI)

Executive summary

The ABI has worked with Grant Thornton UK LLP to assess the cyber insurance market in the UK to help identify the needs of SMEs and the availability and suitability of current cyber insurance offerings. This report makes recommendations on how to increase access and take-up of current and future insurance products and improve the resilience of SMEs.

Cybercrime and cyber breaches continue to increase in number and severity year upon year, manifesting for most businesses in the UK as the top risk they will face. Cyber Insurance continues to be one of the best cyber risk mitigation strategies available to SMEs in the UK, helping to prevent and alleviate the impacts of a cyber-attack, and raise the preparedness and cyber hygiene of businesses in many cases[1]. With comprehensive products, incorporating many value-add services that benefit the SME buyer, it presents one of the best value risk mitigation strategies available.

There are around 5.6 million SMEs in the UK[2], contributing more than £2.6 trillion in turnover. SMEs contribute over 50% of UK GDP and account for around 99.9% of all businesses in the UK. In 2024, 50% of UK businesses have suffered some form of cyber security breach or attack[3]. Supporting SMEs is essential to ensuring the long-term economic growth of UK PLC and commercial prosperity in the UK.

The sophistication of cyber-attacks and challenges for SMEs are also increasing. AI powered hackers continue to evolve their own very successful attack strategies, while new laws that require improved cyber hygiene and reporting are being introduced. The UK Cyber Security and Resilience Bill is expected to make cyber reporting stricter and require businesses to raise their resilience, at least in certain portions of the economy. UK regulators also continue to raise the bar and prioritise cyber resilience practices and scrutinise businesses' data privacy controls.

There is clearly an opportunity and a growing need to improve the cyber and operational resilience of SMEs in the UK, and a growing commercial opportunity for the insurance industry to broaden and deepen its support for SMEs.

This report includes analysis of the SME market, research and interviews with insurers, brokers and businesses with and without cyber insurance. A number of common themes and opportunities to enhance cyber awareness and adoption of cyber insurance among SMEs were found:

- Many SMEs think they are too small to present a target to cyber-criminals. Proactive education and marketing activities can help communicate the risks and impacts of a breach or disruptive event to better position cyber insurance and the benefits it can bring.
- Brokers may benefit from additional support from insurers, helping them to communicate the differentiators and value proposition of cyber insurance policies and how they differ from typical insurance solutions.
- SMEs reported that they cannot identify a single and holistic source of government cyber security guidance relevant to their needs. Government can harmonise and centralise the range of guidance available and proactively raise awareness of where to find trustworthy best practices.
- Cyber insurance can be (and is often) positioned as a comprehensive suite of services that are available throughout the policy's duration, in addition to traditional indemnification.
- Promoting the ongoing benefits and services available through the broker and insurer is key to improving SMEs' understanding of cyber insurance.
- The cost of SME Cyber insurance is typically competitive and presents good value. More, however, needs to be done to communicate this value in an accessible way.
- Reducing the onboarding burden of cyber insurance processes for buyers, brokers, and insurers can significantly improve accessibility for SMEs. This can be achieved through the use of streamlined proposal forms, online platforms, and greater use of insurtech. Additionally, automated onboarding and approval workflows can further enhance these benefits.
- Strong reliance on statistical models for low risk insureds, automated security risk appraisal tools, training and capability development and partnerships with external vendors to better assess risk profiles will also help reduce the onboarding burden, and increase access to the cyber insurance market for SMEs, whilst also increasing the profitability of the SME segment.

Evolving the mindset of insurers and brokers, tailoring the products and how they are sold to SMEs will help reach more insureds in order to address the protection gap and harness the opportunity this market presents. However, the most significant barrier to take-up identified in this research, is the widespread lack of SME cyber security awareness.

[1] What does cyber insurance cover? What does cyber insurance cover?
[2] See Appendix D: Definitions and Terminology, for analysis of how SMEs are defined by government, trade bodies and insurers, and the various definitions of cyber crime.
[3] Cyber security breaches survey 2024;

Key Recommendations to Boost the SME Cyber Insurance Market

There is a large market of addressable SMEs. These businesses are being proactively and effectively targeted by cyber-criminals, and they are statistically less well-prepared to respond to these incidents, relative to larger businesses with sizeable investments in cyber resilience maturity programmes. SMEs are exposed to a disproportionate risk from existential threats arising from a cyber-attack: one relatively minor incident can put them out of business. All businesses, and especially smaller ones, would benefit from effective cyber insurance solutions and many would engage with it. This should be part of widespread coordinated efforts to improve security practices. However, there are significant challenges in growing the market.

Many SMEs expressed that:

- they felt that their risks from cyber-attacks were low;
- they did not require insurance or were already covered for such risks in other policies they held; and
- that the insurance product was too expensive or complicated to suit their modest requirements.

These misconceptions could be addressed through consistent and persistent messaging from government and the insurance industry. Cyber insurance often folds in many valuable services that benefit the SME buyer. By reference to external security solutions and consultants, cyber insurance is typically cheaper when compared to many IT consultancy and technical solutions, and presents one of the best value risk mitigation strategies available. More SMEs might engage with insurance products if they were presented and sold to them in more accessible ways.

Challenges in the SME Cyber Insurance Market

- Many SMEs continue to underestimate the cyber risks they are exposed to and have not recognised the value of risk management and risk transference solutions.
- Risk assessing potential insureds and onboarding SMEs with potentially significant exposures often creates commercial challenges in a market that already offers slim profits, especially as the market softens.
- Friction and inefficiencies in insurer and broker onboarding processes discourage potential customers from buying insurance, limiting the profitability and value of the SME cyber insurance market.
- The insurance market and wider cyber practitioners lack a common lexicon for technical terms, leading to difficulty for potential insureds in understanding product fit and the value of comparable products.
- There is a need for enhanced joint support and education efforts by insurers and brokers to better communicate the value of insurance products to potential customers.
- Government's approach to cyber security does not appear to be consistent or cohesive in the support provided to SMEs. There are many messages and lots of advice available, but it is scattered and occasionally inconsistent.

There are numerous opportunities to address these concerns and increase uptake in the SME segment, summarised below.

In-depth research insights, recommendations for specific stakeholders, definitions and methodologies are provided later in the report.

The Strong Value Proposition of Cyber Insurance

SMEs are often surprised at the excellent value proposition presented by cyber insurance solutions available in the UK market. The price of typical UK SME cyber insurance solutions is not the major challenge to growing the market.

> **The opportunity to offer a comprehensive suite of valuable risk mitigation and security benefits, alongside traditional indemnification, positions SME cyber insurance as one of the best value risk mitigation strategies available to this segment. There are also a range of products that offer more narrow coverage depending on the SME requirements.**

Marketing these solutions in a way that speaks to the SME buyer's specific needs and concerns should be a top priority for those seeking to reach SMEs.

Endorsements of the Benefits of Cyber Insurance

SMEs can be directed towards authoritative information on the value of cyber insurance.

> **The National Cyber Security Centre (NCSC) notes that "as well as minimising business disruption and providing financial protection during an incident, cyber insurance may help with any legal and regulatory actions after an incident.[4]"**

The UK government and Counter Ransomware Initiative (CRI) also recognise that "Cyber insurance can be an important risk management practice. CRI members recognise the important role that cyber insurance can play in helping to build resilience to cyber-attacks, including through supporting the companies they insure to improve their protective measures.[5]"

Cyber Education and Awareness Campaigns

Many SMEs are unfamiliar with cyber risks and associated jargon, often fail to understand the evolving complexity of cyber risks, and are calling out for better preparedness, education and assistance both pre-insurance, during the life of the policy and especially during the after-math of a cyber-attack.

> **SMEs would benefit from multiple means of education to reinforce consistent, joined-up, constructive messages using clear and consistent language and a singular well-known source of authority to link them. This can include guidance from government (local and national), insurers, brokers, trade bodies, cyber security consultancies, and cyber support firms. Examples such as the ABI's guide to "What does cyber insurance cover?[6]" provide localised accessible and comprehensive guidance signposting.**

Awareness amongst SMEs could be improved to help them understand that they are not too small to be a target. A common attack mechanism aimed at this segment may be vulnerabilities in software that they use such as popular blogging, Point of Sale and eCommerce platforms aimed at SMEs.

They must also understand that if they outsource their IT operations, they are still responsible for their cyber security. "Out of sight" risks must not be "out of mind" risks.

Insurers and brokers can help illustrate these concerns in an accessible way. Examples include, "how long could your business operate without email?", and "if your employee health records are destroyed by hackers, can you allow staff to work on your production lines?"

Security Standards and Certifications

SMEs can benefit from meeting clear basic standards, such as the Cyber Essentials Scheme (CES) for the very smallest businesses, CES+ style standards for the slightly larger, and then regulations such as Network Information Security 2 Regulation (NIS2), ISO 27001, DORA etc. for even larger businesses.

As part of their wider considerations for offering coverage, insurers and brokers can support SMEs with their understanding of which standards are appropriate for their business, how to implement them and obtain the relevant certifications. This will also support SMEs when developing their governance around security posture.

Minimum, fully embedded and strongly evidenced, government expectations of security and best practices would help strengthen the market view of risk at a high level, and support the uptake of the products and overall resilience of UK PLC.

Raising awareness of cyber risks typically takes the SME on a journey to seek out mitigations, including cyber insurance as a risk management strategy for SMEs.

Supply Chain Risks

Cyber insurance helps SMEs demonstrate strong business continuity standards, supporting cyber hygiene and resilience in business operations.

Small businesses often have relatively weaker cyber security, making them targets for cyber criminals and impacting other organisations that they work with. Large businesses have an important role to play, to enforce minimum cyber security standards from SME suppliers, seeking evidence of compliance. This includes standards such as ISO 27001 and CES+ as well as insurance and other measures

Insurers consider accumulation risk in supply chains, evaluating potential loss exposure from one event affecting multiple entities and this supports understanding of SME risks.

[4] Cyber insurance guidance;
[5] CRI guidance for organisations during ransomware incidents;
[6] What does cyber insurance cover?

Grants and Support

SMEs could be advised or made aware of the NCSC grants and other support available to them to improve their cyber resilience. More funding could be made available for SMEs who cannot afford commercial cyber security.

"Appendix G: External Cyber Advice and Guidance" highlights numerous government and insurer promoted resources available to SMEs at low or no cost to support improving their security posture. SMEs can be educated and encouraged by the insurance industry and government to build an appropriate level of resilience, including by engaging with cyber insurance. Brokers play an essential role in interfacing with these buyers and insurers can support them by signposting information and developments in the cyber threat landscape and insurer products, supporting them with information reports and educational sessions that weave in government messages and resources where appropriate.

Bank Lending

The SME's cyber security posture and risk management methods such as cyber insurance could be a positive influencing factor that lenders consider in the SME financial loan application process. Additional evaluation methods could support lenders making investment choices, especially in the current environment of constricted SME lending. SMEs can consider communicating their resilience in the bank lending process: a more robust business is a better customer for a lender.

On-boarding, Advice and Coverage and Gaps

Efforts by insurers in the UK in simplifying onboarding hurdles are welcome, including potentially reducing or indeed eliminating complex documentation, exclusions and technical jargon. Some scale their onboarding requirements, ranging from a single page of information for a micro business to a handful of pages for an SME, and full cyber due diligence for a larger business. Tailored approaches like this were greatly appreciated by SMEs surveyed and increased the reported likelihood that they would buy a policy.

Greater use of technology and direct sales in the cyber insurance management process can also lower insurers' potential cost and risk burden, increase take-up and profits and improve the quality of the product fit for SMEs.

SMEs could be advised pro-actively by their brokers of cyber cover already included in other policies that they hold, and the gaps that are to be covered by cyber insurance. Simplified illustrations of coverage, including information about excesses, limits, exclusions etc. would strengthen this information.

SMEs could be attracted by a more 'off the shelf' product offering, especially those with the smallest budgets. This has proven commercially challenging for insurers, given the high exposure vs low budgets of many SMEs. However, it could be achieved, at least partially, through simplified onboarding documents and processes, efforts to clarify and harmonise terminology used in documentation, and improving the SME customer experience through digital solutions and tailored, insurtech-supported proposal forms.

> **Some SME businesses commented that they would prefer to buy from an insurer that had a fully online process rather than a paper based equivalent.**

The Skills Gap

In 2025, government has announced new regional skills projects to bolster UK cyber defences and deliver on their Plan for Change, with more than 30 projects being launched across England and Northern Ireland to deliver targeted support to boost the UK's cyber resilience[7]. This is vital across all areas of the economy, as having experienced cyber experts available is statistically one of the best ways to lower the impact of a cyber incident. However, there is a widespread cyber skills gap in the UK. For the SME, fewer dedicated cyber security staff and lower levels of cyber breach experience result in proportionately more expensive breaches. They take longer to resolve compared to breaches in larger, more experienced organisations, resulting in a greater impact from business interruption, greater loss of client confidence, greater commercial impacts on supply chains around the SME, and a higher chance of a complete commercial failure. Many SMEs do not survive a single cyber-attack.

Insurers and brokers are also challenged by a skills gap and there is a competitive market for experienced cyber insurance practitioners. Less tailored insurer cyber breach handling may result in slower (and possibly more expensive) resolution of a cyber incident. Some brokers report feeling less comfortable providing detailed cyber security advice to SMEs. Others are concerned that they do not fully understand the complexities of cyber security and how the policies can address them. The lack of cyber security professionals across the board and especially in brokers and SMEs will increase a lack of awareness of the risk SMEs face and their possible impacts.

[7] Regional Skills Projects;

The ABI and Lloyd's have been working to support technical understanding of cyber risk in insurance and published 'Components of a Major Cyber Event: A (Re)Insurance Approach'8 with a comprehensive technical cyber glossary included. There should be widespread effort to increase cyber skills in the UK, and insurers and brokers should upskill their technical teams internally or outsource support, and redesign approaches where capacity allows. Those aiming to service the SME segment should stay abreast of the rapidly evolving technical cyber requirements specific to SMEs.

The Value and Risk of Data

It's a legal obligation for businesses to implement appropriate cyber and data hygiene when processing personal data[9]. SMEs need to understand the value of the data that they hold and prepare to deal with a cyber-attack or a data error, and the fallout.

Data risks may be particularly acute for SMEs who may, for their modest size, carry relatively high volumes of sensitive data, including customer data, supplier information, financial records, health records, employee data, commercially sensitive intellectual property and many other types of valuable or sensitive information.

Keeping in mind that a resilient business is less likely to suffer from a breach or attack, and knock-on legal actions, supporting data security helps to manage profitability for the insurance industry. Raising minimum standards within SMEs will keep them safer and present better insurance opportunities to the industry.

> **SMEs should get familiar with understanding the types of data they hold, how it is secured and the controls around it. This includes information about the impact of evolving regulation, reputation, litigation risk, formal cirtifications, and scrutiny in specific industry sectors. Insurers and brokers can support these conversations and present the tools and approaches to identify the answers.**

Simple ways to address risk

Many risks from cyber-criminals could be addressed using relatively accessible and low cost or free cyber hygiene improvements, and these could stop or mitigate many attacks or breaches. Around 97% of cyber-attacks could have been prevented by implementing basic and often free cyber security habits. The ABI's online Cyber Safety Tool [10] helps a businesses generate a tailored action plan with low cost and relatively easy to implement actions to improve their risk posture.

Brokers and insurers can distribute material such as the "Top Ways to Improve your Cyber Hygiene", in plain English with links to free government advice such as that on the NCSC webpages, along with product information.

8 Guidance on Major Cyber Events;
9 Laws about data protection;
10 Cyber Safety Tool

Top ways to improve SME cyber hygiene
Based on the ABI SME cyber safety tool

Conclusions and Observations from Analysis

SMEs are the backbone of the UK economy, forming 99.9% of businesses and contributing over 50% of financial value. However, cyber-attacks are getting more sophisticated and are ever increasing in number. SMEs are shown to be easier targets, low hanging fruit to gain access to computer systems, valuable and sensitive data, and increasingly connected supply chains.

Many SMEs have not addressed cyber hygiene, do not have "tried and tested" incident response plans in place, adequate cyber resilience mechanisms, and relatively few have obtained and maintained cyber insurance. This report examines inhibitors, causes of resistance and perceptions, and misconceptions that the SME buyers and brokers and insurers may have about insurance products.

A number of common themes have emerged from our research:

- There is a perceived lack of harmonised government support for SMEs from a single golden source.
- SMEs do not know where to seek guidance as there are a plethora of sources, much of which they may not be familiar with.
- Government cyber information is based on a 'pull model' requiring the SME to find it, rather than a 'push model', and many SMEs are not being proactive in seeking out good guidance.
- Insurers, and others more broadly, do not have a common cyber lexicon that can be used uniformly in policies, making it difficult to compare and contrast different products.
- Insurance is often sold as a 'product' without explaining that cyber insurance is a 'service' that starts at pre-inception and carries on throughout the life of the policy and beyond.
- Cyber-attacks and mechanisms to cause loss and damage to businesses evolve daily. Insurers and brokers need to evolve in lockstep with these threats and tailor their solutions and marketing to reach the SME buyer.
- Some insurers and brokers are still using paper-based processes for proposals, policy management and claims. SMEs indicated that they wanted a faster and simplified proposal process.
- Many SMEs have not addressed the possibility of a cyber-attack or other disruption, as they think that it won't happen to them or that they are too small to be a target. Both are misconceptions that can cause catastrophic failures for the businesses. Insurers and brokers can communicate the reality of these risks and tangible solutions.
- Many SMEs do not understand the value of the data that they hold, the possible impacts of a cyber-attack on them and how cyber insurance can form part of their governance and risk management strategy.
- There is a skills and training gap in cyber insurance, especially in areas such as broking and cyber incident handling. The industry would benefit from broader skills development efforts, and increased investment in training and development exercises and partnerships.
- A number of SMEs commented on the perceived high cost of cyber insurance. This misconception requires appropriate marketing and broker momentum to address. SME insurers have priced their products competitively to reflect the risks they're taking on and the value added support they are offering.

Underpinning all of the observations in this report is the need for increased awareness of the value that cyber insurance can bring to SME resilience. Government can do much to support these specific requirements and provide information about up-to-date mitigations, and awareness of evolving threats globally.

There is much to be done collectively and there is a very large and addressable market of SMEs who desperately need support to bolster their cyber hygiene. Cyber insurance is an invaluable tool to prevent and alleviate the impacts of a cyber-attack, and raises the general hygiene and resilience of businesses across the UK. It continues to be one of the best value cyber risk mitigation strategies available to SMEs in the UK.

Appendices and Additional Research

Appendix A: The SME Market Opportunity

Spotlight on the cyber insurance market

Cyber Insurance Uptake

Take up of cyber insurance by SMEs is relatively low, when they could be the business group that benefits most from the valuable solutions it offers.

- In the government's Cyber Breaches Survey, 43% of businesses reported being insured against cyber security risks in some way, typically via an 'add on' to a wider insurance policy. 25% of medium businesses reported having a specific policy in place[11].
- Underwriter CFC states that 'SME businesses buying cyber insurance was only 15% in the UK[12].
- The Federation of Small Businesses (FSB) 'Paying a Premium'[13] research found that only 10% of small businesses have cyber insurance[14].

Taking the FSB's 10% estimation, that would leave the addressable cyber insurance market at over 230,000 SMEs (see "Appendix D" for calculation).

Why SMEs need Cyber Insurance

Whilst cyber security is the responsibility of the business owners and management, when a breach or attack happens, cyber insurers have the opportunity to provide crucial support services, liquidity, and "breach management" facilities to help the business react, respond and recover.

> **Cyber insurance solutions typically provide access to vetted cyber incident management professionals, ready to deploy almost immediately, providing significant psychological reassurance to the SME, as well as providing opportunities to stop or limit the impact of the incident quickly.**

The Value of Cyber Insurance

There are basic policies available for under £100 and even some very limited free coverage that comes along with Cyber Essentials, which still has low uptake. SME policies with a fuller suite of services may cost hundreds to low thousands of pounds and could be paid monthly to assist in cash flow for the SME.

A popular yet inaccurate explanation for low uptake is the SME's perception of the high cost of standalone cyber insurance policies, which is not the case.

Despite a wide range of product offerings, there are some negative reports on product value. There is anecdotal evidence that premium can rise from £50,000 to £250,00 per annum following a large cyber incident, and large changes in premium can make it hard to invest in cyber insurance.

In a challenging economic climate, SMEs may be inclined to regard cyber insurance as a low probability, low impact risk, and thus a "nice to have" rather than an essential risk management tool. They may be required to prioritise budgets away from cyber security protection and cyber insurance to day-to-day financial challenges. However, the cost of cyber insurance for SMEs is typically significantly more cost-efficient than even basic third-party cyber consultancy solutions, which can cost hundreds of times more. Insurers can also add an extra layer of certainty that cyber solutions are well configured to address the actual SME business risk.

The typical purchaser of cyber insurance in an SME might be the business owner, finance manager, financial director or chief financial officer. Typically, these roles will have little day to day familiarity with the cyber risks faced by the SME and the impact of a cyber-attack. Thus, they may be somewhat distanced from the value proposition of cyber insurance and the benefits that it brings. They will however, understand the compelling benefits that insurance can provide to a business in terms of supporting financial stability, investability and responsible governance.

Types of Insurance

Some SMEs comment about the complexity of cyber insurance and concerns about whether it suited their needs. This is partly because cyber concepts are not standardised, or well understood and cyber insurance can be perceived as an overly technical product. The ABI provides well respected guidance for potential Insureds on

[11] Cyber security breaches survey 2024, Department for Science, Innovation and Technology, 9 April 2024 (p28) para 2
[12] UK insurance market over cyber 'hurdle';
[13] Paying a premium?; |

14 Discrepancies may be due to differing sample populations, Cyber Breaches Survey includes more charities, CFC is likely to include more higher revenue SMEs and the FSB may capture the smaller lower turnover businesses.

how to stay abreast of policy exclusions and coverage adequacy[15]. For example, cyber insurance typically is split into two areas:

- First party risk - restoration of systems and management of business interruption; and
- Third party risk – claims against the business by any relevant interested third party, following a data breach or security breach.

Insurance is not a right, and SMEs may have to meet specified requirements to obtain cover; these may include undertaking some cyber hygiene actions prior to cover being granted, or they may incur an increased premium for not implementing them. These evaluations are often made by the insurer based on statistical analysis of parameters identified by the insured and the broker.

SME cyber Insurance solutions often provide a suite of support solutions such as:

- Breach response assistance.
- Business interruption support.
- Call Centres to handle customer questions.
- Communications strategy and media liability.
- Cyber theft and fraud coverage.
- Damage to IT Systems and information.
- Data theft.
- Data restoration.
- Hacking, extortion and ransomware.
- Increased cost of working support.
- Legal assistance and regulatory costs.
- Legal Liability.
- Notification services for affected employees as well as clients.
- Possible notifications to regulators in relevant jurisdictions of operations.
- Public relations services.
- Specialised breach Counsel.
- Specialist forensics consultancy.

Some SMEs may assume that their cyber risks are already covered by other insurance policies they hold. In the UK this has been regulated against, and insurers are obliged to inform their insureds of this change, however, insureds still have to understand their policies and what is covered to know if cyber is included.

Cyber Insurance – shaping the product to fit the business

At 'Insurtech Insights' on 20 March 2024, Lucy Scott from Lockton stated that micro businesses 'simply could not comply with the level of security that was suddenly expected of them overnight if they were to purchase a cyber insurance policy' Lucy went on to explain that the insurance community has made good progress in making cyber insurance more accessible for those businesses, for example by offering affordable support with implementing the required tools.[16]

> **Despite the barriers and relatively low take up of cyber insurance, there are many ways to refine current and future cyber insurance solutions to help address the UK SME cyber insurance protection gap.**

Cyber is ultimately a discretionary purchase and so it is important to establish best practices in cyber security, whilst acknowledging that the SME can choose their own cover that's right for them based on what's available in the market at the time vs their needs and resources. Helping businesses reduce cyber risk and to prepare for business interruption is beneficial to both the insurer and the insured.

Commercial Combined Policies can be another way to tailor cover for SMEs, for example by combining professional indemnity (PI), technology and cyber cover. However, it is crucial to ensure the SME has enough coverage for each of the risks they face within these policies and that the crossovers between coverages are well designed.

Making exclusions work for the SME and the Insurer

Cyber insurance policies will have exclusions specific to the client and the risks faced and these can vary between policies.

The insurance market must communicate a breadth of possible and diverse exclusions to any prospective buyer so that they know exactly what they are covered for and specifically
what is excluded, in line with strict regulation.

The ABI publishes advisory notes for potential insureds describing the variety of insurance cover available, including exclusions to look out for and how to go about purchasing cover.[17]

[15] What does cyber insurance cover?
[16] Insurance Times, 24 March 2024
[17] https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/cyber-insurance/what-does-cyber-insurance-cover/

Challenges in providing SMEs with solutions to systemic incidents

SMEs require straightforward simple language to understand cyber risk and cyber coverage, yet it is challenging to address cyber risk in a simplistic way given the complexities of systemic risk involved.

The whole world is grappling with the unknown unknowns of large scale cyber events, as they begin and spread in seemingly random ways and can lead to outsized impacts beyond expectation. These evolving threats are not all insurable, and indeed should not be in many cases (in line with regulatory approaches). However, markets, regulators and commercial solution providers must work together to understand and reduce the risk of these threats becoming unmanageable and leaving victims without recourse.

So far, cyber insurance loss ratios have been relatively similar to other insurance lines, even if there is still uncertainty over potential losses and large claims events. Material published by the ABI in 2020 stated that: "one insurer reported a cyber loss ratio was in the region of 60%. This is in line with the ratios reported in motor (69%), income protection (53%) and property insurance (51%). Insurance for life and annuities and pensions have higher claims ratios (169% and 116% respectively)." 18 Loss ratio is the percentage of claims that an insurer receives in relation to the premiums earned. Despite the uncertainty around systemic risk, they indicate that cyber insurance is a profitable market.

See Appendix H: The FCA and PRA for further discussion of systemic incidents.

Cyber Insurance Supporting Supply Chain Risks

Many small businesses are in an organisational supply chain and may have weaker cyber security in place than the businesses to which they are providing services. Almost all of the UK's FTSE 100 businesses were exposed to supply chain breaches in the last year[19], and through these businesses, hundreds of SMEs suffered knock-on cyber impacts and losses. As larger organisations are increasingly required to enforce minimum cyber security standards from suppliers, many will seek evidence of security standards such as ISO 27001, CES+, and assurance that the supplier follows frameworks that keep systems up to date, regularly patched, and that their data is held securely and continuously monitored against attacks. These due diligence and supply chain risk assessments can provide assurance that the SME invests well in their own cyber risk management and will not pass vulnerabilities back into their customers' systems.

> **Investing in cyber insurance allows the SME to demonstrate its commitment to strong and improving business continuity standards.**

External cyber advice and guidance available to SMEs, brokers and insurers

Cyber risks are constantly evolving and present a challenge to insurers and brokers to "pin down". However, a wide variety of resources are available from a broad range of sources. These can be invaluable resources to SMEs, but also for insurers and brokers, to continue to learn about evolving threats and how to deal with them.

These sources will generally agree on high level concepts but may contain differences or indeed contradictory recommendations on more technical areas. There is no single source of comprehensive information targeted at SMEs. This could present an opportunity for the insurance industry to support and sponsor joined up guidance.

Many sources of free information, consultancy and guidance available on evolving cyber risks and risk mitigation techniques are listed in **Appendix G: External Cyber Advice and Guidance.**

In the financial sector, a major buyer of cyber insurance, the FCA has encouraged businesses, including SMEs, to develop healthy cyber security and resilience environments. All SMEs, but especially those operating in the financial sector, will almost certainly improve resilience from the implementation of effective cyber hygiene and the use of robust cyber insurance solutions.

For insurers themselves, the PRA will also obligate insurers to maintain their own appropriate and robust cyber security standards. In its "Insurance Supervision: 2025 priorities" letter[20] it stated that *"the cyber threat landscape facing the UK's financial system continues to evolve rapidly, and we view the ability of firms to detect, respond to and in particular recover from cyber-attacks to be a cornerstone of the financial system's resilience."*

Reference is made to multiple sources of regulation, guidance and governance in **Appendix H: The FCA and PRA.**

[18] The value of cyber insurance to the UK economy;
[19] Supply Chain Attack Haunt UK's FTSE 100;
[20] Insurance Supervision: 2025 priorities;

Proposal Forms

The process of selecting an appropriate policy and comparing them to determine the cover that each provides and what exclusions exist may be complex, overwhelming and potentially off-putting. Indeed, it may result in incomplete or inaccurate information being provided.

One SME made reference to a 54 page proposal form which they found extremely difficult to complete because of the modest size of their business, with limited resources available to commit to this exercise and their perception that cyber was a low risk to their business: was the effort worth the value of the service offered?

The nature of the risks faced by the SME, and thus the insurer, can be significant and potentially costly in a claim, and so it is understandable that the proposal form is a useful tool to assess the risk profile of the SME. However, **disproportionate complexity relative to the size of the SME business may be off-putting to a relatively unsophisticated buyer.**

Insurers highlight that given the potentially low profit per policy to the insurer for SMEs, putting resources to reducing lengthy proposal forms and to obtain adequate diligence about the business can be a challenge.

There is, however a trend of insurers and brokers using more online quotation systems with more accessible and much reduced proposal forms. **Use of technology and digitisation can significantly speed up the process of obtaining quotes.**

One insurer does not ask any cyber questions for SME proposals with a very small turnover (<1mnTO) if they have CES; they will ask a handful of questions for those with a moderate turnover and deploy a full questionnaire for those above a larger threshold.

> **The traditional insurance industry is being disrupted by the introduction of insurtech approaches, which offer customers more modern and accessible ways to conduct business, easing the burden and** improving the value of gathering information, executing contracts more efficiently, and analysing information more accurately.

The insurtech approach typically builds upon technologies such as AI, Data Analysis and the Internet of things (IoT). The latter allows for remote analysis and monitoring of systems such as factory production equipment used by the SME.

A number of commercial and bespoke “Digital Risk Quantification” (DQR) tools also exist to support cost evaluations of available solutions vs statistical risks presented by a business. For example, DRQ can allow the SME and the insurer to evaluate if implementing phishing protections would statistically reduce the SME’s risk a significant amount, especially compared to alternative available options such as a better firewall. These DRQ tools can allow insurers and brokers to use software and data models to evaluate the specific SME insured’s current and evolving risks and mitigants accurately and quickly.

Insurtech is changing the cyber security insurance industry by offering increased connectivity to all devices on an insured network using software “agents”, more personalised insurance products, full turnkey automation of the contracting process and use of AI and better data to allow for modelling of current and potential future risks.

One insurtech stated that they used over 1,000 data points and turned this into eight metrics to be used in underwriting. They stated that they have insight into many thousands of cyber loss cases allowing them to underwrite more accurately and faster. **They also deployed software on the insured’s computer systems so they could detect infrastructure changes and emerging risks and cyber-attacks, providing an up-to-date and potentially continuously updated risk profile of the SME.**

The underwriting process and getting better information

Insurers and brokers need better, more accurate and more up to date information. The insurance industry may need to evolve to accommodate this.

The underwriting process entails reviewing an insured’s risk profile, assessing their risks and identifying an insurance package offer that includes their required coverage.

In a time when cyber threats are constantly evolving, getting access to relevant cyber security incident data is difficult using traditional means. For an underwriter to write traditional policies for traditional risks (e.g. fire or flood) there is a long history of these types of incidents on which to formulate a model. As cyber risk is such a relatively new category, with constantly evolving threats and long tail impacts that continue to grow, the lack of comprehensive statistical data can make it significantly more difficult to formulate a model for SME cyber risks. What data there is may be out of date or incomplete as claims data is not fully shared by all insurers.

This lack of data is exacerbated by victims of cyber incidents who can often elect to cover up breaches or fail to report or share information on these events and their impacts, out of

concern for potential reputational impacts, except where they are mandated to by legislation, regulation, potential litigation or other specific requirements.

The lack of data is not simply due to the immaturity of the cyber insurance industry; it is also a product of the lack of information sharing, both between insurers and within the insurance industry.

Some insurers use CyberAcuView, which provides access to a repository of attacks and causes of loss, but it is not used by all insurers and will only be able to report on claims; clearly it cannot encapsulate breaches that are unreported.

> **The insurance market can develop and embrace more widely supported information sharing platforms to improve the effectiveness of the whole market. Innovations such as the ABI Cyber Market Data Collection, Cyber AcuView, and the Cyber Monitoring Centre should be actively promoted and encouraged.**

Systemic risk is also a growing area of concern and there has been a dramatic growth in supply chain attacks to reach the target. Insurers greatly benefit from understanding the nature of not only the potential insured, but also the ecosystem of third parties around it. They need to know this information and the possible effect of accumulation for consideration when underwriting risk.

A potentially more significant challenge to underwriting the risk is that even if more data were available, that data may quickly become out-of-date as a result of the changing nature of cyber risk.

The insurer and broker skills gap

Skills shortages equate to higher breach costs. The insurance industry must continue to invest in acquiring and training technical staff to address evolving needs. The UK government announced in January 2025 that more than 30 projects are to receive funding to deliver targeted support including training to boost cyber skills and new ways to protect businesses against cyber threats, which demonstrates the broader importance and commitment to tackling this issue.

SME insureds typically have fewer cyber security specialist skills in house compared to larger organisations. In Appendix F: Evaluating the Cost of Breaches, the “Skills Gap” section evaluates research that shows that breaches that take longer to resolve are typically more expensive. Lack of trained staff, prepared crisis plans and processes and access to dedicated technologies, has the result that an SME breach is typically more costly, per employee, than a cyber-attack in a larger business.

Insurers and brokers are challenged by a competitive market for experienced cyber insurance practitioners. Many have strong cyber teams in place, however, skills shortages limit availability and push up the cost of this expertise. The lack of cyber security professionals across the board and especially in brokers and SMEs will increase a lack of awareness of the risk SMEs face and their possible impacts.

Insurers and brokers can upskill their technical teams, where capacity allows for it, and stay abreast of the rapidly evolving technical requirements of the market, and the specific needs of the SMEs.

Making the claims management process better for all

The claims management process traditionally involves technical skills in manually reviewing each claim, loss-adjusting the incident, deciding what compensation to award and then remitting that compensation.

Cyber claims inherently require real-time response, and this is often the USP of the insurance product offering. To achieve this service for SMEs without creating a loss-making book is a significant challenge.

There is much room for technology use and innovation in the claims space to support development of a profitable SME line. Parametric or quasi parametric payout policies could remedy this, however, it can be equally challenging to find a ubiquitous parametric trigger. A binary, yes/no decision on whether a claim should be paid requires a trigger that anyone could agree with. For example, in aviation, if it rains on the airfield above X cm, the policy pays out. In cyber, there are many human made reasons that an outcome might be realised, if there's a certain cloud down time incurred there can be many different factors as to why it occurred as well as in built latency that makes the downtime unpredictable.

The immediate solutions to cyber claims management are not forthcoming and so the market must, and will continue to work to develop solutions for SMEs here.

Appendix B: Cyber Security – The Evolving Threat and How to Manage it

Drivers of Cyber Risk, and how exposed is the SME segment?

Why SMEs are a target for cyber-criminals

SMEs are a sweet spot for cyber criminals: the targets are plentiful, they have relatively low cyber security standards in place, and a cyber-attack is typically highly damaging due to the victim's inexperience in resisting and recovering from the attack. As a result, ransomware attacks in particular are lucrative. Surveys of UK businesses have reported that 59% of UK businesses that experienced a ransomware attack have paid the ransom[21], despite 66% having a policy in place not to pay. Although many business leaders are aware that paying a ransom spurs a growing industry of ransomware criminals, ransomware attacks continue to grow by double digits year on year.

The FSB reports that 72% of small businesses have experienced cyber-crime between January 2021 and January 2023[22].

Research shows that for larger organisations, business spend on cyber security is in the region of 0.2% to 0.9% of annual turnover23. Although equivalent information for SMEs was not available, relative investment in cyber security professionals, technologies and controls is much lower in micro and small enterprises and so the ease of successfully attacking SMEs is relatively higher.

The recent Hiscox Cyber Readiness Report 2024[24] shows more positive trends, noting that at least in the US, "on average, firms of any size spent 11% of their IT budgets on cyber security". It also notes: "Smaller firms continue to allocate a larger proportion of their budget to both IT in general and cyber security specifically".

The relatively lower level of cyber resilience in SMEs makes them attractive targets for hackers. Hackers are commercially minded and attracted to understand the nature of SMEs, how and where they deliver products and services, and the valuable role they play connecting other larger and smaller businesses together. For example, in extortion attacks, the criminal behaviour is driven by the amount of pain and disruption that can be inflicted upon a business from interruption to their typical ways of working and the knock-on impact on the chain of businesses above and below them.

> **Hackers may target email systems, production environments, logistics systems used to track deliveries, web-portals used to share material with customers, Point of Sale systems and customer databases.**
> **Any one of these attacks could cause catastrophic business interruptions to SMEs who don't have strong risk mitigants in place. An attack on the production capacity of an SME could result in the business collapsing due to lost business, legal obligations and reputation harm.**

The impact of attacks on SMEs

A cyber-attack on a smaller business can result in irrecoverable financial and operational harm, and quicker than many businesses might imagine. Marketing based on doom and gloom can be seen as heavy handed, however insurers and brokers are well positioned to communicate realistic scenarios and risks to SME buyers who might not be aware of the challenges of a cyber event.

> **60% of small businesses suffering a breach/successful attack go out of business within six months[25].**
>
> **81% of all UK businesses who suffer from a cyber-attack are small to medium businesses and the cost to UK businesses overall is estimated to be £27 billion per annum[26].**

[21] Over Half of Hacked UK Firms Pay Ransom;
[22] Cracking the Case, FSB, December 2023;
[23] Financial services firms spend;
[24] Cyber Readiness Report 2024;
[25] Is your front door open;
[26] UK Cybercrime Statistics 2025;

Research by Sky Business[27] reports that most UK SME business decision makers estimate they would be forced to stop trading for an average of four days following a cyber-attack. 8% of businesses who have not been victims think an offline period would last eight days or longer compared to 24% of those who have experienced one before. This suggests that businesses underestimate the impact. The research also notes that micro businesses (those with 1-9 employees) were more likely to underestimate the impact of a cyber-attack on their business, with 29% saying an attack would not cause their business to close. Only 10% of medium businesses (with 100-249 employees) said an attack would not cause business closure.

SMEs are proportionally more at risk from cyber incidents compared to larger organisations, with research showing the average cost of a breach, per employee in the business, is around four times higher for an SME than a larger business[28]. "Appendix F: Evaluating the Cost of Breaches" provides additional detail on the research conducted for this report into the cost of a breach on a UK SME.

The typical impacts on an SME include:

- Business interruptions - due to external supply chain breaches or attacks.
- Loss of sensitive corporate / client information and resulting liabilities.
- Physical damage caused by damage to production equipment and computer systems.
- Privacy breaches including loss, theft or unauthorised disclosure of Personally Identifiable Information (PII).

These impacts can cause knock-on issues such as:

- System downtime leading to business interruption – this can stop or slow down production from either the SME's own systems or those of a critical supplier or customer.
- Intellectual property (IP) – threat actors may steal commercially sensitive information including plans and product designs and use ransomware to hold them hostage, or just publish them publicly. Small businesses such as law firms, with disproportionately high value IP, are a favoured target.
- Crime – fraudulently intercepting or creating payments made by the SME can lead to financial loss (known as "Payment Diversion" and "Business Email Compromise" scams).
- Data breaches and loss of Personally Identifiable information belonging to private individuals, e.g. customers and employees, can lead to the Information Commissioner's Office fining an SME significant sums. Other regulatory and litigation risks can follow.

Smaller businesses that have not engineered sophisticated cyber security solutions, backup systems and business continuity protocols, may find themselves severely damaged by a cyber-attack. They often lack experts in the business with the experience of dealing with sophisticated cyber-attacks, and senior management may find themselves distracted from day to day operations while dealing with the crisis. Business interruption and brand damage may result in the business being unable to recover from the attack.

Cyber insurance solutions aimed at SMEs typically fold in resources including cyber incident handlers, legal resources, reputation management and access to cyber security experts. These are invaluable resources that could be the difference between the SME surviving an incident, or it going out of business entirely.

The rising threat

It is well recognised that cyber-attacks are on the increase year on year and it is now a case of 'when' an attack happens and not 'if' it happens. Cyber threat actors can be expected to continue to improve their methods of attack, especially by leveraging. AI. Emerging technology can lower the barrier to automate attacks, find vulnerabilities, exploit weak passwords and known bugs in systems and draft more realistic, automated phishing emails. These developments will impact any estimates of frequency and severity based on historical cyber-attacks, potentially making insurer industry models outdated.

Protection, detection and response cyber security technology and procedures are also constantly evolving, making it extremely difficult to quantify the effectiveness of different protective measures. Insurers need to be kept abreast of the constant "cat and mouse" of threat actors and responders' skills.

[27] SMEs miscalculate the cost of cyber-attacks on their business;

[28] Cyber Security Breaches Survey 2019;

Some indicators of this are listed below:

> **The UK National Cyber Security Centre's (NCSC) Annual Review 2024[29] observes year on year increases in incidents they handle, with a trend in "highly significant and significant" incidents, and increasing numbers resulting in exfiltration i.e. theft of data from the business.**

The list of "Common Vulnerabilities and Exposures", an industry wide catalogue of cyber vulnerabilities, details around 44,000 vulnerabilities identified in 2024, a 30% increase from 2023. Many of these are new, "zero day" attacks with a classification of "critical", meaning that there was, at the time, no security defence available[30].

The Allianz Risk Barometer 2024[31] surveys over three thousand respondents across the world. It has consistently reported for some years that the top two risks in the UK were:

- Cyber incidents (e.g., cyber-crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties); and
- Business interruption (including supply chain disruption).

For smaller companies (those with an annual revenue of less than $250 Million), these two risks were rated #1 and #3.

AXA reported 'Cyber Security Risks' and 'Risks Related to AI (Artificial Intelligence) and Big Data' as their #2 and #4 top risks[32].

The Federation of Small Business (FSB) reports that phishing is the most frequently reported cyber-crime for small businesses, at 92%[33], with the NCSC noting that "Ransomware attacks continue to pose the most immediate and disruptive threat" to many businesses[34].

The DSIT Cyber Security Breaches Survey 202435 lists the **most common attacks against SMEs as:**

- DOS (denial of service) attacks - to restrict network access to legitimate users
- Home / remote working compromise - with possible lack of corporate security controls in place which may be present in the office
- Ransomware attacks - preventing access to corporate systems until a ransom is paid (with maybe still no access, even if ransom is paid).
- Supply chain compromises

Cyber threats continue to evolve on an hourly basis, and the number of SMEs representing UK PLC make them one of the most vulnerable commercial groups. These businesses are generally less cyber resilient and less able to recover from a cyber-attack, and can benefit from the solutions cyber insurance offers.

Underestimating the risk

Cyber-attackers are attempting to probe for vulnerabilities in every SME in the UK. A successful attack will have a high probability of permanently destroying the business due to limited resources to identify and remediate from it.

The UK government states that "the NCSC believe that the severity of the risk facing the UK is – widely – underestimated by organisations from all sectors[36]."

Yet many SMEs do not believe that they will succumb to a cyber-attack. Reasons given include:

- We have Cyber Essentials so we are protected.
- None of the SMEs that we work with have been subject to a cyber-attack.
- It only happens to large organisations.
- We have good cyber security in place and so do not need cyber insurance.
- We have outsourced IT and cyber security is an IT issue, and we have the outsourcer doing cyber security.

Some SMEs have problems engaging with senior management on cyber security issues. This is exacerbated by some executive boards, senior management and other stakeholders not having a cyber security practitioner available to explain cyber security risks and impacts.

[29] Annual Review 2024;
[30] 2024 Midyear Threat Landscape Review;.
[31] Allianz Risk Barometer;
[32] Future Risks Report 2023, 10th Edition;
[33] Cracking the Case, FSB, December 2023;
[34] NCSC Annual Review 2024;
[35] Cyber security breaches survey 2024, Department for Science, Innovation and Technology, 9 April 2024;
[36] Annual Review 2024;

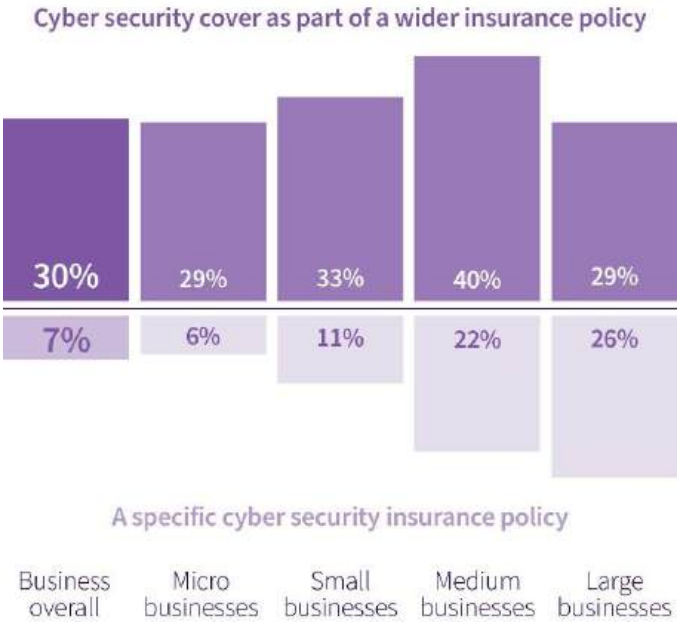
Leaving cyber to IT, or outsourcing IT operations to a third party is not the same as engaging with cyber risk issues, and IT teams may not have cyber skills. The business and its leaders will still be liable for its operational resilience.

Smaller businesses on average, invest less in cyber security compared to larger businesses. The Allianz Risk Barometer 2024 calls out SMEs as being "much less likely to have mitigating measures in place" They tend to overlook, underestimate or are less conscious of cyber security risks and are less well prepared to deal with them. Many SMEs lack dedicated cyber security staff and sophisticated threat detection systems. Too few have access to the resources available to them in cyber insurance solutions.

The DSIT Cyber Security Breaches Survey 2023[37] comments on the lower take-up of cyber insurance and lower cyber skills in SMEs compared to larger businesses, noting

"This may reflect the idea that medium businesses tend to have more resources than smaller businesses to be able to afford insurance, while possibly **not having the skills or tools to be able to address all cyber security risks internally** like larger businesses."

DSIT Survey 2023

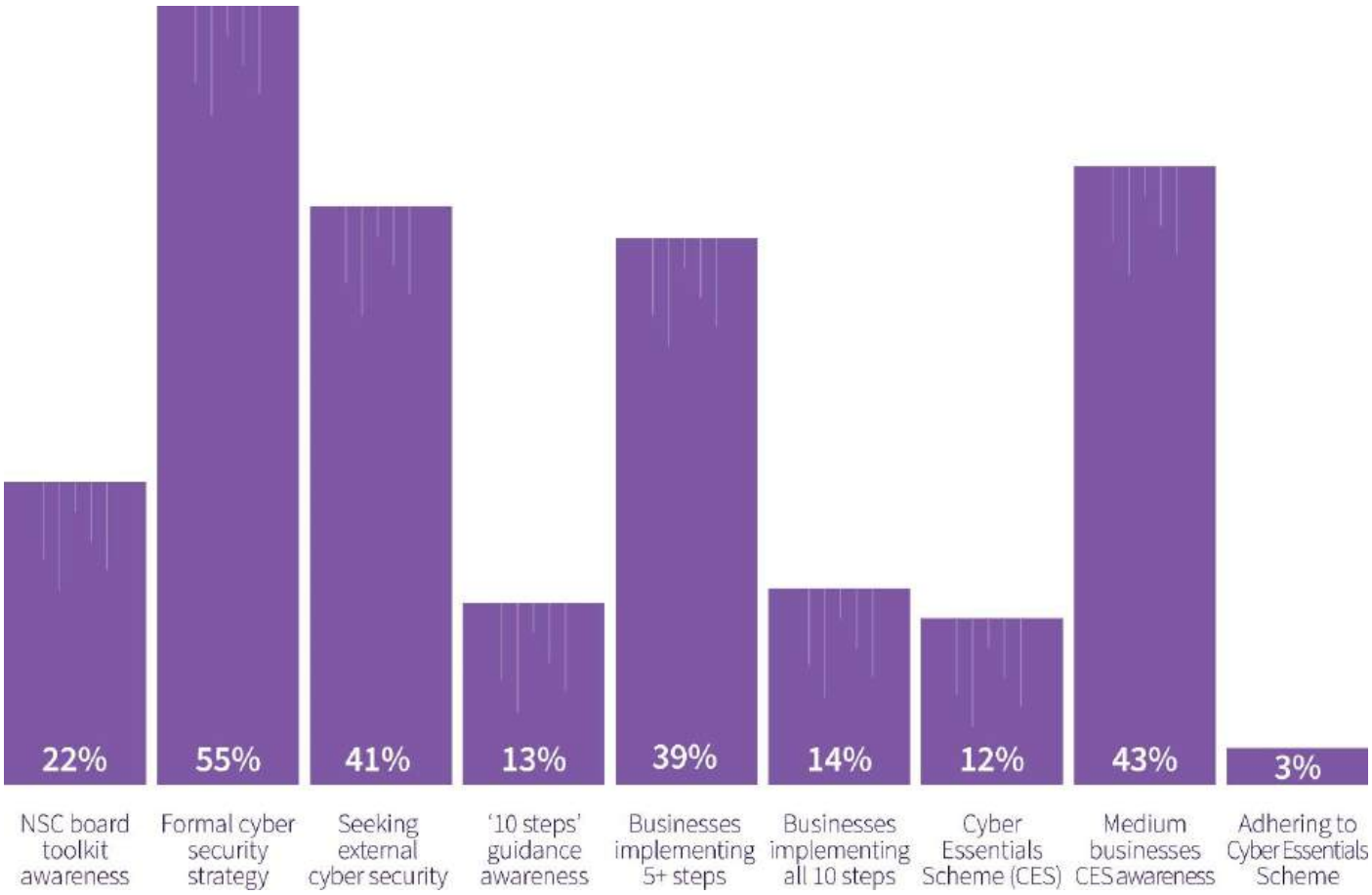


The DSIT Cyber Security Breaches Survey 2024[38] highlights the risks of lower cyber investment in SMEs:

"Qualitative data shows a similar set of issues to previous years that prevent boards from engaging more in cyber security, including a lack of knowledge, training and time. It also highlights a contrast between more structured board engagement in larger organisations, compared with **more informal approaches in smaller organisations**, where responsibility was often passed onto external contractors."[39]

[37] Cyber security breaches survey 2023;
[38] Cyber security breaches survey 2024, Department for Science, Innovation and Technology, 9 April 2024;
[39] Cyber security breaches survey 2024;

The illustration below shows the relatively low awareness and implementation of common cyber risk strategies in smaller businesses[40].



[40] Cyber security breaches survey 2024, Department for Science, Innovation and Technology, 9 April 2024;

SMEs might not be aware that Microsoft describes Multi-Factor Authentication (MFA) as "one simple action you can take to prevent 99.9% of attacks on your accounts". This simple technique requires users to log in with two forms of information, such as a password and a code sent to the user's phone. The IBM 'Cost of Breaches Report, 2024' further notes preparing and testing an incident response plan is one of the best investments a business can make to improve their cyber security and training staff is also particularly cost effective. Insurers have a great opportunity to share this kind of knowledge and expertise with SMEs and potentially improve cyber hygiene and prevent losses, as well as bolstering the commercial value and take-up of the product.

Research from insurer Cowbell indicated potential over-confidence and under-preparedness in SMEs:

77% of surveyed UK SMEs do not have any **in-house security.**

32% of CEOs were confident a **cyber-attack** would not impact their ability to do business.

10% of all business leaders said they do not need to improve their position regarding **cyber risk.**

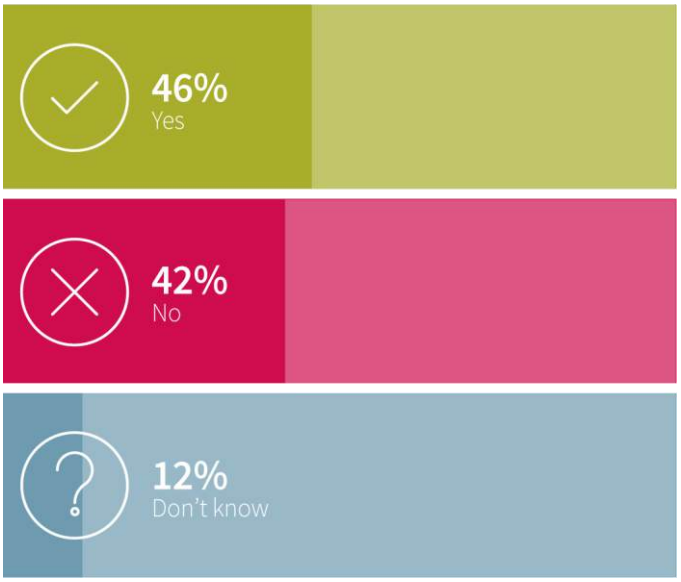
87% did not consider **reputational damage** as a significant risk to business (although it should be noted that the IBM 'Cost of Breaches Report' 2024 disputes this[41])

Grant Thornton surveyed SME businesses about their current, perceived and aspirational readiness for cyber risks. The surveys spanned a number of stakeholders responsible for Cyber Risk in their business. Most respondents were small and medium businesses, and generally the role of the cyber security stakeholder was the CFO.

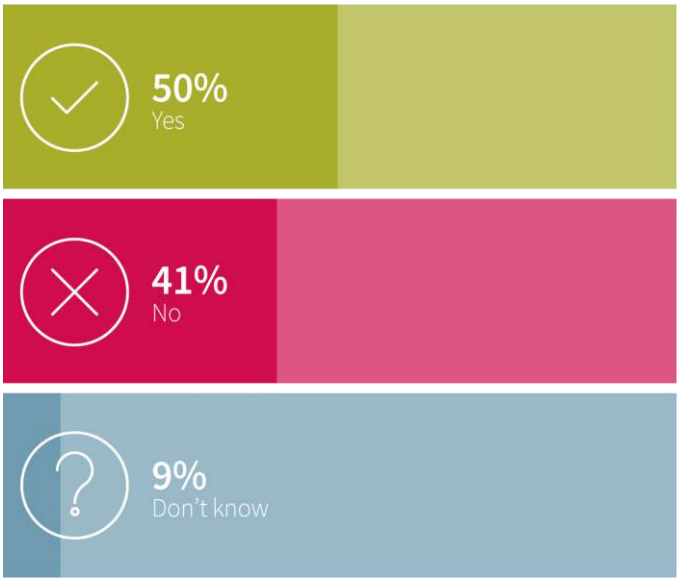
Over half of the businesses did "not feel that confident" in "the quality of the business continuity arrangements and data and cyber strategies" of the business, although the confidence increased with organisational size.

[41] Cost of a data breach 2024 | IBM

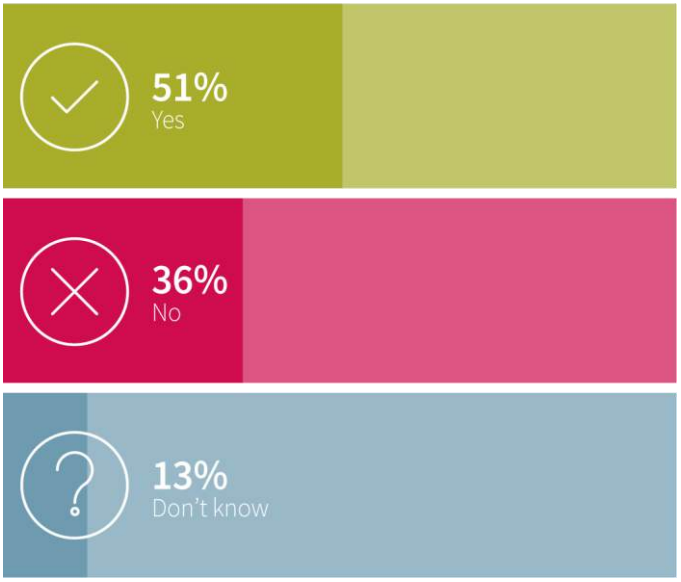
Have you implemented and incedent response plan for a data breach?



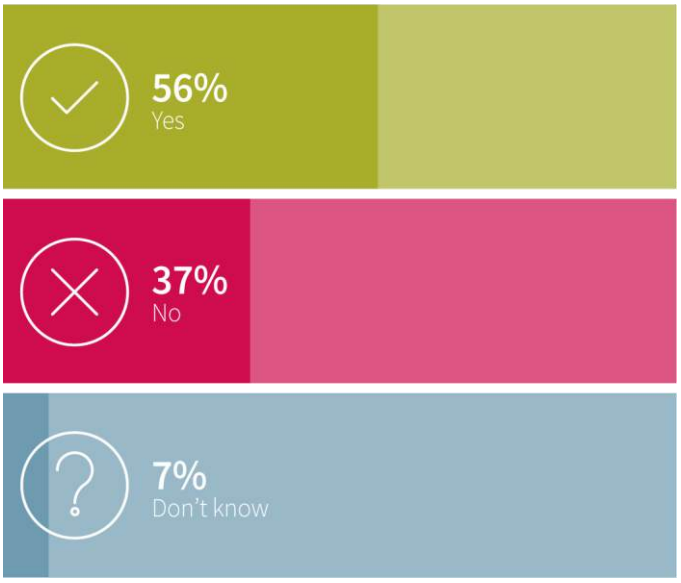
Do you provide training for your people on data security?



Do you monitor regularly for cyber/data threats?



Do you provide training for your people on cyber security?



The ability of your security processes and tools to detect and prevent data breaches

The quality of your business continuity arrangements and data and cyber strategies will allow you to respond efficiently following a cyber-atytack/datya breach

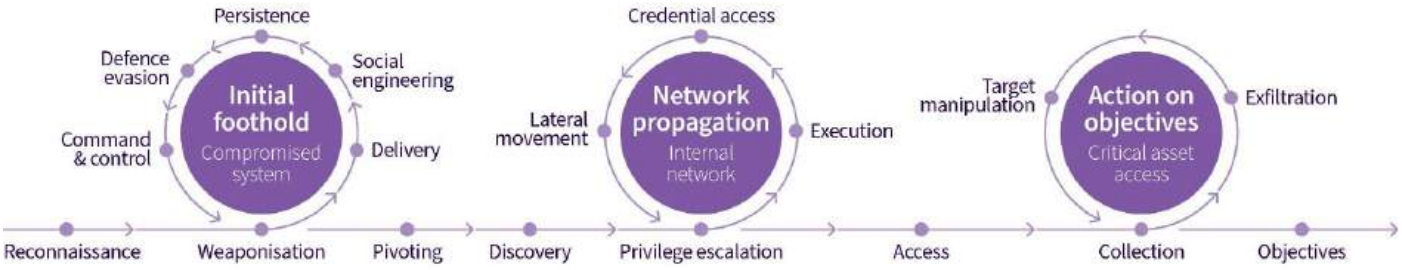
Your ability to effectively manage a change in customer service and staff demands following a cyber attack/data breach

You have effective systems and channels in place to enable you to notify governing bodies and customers within 72 hours following a cyber-attack/data breach

The "Cyber Kill Chain[42]" is a widely used method of understanding and communicating the typical phases of a cyber-attack. A common flow is:

1. The threat actor will take advantage of a phishing vulnerability to compromise the email system of a business, perhaps through social engineering and identity/password theft.
2. This can allow the attacker to "migrate" to other parts of the business, rapidly identifying the "crown jewels", which is the data held by the business that is likely to create the most harm or value, and leverage for the criminals.
3. The hackers will then commonly exfiltrate, i.e. steal the data, and they will often simultaneously encrypt the victim's data to make it unusable without access to a decryption key (which may or may not work).
4. They will commonly destroy backups in this process, if they can be readily identified within the computer environment. This improves their bargaining power.
5. Finally, the hackers will trigger their ransom demand process.

   The ransom will typically force the victim to contemplate paying it, or potentially expose themselves to prolonged business interruption whilst they attempt to remove the criminal's damage from the business, restore from backups and restore functionality to their environment. Even if a ransom is paid, restoration of the system can take days or weeks and is sometimes not possible where data has been damaged.



Choosing to pay a ransom may, in the best case scenario, also allow the victim to "control the message", by encouraging the criminal to destroy copies of the data they have stolen, and allowing the business to return to 'normal'; however it's vital to acknowledge that there is no obligation on the criminal to do so. Insurers will not advise on whether to pay a ransom in the UK; for more information about how businesses can respond in a ransom event, the ABI's work with the UK Government and CRI offers pragmatic support[43].

Other impacts may persist, including the threat of "double and triple dipping", where the criminals attack again, or guide other hackers to get access to the SME's systems. They may also cause additional harm by selling the victim's data on dark-web data markets for additional profit.

Some have even reported threat actors proactively "tipping off" regulators and other parties about the breach to cause further damage, or to gain further leverage over the victim[44].

> **Cyber insurance can help shorten or break the stages of the "kill chain", dramatically reducing the cost and impact of a cyber event.**

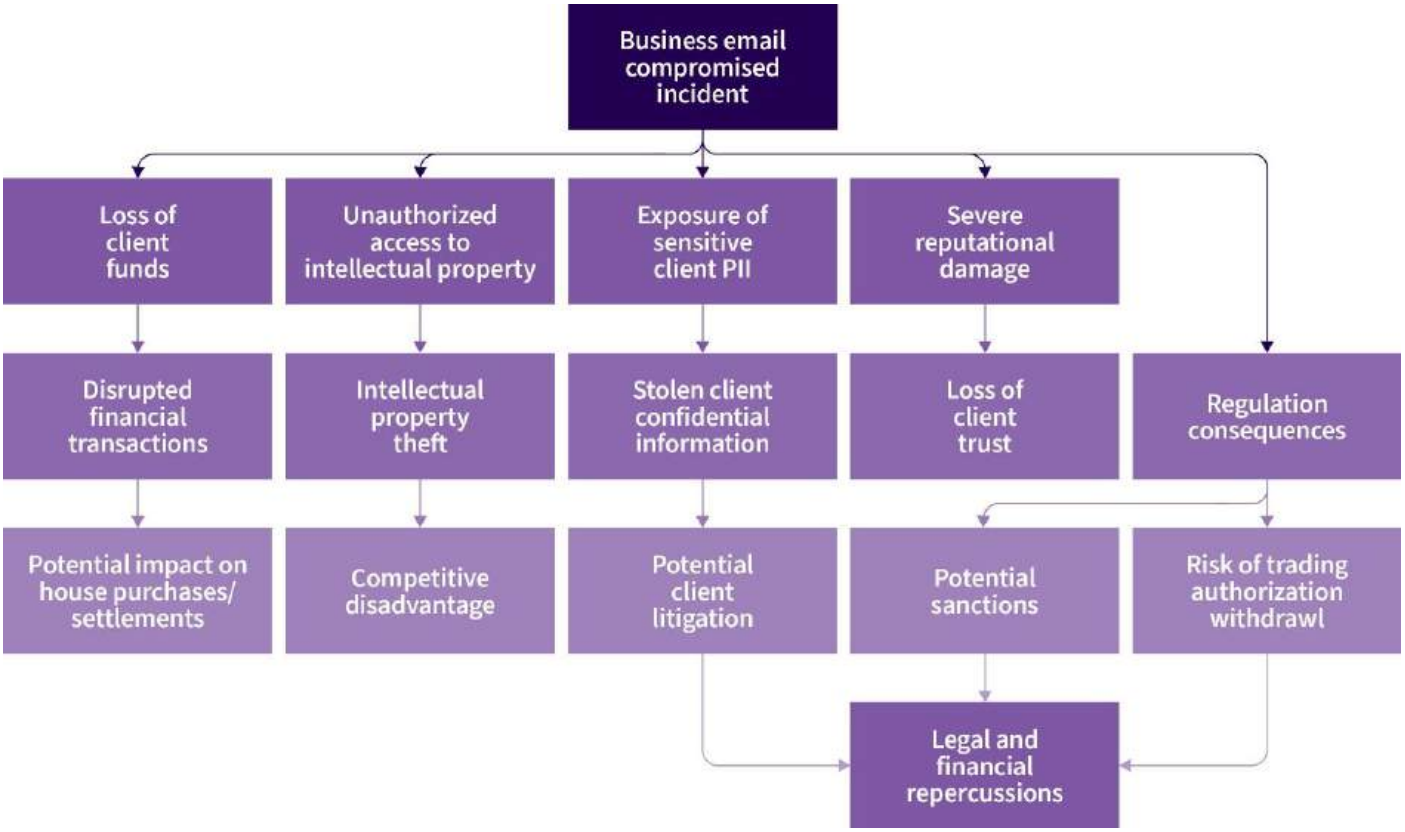
Insurance solutions such as crisis management, PR/communications management, regulatory reporting support and cyber incident investigation can all dramatically reduce the impact and the interruption on the business. Remediation services provided by the insurer will also support the SME in getting back to an operational state by rebuilding damaged systems; these value-add solutions alone can save the victim days or weeks of down-time and cost.

[42] Wikipedia;
[43] CRI guidance for organisations during ransomware incidents;
[44] Hackers blow regulatory whistle over data breach;

Case Study: A small solicitors business in the UK could see impacts such as:

- Loss of client funds caused by a Business Email Compromise i.e. a fraudulent email instructing payment to be sent to the attacker's bank account and not the client.
- The attackers gain access to valuable intellectual property and confidential commercial information.
- Attackers access sensitive Personally Identifiable Information (PII) such as onboarding / know your customer (KYC) records and banking details.
- Knock-on impacts on transactions such as a house purchase that was intended to be completed with those funds.
- Loss of goodwill and trust in the business.
- Potential for regulatory sanctions or even loss of trading authorisation by the Solicitors Regulation Authority.
- The business could be sued by its customers and other impacted third parties.

What does an SME cyber-attack look like?



Regulatory investigations

Government and regulators are continuously raising the bar for mandatory cyber hygiene expectations standards and reporting obligations if businesses suffer a cyber-attack, as technology adoption evolves. There is also a growing trend of legal class-actions in the UK against businesses that have under-invested in cyber resilience, and SMEs are a heavy focus. Insurers can support SMEs in staying abreast of their evolving compliance risks.

UK regulators are not shy to call out SMEs for failure to secure themselves against cyber-attacks; however, they generally don't "name and shame" businesses that have suffered cyber-attacks. In other jurisdictions such as the US this type of public reporting is more common and has driven the development of data privacy laws and the creation of the cyber insurance market. While naming and shaming may not be the best approach on its own to increase security, it does drive a certain level of awareness that supports investment.

The UK Information Commissioner's Office (ICO) requires businesses to notify them "of a breach if it is likely to result in a risk to the rights and freedoms of individuals. If left unaddressed such a breach is likely to have a significant detrimental effect on individuals.[45]" This requires a qualitative judgement from the business, as well as to make sure that the business is within the 72 hour reporting timeframe.

SMEs have been called out for failures in securing client, customer and employee data especially in sectors such as banking, high street mortgage brokers, doctors and lawyers. A recent example was a cyber-attack on a UK SME solicitor's firm. The business was issued with a £98,000 fine by the ICO after they fell victim to a cyber-attack. The ICO observed that "a lack of sufficient technical and organisational measures gave the attacker a weakness to exploit"[46].

The ICO does not consider payment of a ransomware fine as a mitigating action, though they have officially said they will look favourably on those reporting incidents to the authorities such as the NCSC.

When the regulators are investigating businesses that have suffered a reportable cyber incident to establish if it warrants a monetary fine or other sanction, they will often assess the business's cyber resilience posture, management engagement with data and cyber issues, and if the business has invested in good cyber risk mitigation strategies.

> **Regulators such as the FCA continue to evolve their stance on cyber resilience and proactive risk management is being expected of SMEs and increasingly needs to be evidenced. Cyber insurance is often regarded as an indicator of a 'healthy and forward-looking' business.**

Are SMEs reporting attacks?

> **SMEs are one of the most attacked market segments in the UK, but only 34% of businesses report their most disruptive breaches outside the business, other than to their IT service provider[47].**

Insurer driven solutions can aid in visibility of the number and nature of breaches impacting SMEs in the UK and many policies will require the insured to report their incidents. This can allow insurers to craft solutions better suited to the evolving market, and specifically for that insured.

Insurance cannot, however, be used to enforce cyber incident reporting. Government can encourage development of imperatives and motivations for SMEs to report promptly and accurately, and this pressure may come from multiple regulatory and legislative levers, for example the Cyber Security Resilience Bill[48].

Statistical modelling of reported incident data is essential in supporting commerciality of insurance solutions, underwriting effectiveness and improving loss ratios. The current regulatory environment clearly results in significantly under-reported losses and claims in the SME segment.

[45] Personal data breaches;
[46] Monetary Penalty Notice;
[47] Cyber security breaches survey 2024, Department for Science, Innovation and Technology, 9 April 2024;
[48] Cyber Security and Resilience Bill;

Appendix C: Detailed Recommendations for Government, Insurers, and Brokers, to Address Barriers and Grow the SME Segment

Government

The UK government and industry regulators are placing significant emphasis on ensuring a resilient UK PLC via cyber, as an important step towards UK growth and competitiveness. There is a need to embed minimum standards of hygiene, governance, financial and commercial resilience and to raise the bar on expectations of cyber hygiene and education for businesses in the UK. Insurance provides a commercial solution to mitigating some of the risks that businesses face; however, insurance is not a replacement for state-sponsored protection for vulnerable UK businesses and citizens. Insurance is a voluntary purchase and can support resilience; it is not a proxy for regulation or legislation.

Finding Relevant Cyber Security Information

There are multiple sources of highly credible cyber security information available from government, such as the NCSC Board Toolkit and Cyber Essentials. However, an SME needs to know what is appropriate to their needs and where to find it. There currently is no consistent and concerted 'push' source of information communicating cyber risks and impacts to SMEs in a harmonised and comprehensive manner from a single 'golden source'.

> **We support the FSB, which states: "We propose that governments across the UK raise awareness through key stakeholder bodies on cyber risk and signpost to relevant information.[49]"**

More Centralised and Joined-up Information Sources

The NCSC provides commendable and pragmatic advice for different sized businesses; however, **more clearly accessible, centralised, widely recognised government advice for businesses of certain sizes is needed. This could include more direct messaging to educate SMEs about the cyber risks they face, and the available remediation strategies, including cyber hygiene and cyber insurance.** The 'Cyber Security Breaches Survey 2024' shows many are not sure where to go for advice, so improving the range of curated SME cyber security advice available would help SMEs know where to look and who is the authority on cyber security advice.

Government departments could consider a joined-up approach in collaboration with insurers, brokers, professional and trade bodies and other organisations. This should repeat the same themes, terminology, and guidance, to reinforce, align and prevent confusion over what best practice is. Working together can help ensure that appropriate cyber risk management is in place to prevent and protect UK PLC from the effects of cyber-attacks and breaches.

Finding the right messaging to the largest possible audience will remain a challenge, and that is why multiple joined stakeholder approaches is beneficial. Some SMEs find that the information provided by government is too technology focussed. They feel it could be more business focussed as the business owns the risk, not the IT Department, and the business should be able to understand and commercially assess its own risks. However, this view is of course challenged by the constantly evolving and complex nature of cyber risks. Other SMEs are concerned that they don't have enough technical information available to them in an accessible and actionable form.

Advertising and Awareness Campaigns

Government could consider a sustained knowledge and advertising campaign to encourage all businesses, and especially SMEs, to implement an appropriate level of cyber hygiene. This could cover multiple communication channels and be ongoing. The current 'pull' model where businesses must seek this advice from government sources could be replaced by a more proactive 'push' outreach campaign.

Awareness and marketing campaigns can articulate and quantify the impacts of a cyber breach and practical steps to mitigate them, going beyond just financial loss. Impacts include issues such as regulatory fines, reputational loss, loss of production, lost productivity and employment, mental health issues and all other possible consequences of a breach.

[49] Paying a premium?;

Speed of Change

There has been some criticism from some respondents about the speed of change within government for guidance not keeping up with the evolving threat landscape. One specific case mentioned is the slowness of the NCSC response to moving from *passwords* to *passphrases*, which reinforces stronger authentication.

> **It is essential for insurers and brokers to be able to access, and to then provide SMEs with contemporaneous and helpful information to address evolving cyber risks and to be up-to-date and relevant in their advice. This must be reflected by credible easily accessible government guidance on basic good practices.**

Insurers and brokers regularly hold webinars and podcasts providing updates and accessible information about evolving cyber threats and mitigations; feedback from SMEs is very positive on these marketing approaches and they can and do weave in government messaging.

Raising SME Minimum Standards

> **There could be a concerted governmental push to get SMEs to implement CES, CES+ or equivalent as a basic minimum standard of cyber hygiene that includes socio-technical and recovery standards. The cost of government certifications and audits could be adjusted or subsidised for SMEs to make it affordable for all.**

Funding, grants, and free or low-cost consultation are available in some forms and are encouraged and this could be enhanced and increased.

The NSCS recommends the use of their "Cyber Assessment Framework[50]" (CAF), audited by independent "Cyber Resilience Audit" suppliers. The insurance industry could work closely with these and other cyber security professionals to help promote the value of insurance as part of a multi-faceted risk-mitigation framework. See Appendix D for further information on CAF.

Additionally, many industries operate in an environment that would mandate more stringent technical and organisational measures than many SMEs, and larger businesses, currently implement. Example SMEs include medical practises and law firms. Insurers may be able to offer targeted marketing campaigns to these valuable and vulnerable businesses and reinforce government messages on basic standards too.

Baseline Security for Government Suppliers

CES or equivalent is currently a required minimum to provide services to UK government. Suppliers of products and services to government are encouraged to, and could be more strongly obligated to carry a minimum baseline of cyber security and risk mitigation capability. These efforts can be amplified and increased across more SMEs.

This could include a minimum baseline of holding a similar qualification as CES for the smallest businesses, and CES+ for slightly larger SMEs, with associated testing and resilience and additional socio-technical and recovery capabilities.

Implementation of cyber insurance by a business Can be (and often is) viewed as an indicator that it has a more mature attitude to cyber security and resilience, and it may be valuable to include it as a risk management solution in the NCSC's list of 39 "Indicators of Good Practice". See "Appendix G: External Cyber Advice and Guidance" for further information on CAF and the IGPs.

Approved Cyber Suppliers

Government could publish a list of organisations and resources that could assist SMEs to improve cyber hygiene, whether by government agencies or approved businesses.

The NCSC publishes a list of cyber consultancies that directs businesses at for consultancy[51] and 30 CAF assured suppliers[52]; there is limited choice for SMEs needing advice and guidance. More suppliers could be encouraged into this scheme to increase bandwidth of resources.

Promoting Grants and Financial Support

Government could consider promoting the availability of more grants and other financial incentives to implement cyber security for SMEs, specifically ensuring that a minimum baseline to a CES+ style standard is implemented. This could expand the current more limited NCSC grants to a wider pool, including SMEs.

Appendix G in this report, "External Cyber Advice and Guidance" details free funded cyber security sessions offered by the NCSC to support small business with implementation, and skills development. These are helpful but are currently limited in scope.

[50] Cyber Assessment Framework;
[51] Cyber Advisor;
[52] CAF assured suppliers;

Bank lenders might also factor in cyber resilience when considering offering SME loans, as ultimately a resilient business offers more secure returns. Additional measures of SME resilience are also more likely to be welcomed in the current environment of constricted SME lending in the UK. The Allianz product, BBVA Allianz Cyber insurance is advertised during the online bank loan application processes in Spain, so there is a bit of industry practice around this.

The Skills Gap

In 2025, the government has announced new regional skills projects[53]. More than 30 projects will help protect the security of the UK's digital economy and grow a pipeline of cyber talent, supporting the government's Plan for Change. Students will be put through their paces in the latest round of Cyber Explorers competition to encourage the UK's brightest young minds into careers in the field.

Government is already considering national and academic campaigns for cyber security careers, promoting the value of cyber professionals to help address the identified skills gap. It could also consider mandating cyber security training for all government funded entities, ensuring that training is undertaken to address the issue that many cyber incidents are caused by human error. Mandatory training will reduce this risk.

Industry Intelligence

> **The NCSC provides threat intelligence via, amongst other outlets; the 'Early Warning' web page, which states that it covers 'any organisation with a UK-based website'[54]. Government can continue to develop ways to safely share this data publicly to support an accurate view of risk and resilience and expand its intelligence picture and share where possible.**

Incident Reporting

> **Government should incentivise and encourage incident reporting and robust ways to receive, process and benefit from the insights of this capability, sharing insights publicly where appropriate.**

While insurance can support (and in some cases does require) reporting to the authorities, external/public reporting of breaches and attacks remains relatively uncommon outside of regulated industries and government must be the one to encourage an increase.

Breach Notification

Government could make mandatory breach notification data available to the insurance industry. The ICO already publishes its data breach data, which the ABI was instrumental in securing. This kind of information sharing could be expanded and developed. Greater understanding of data breaches will assist in establishing risk postures and possible remediation strategies, including cyber insurance and its value to UK businesses.

It has been observed in other jurisdictions and industry sectors that "naming and shaming" often has the opposite to the intended goals, causing businesses to hide information about breaches, potentially distorting views of cyber resilience. However, anonymised breach information will benefit the entire market of businesses and the insurance industry.

The Regulators and Evolving Legislation

Regulatory certainty and consistency should always remain the goal across jurisdictions, to support SME compliance.

The ICO could be encouraged to promote cyber insurance as a valuable cyber security control. The ICO website has cyber security advice available, however, it makes very limited reference to the cyber insurance industry. ICO breach investigations tend to regard cyber insurance and associated risk management as possible valuable mitigation in the event of a cyber-attack, lowering or avoiding the need for a fine for a data breach.

Embedding Cyber Governance Code of Practice

The proposed 'Cyber Governance Code of Practice' was launched on 15 May 2024, as 'new voluntary codes of practice for consultation'. Consideration could be given to make this mandatory and include a reference to the benefits of cyber insurance as part of risk management. These codes are difficult for the insurance industry to apply until they have been tried and tested and are embedded practices.

[53] Regional Skills Projects;

[54] Active Cyber Defence;

Insurer Recommendations

The cyber insurance market has been challenged in recent years by the significant increases in cyber threats such as ransomware, and it has responded proactively. The industry has made available significant pricing reductions for some sectors, expanded policy coverage for risks such as supply chain interruption following pressure from the market to cover them, especially following recent systemic cyber events. It has continuously evolved in its cyber expertise to provide coverage even where underwriting information and claims history may not be as developed as in more long-standing lines.

> **Collaboration is essential to addressing the protection gap. Despite ongoing efforts to grow the SME cyber insurance product offering, uptake is still relatively low in the UK. Estimates of take-up vary between approximately 10%-15%. Insurance approaches alone aren't enough to attract SMEs to market, however, there are meaningful actions that insurers can take to support market growth based on best practices.**

The insurance industry continues to demonstrate strength in tackling relatively new and emerging risk, and further insurance focused recommendations are given to grow the SME cyber segment, below.

The Need to Support Different Types of Insurers

One interviewee classified insurers into three types:

1. Traditional insurers who have not entered the cyber market, preferring to sell traditional categories that they have extensive experience in selling.

- Financial Line Insurers who cover a broad spectrum of professional and financial risk and will sell cyber insurance to large clients.

2. Insurtechs who are often private equity backed with aggressive growth targets. These firms are often cyber mono line insurers who have been borne out of technology expertise in areas such as AI, Big Data, the Internet of Things (IoT), mobile apps, Blockchain, or the defence space, to secure transactions and utilise virtual assistants (Chatbots) etc. The adoption of these technology driven solutions can improve customer experience, enhance efficiency, increase real time information relating to risks faced by the insured, and lower costs of managing policies. These approaches make insurtechs often more innovative than the more traditional insurance firms, allowing for new products and ideas to be developed, and to improve accuracy within the cyber insurance lifecycle. These firms may not hold the same capital base or be regulated in the same way as a traditional insurer and so can be more volatile.

Encouraging a Standardised Lexicon

Cyber insurance varies in terms of the types of coverage, exclusions and conditions found in different standalone policies. This indicates a healthy and competitive growing market. However, as with any fairly new area of risk, the basic terminology and market consensus on the underlying probability of events occurring, as well as legal precedence for coverage is still evolving. This is especially true for SMEs where there is lower penetration, less insurance in place, and less reporting data available. Essentially there are many unknown unknowns at this stage of the market growth.

Some SMEs found that inconsistent terminology is confusing for potential buyers – particularly SMEs – making it especially difficult to compare different policies, coverage and exclusions.

Brokers also highlight that this lack of understanding is a significant obstacle and can even make it challenging to sell cyber insurance.

To add to the complexity, it takes a high degree of specialist skill to write cyber policy wordings. This skill set is a scarce commodity given the cyber skills shortages and niche technical knowledge of a cyber legal expert who also has an insurance specialism.

> **SMEs indicate that moves to standardised terminology, even when products can differ commercially, will greatly assist in evaluating policies. This will also allow underwriters and brokers to better communicate the different value propositions between competing products.**

There have been excellent efforts made by the industry. Aviva is one example of an insurer who has rolled out an SME policy, with a broad range of cover, streamlined on-boarding, and plain English language, making coverage easy to understand for brokers and clients. This approach addresses the SME with a higher turnover than most small and micro-SMEs. Similarly, the banking industry has spearheaded campaigns such as Crystal Marks and are currently proactively "de-complexing" many of their onboarding documents.

Other examples are the Lloyds model wording for certain exclusions and requirements for cyber insurance55, and work by the ABI and Lloyds on the 'Components of a Major Cyber Event: A (Re)Insurance Approach'56which explains differences in language such as named perils vs causation-based language. The goal of that document is to help establish clear definitions and underlying technical terminology, setting out the factors (re)insurers should consider, and it provides a glossary of terms and a framework to follow when defining what constitutes a major cyber event. The NCSC also has a Glossary of technical terms. Some insurers are providing "Apps" for their brokers to support familiarity with jargon and workflows.

Trade bodies and the insurance market can continue to harmonise agreed terminology and concepts to make it easier for SMEs to understand the value of the solutions available to them.

Consistent terminology allows SMEs to compare and contrast solutions, whilst also empowering the Insurance industry to remain dynamic and create innovative and differentiated solutions in a competitive market.

Simplified Proposal Forms and Onboarding Experiences

Some proposal forms are still paper-based, and a number of them are long and complicated. These can potentially frustrate an SME buyer, with some buyers feeling that the effort required to complete the paperwork is not worth the perceived value of the product.

Some insurers also speak to the challenge of onboarding SME customers, and the relatively high onboarding cost and SME exposures for the relatively low cost of the policy.

> **A shift towards proposal forms, that are simplified and tailored to the size and complexity of the potential buyer, perhaps supported by insurtech/software solutions and statistical models could allow the insurer to better risk-assess the SME without the use of onerous onboarding processes.**

A number of insurers already implement such solutions. Greater use of digital onboarding processes where possible, to lower the human cost and time required to place the product with the SME could also alleviate issues.

Online proposal and claims handling solutions are encouraged.

Helping Brokers to Help Insurers

Some brokers state that they avoided selling cyber insurance and concentrated on other categories and products they and their clients understood better. If a broker finds queries from the potential insured were difficult to answer they could avoid selling cyber insurance in the future.

To tackle this, some insurers provide cyber insurance training to their brokers on a regular basis; which shows efforts to raise awareness of technical cyber concepts, products and differentiators. **Insurers could consider creating and distributing generic marketing material including SME specific case studies for use by brokers, who can create their own targeted material for their client base.** Insurers could even consider accompanying brokers on visits or potentially be available by video conference in the event that a broker needs specific cyber advice or policy coverage to which they do not know the answer. Insurers actually reported doing this in many cases already, however, there may be significant cost implications to consider here.

Knowledge Sharing

As with any insurance product line, insurers could be encouraged to share information on cyber claims with each other so that there is objective evidence for underwriters to be able to make accurate risk assessments.

The use of joint efforts such as CyberAcuView, ABI Cyber Market Data Collection, and Cyber Monitoring Centre should be actively promoted and encouraged, however, only for anonymised information that does not contain commercially sensitive information.

Insurer's data aggregation tools may create competitive advantages for some, and increase access to the market for others. It can also support wider understanding of risk within key groups such as government.

Bandwidth

Several insurers stated that they did not have the technology setup to make the cyber insurance process faster, more efficient and to better meet prospective SME iInsureds' expectations.

Anecdotally, one insurer strongly acknowledges the value of the SME segment, and indeed their US arm insures many SMEs for cyber and has engineered its processes and training to market to and risk assess SMEs in a cost efficient way. They have achieved significant market share there.

[55] Cyber war clauses;

[56] Guidance on Major Cyber Events;

However, in the UK they have not built an equivalent capability. "24-hour turnarounds" designed for more off-the-shelf insurance are a pain point in a business designed for slower, more considered large risk placement. They feel that given the slim profits on SME products, they are hesitant to re-design a solution that retains commercial value. To add, there is strong market competition from those early movers and agile insurtechs. Finally, there are many costs and uncertainties associated with searching for 'new new' SME businesses, who are purchasing cyber insurance for the first time.

Automated and off-the-shelf designed products, perhaps coupled with remote pre-insurance due diligence systems, could make things more cost effective.

Adapting Cyber Insurance to the Evolving Threat Landscape

Amidst the trend of increasingly sophisticated and widespread cyber-attackers lies the need for underwriters to reflect threat conditions. Insurers will and should continue to take into account many considerations when designing cover, determining premiums and modelling exposure, including the risk landscape, level of cyber hygiene and the stated and actual risk mitigants in place, as well as wider market conditions.

> **The impact of the evolving cyber threat landscape on cyber insurance is especially important to consider. Examples of significant recent changes include AI being used by threat actors to lower barriers to entry, mimic their targets more realistically, and improve effectiveness of attack mechanisms such as Business Email Compromises, Cyber Crime as a Service (CCaaS) and Ransomware. It is essential that insurers keep their approaches up to date with current threat intelligence and model risks and exposures appropriately.**

Many in the insurance market use approaches that evolve with the developing threat landscape and relative security posture of the insured. Increasing risks and lower security may be reflected in increasing premiums or even the decision not to offer coverage. In a soft cyber insurance market, even if the threats are elevated, it can lead to trends of lowering premiums, more relaxed terms of coverage and risk control requirements and potentially more discretion around the risks the industry is prepared to prudently accept. During these periods it's important for trade bodies such as the ABI to share best practices in areas such as risk controls.

Raising Security Standards

Some insurers provide discounts for good cyber hygiene including recognised certifications, skills and capabilities. Some required basic certificates as a precursor for low turnover SMEs (typically <£1mn TO) being accepted for a cyber insurance policy. The CES scheme, whilst not enough on its own for most SMEs to get cyber insurance, is very low cost to achieve and demonstrates that the insured is conscious of cyber security risks and has looked into whether they are in place and working.

There might be a whole economy benefit to having a minimum standard for low turnover SMEs, a more up to date, in-depth version of the CES+ (or equivalent), allowing for a level of independent assurance to protect against and recover from a cyber-attack. Below this, for the lowest turnover businesses such as £<1 million, CES may be appropriate. Above this, businesses could work up to the variety of recognised ISO or other standards relating to cyber security, business continuity, crisis management and resilience. This development of shared standards that are tailored to the risk could provide a better insured to the insurers, with better risk management both pre-, during, and post- the insurance product being triggered.

Large enterprises typically follow a similar and evolving "cyber maturity" framework and insurance can spur this journey of growth for SMEs. For example, if an SME bank loan was contingent on the ability to demonstrate proactive risk management via insurance solutions and associated assurances.

Cyber Partnerships

Insurers increasingly choose to explore partnerships with other solution providers in the cyber ecosystem. Large carrier partnerships with mono-line cyber MGAs and cyber specialist firms is an increasing trend in the market. Cyber security consultancies and law firms are already working closely with businesses of all sizes across all industry sectors in the UK too. They are well appraised of evolving risks and solutions to manage active threats.

> **Insurers and brokers can establish partnerships and working relationships with specialists to increase the value proposition of their products and the effectiveness of the pre- and post-purchase experience for the SME. Alternatively, they can develop their own in-house expertise which is perhaps more robust and cost effective long-term.**

Businesses with specialist cyber expertise can provide advice and guidance to the insured, as well as those seeking insurance cover but who currently do not meet the required

level of cyber hygiene.

Tools already exist to automatically assess the insured's cyber risk posture and current vulnerabilities and some insurers are building and using these tools. They often draw on external scanning data and threat intelligence.

Some cyber insurers, brokers, consultancies and law firms offer free or low-cost cyber health checks to SMEs (either directly or on behalf of the insurer) to go beyond a simple one time "check-up". This consultancy would turn a 'poor' or unquantified risk into a better customer for the insurer, whilst providing value and differentiators and a closer relationship with the insured.

> **The ability to provide real-time threat data to an insured about to suffer a cyber-attack or breach of some kind, is arguably a completely unique and highly prized offer when combined with the traditional insurance indemnification offer.**

Utilising Automation and Technology

Some insurers and claims handlers are deploying standardised platforms for claims management, used internally and by cyber security vendors, allowing for more standardised handling of claims, and to better consolidate metrics and statistical trends.

> **Technology tools can reduce cost, provide a harmonised approach, and can increase the perceived quality of customer service received by the SME. Automated vulnerability scanning can also be used in assessing a prospective insured's cyber hygiene prior to insurance, and continuously during the life of the product. These low-cost solutions allow for proactive assessment of weaknesses and gaps.**

Relatively low-cost solutions also exist to provide continuous monitoring of the cyber hygiene of a business, remotely, providing intelligence to the business and the insurer about the live cyber-health of the business and possibly real-time feedback to prevent attacks. These can be aligned to standards setters such as CES, NIS2, ISO 27001 etc, proactively signalling if, for example, virus defences have been disabled.

Such tools allow insurers to differentiate their products and to increase the value proposition of the insurance product, turning it from a passive safety net to a proactive solution for risk minimisation and cyber crisis management. Technological solutions can provide better risk management for the insured and reduce the number of claims, helping to improve loss ratios and improve the value to the insurer and the insured.

Value-add services such as cloud security, password audits, immutable backups, breach management tools and teams, Incident Response Plan templates and drafting, and cyber war-games all help decrease the risk profile of the insureds, whilst increasing take-up and retention. Such services can be relatively low cost but present very high value.

Greater use of a variety of technology solutions can decrease the SME's risk posture and increase the value and attractiveness of cyber insurance.

Value Proposition vs Price Sensitive SMEs

The insurance industry should continuously reinforce the value proposition of the insurance product, clearly illustrating the value-add suite of insured and risk management tools.

Some SMEs baulk at the actual or perceived cost of cyber insurance and the level of the excess. Some choose to ignore insurance or choose not to renew, seeking alternative risk transference including self-insurance. Others may not have any coverage or contingencies in place at all. However, cyber insurance products aimed at modest SMEs are considered as cost effective and presenting good value.

360 cyber resilience solutions are almost certainly more expensive than the most basic insurance coverage, however, buyers commented that they understood what was included and excluded, contractually, and they were paying to improve their standards, not merely maintain it: risk management added to the traditional insurance risk transference product. In reality, many insurance products support improved security posture as well as offering risk transfer.

Value-add services that include (and highlight) partnerships with insurers, law firms, breach response teams and Public Relations/Communications teams and cyber consultancies can increase the perceived value of insurance for those SMEs with an appropriate budget and sophistication to utilise them. In a cyber crisis few SMEs without cyber insurance would be able to afford and quickly deploy the suite of expert skills available to them via an insurance product.

Marketing, Direct Sales, and Sales Partnership Strategies

Insurers could consider more direct marketing to SMEs as well as to and with brokers, if they have the commercial appetite. They could focus awareness and marketing campaigns around articulating and quantifying the impacts of a cyber breach or attack specific to SMEs. These are not just financial but include issues such as regulatory fines, reputational and goodwill loss, loss of

production, loss of access to and availability of data, loss of jobs, mental health issues and all other possible consequences of a breach.

Increasing the availability and uptake of insights, news bulletins, webinars, educational sessions and product walk-throughs can help increase familiarity with cyber risks, the challenges to insurers of managing a cyber incident, and the impact of cyber events and the value of insurance. These insights would allow the industry to better communicate policy details and coverage in a fashion that is digestible both by potential SME insureds, as well as brokers that do not specialise in cyber insurance.

The conversion rate of direct marketing and online sales is much more effective in the SME segment, especially at the smaller business end, than via a broker. **Insurers might differentiate which coverage is best sold via broker vs which may be more successful via online direct sales.** One respondent insurer selling policies direct to SMEs had a conversion rate of 70%, whereas sales through brokers had a conversion rate of 20%.

A more labour intensive sales partnership approach may be more successful for higher turnover SMEs as the associated costs will also be high. Some insurers are also developing their own in-house broking teams which will naturally increase this partnership style approach between broking and insurance but with additional efficiencies baked in.

Some law firms are providing "Apps" for their brokers to support familiarity with jargon and workflow.

Value Add Solutions

Insurers could help to raise awareness of cyber risks to SMEs and demonstrate how they provide assistance and resilience. This could focus on case studies on the impacts of a cyber-attack on SMEs, and details of the prevalence of such attacks as well as mitigants that are proven to work for many.

Many online and offline resources exist to support SMEs with cyber risk, inside and outside of the insured space. Several of these are detailed in "Appendix G: External Cyber Advice and Guidance". Insurers and brokers can familiarise themselves with resources like these and direct SMEs towards them.

These approaches will help strengthen awareness of the value proposition of cyber insurance products, and also reduce the risk presented by the insured through more effective implementation of mitigation measures.

Claims Handling and Breach Experience

Given the evolving nature of responding to cyber events, the claims process can fcontinuously change.

It is vital to continuously train cyber claims handlers, as well as brokers, to stay abreast of evolving cyber threats, trends, and the potential cost impacts of evolving threats. Careful design of the claims process specific to cyber risk is important, with use of technology and automation, alongside raising the level of familiarity that claims teams have with cyber concepts and baseline cyber security practices, or creating partnerships with specialists.

Trade Body Collaboration

The insurance industry should consider working with relevant bodies such as the FSB, chambers of commerce, police, local government, the ABI, and other relevant organisations to promote the need for cyber insurance. Joint marketing activities with police units such as Cyber Griffin, cyber consultancies and law firms can all help reinforce the value of insurance solutions. Many such events are already aimed at SMEs and greater coordination can support this further.

There also needs to be a shared approach to common issues such as shared lexicon with these partners.

Brokers

Brokers act as a key intermediary and are essential for communicating the value of insurance products and finding alignment of solutions with the Insureds. The recommendations for brokers focus primarily on raising their familiarity with the specific challenges of cyber breaches and risk management for SMEs.

The SME segment can be challenging for brokers. Value added services and technical knowledge comes at a premium, and the exposure of SMEs can be high, while SMEs often may expect low premiums and face to face servicing. This is a potentially loss-making dynamic, especially in a soft market. One broker said anecdotally that in a soft market clients may simply go elsewhere for cover, rather than make the sensible insurer recommended improvements. Explaining the value of the product and broker education is paramount to overcoming some of these challenges, however, the insurance industry alone cannot overcome the widespread lack of cyber preparedness in the UK.

Building Familiarity with Cyber Risk Policies

Some non-specialist brokers (or insurers) may not fully understand the complexities of cyber security or the policies that they are trying to place. Therefore, they may feel challenged in articulating the risks an SME faces or the possible impact of a cyber-attack and the valuable benefits of a cyber insurance policy. Lack of familiarity with exclusions and appropriate policy coverage were also a concern.

Cyber insurance aimed at the SME segment does not appear expensive and there is a range of coverage and premium available. Respondents appeared surprised by the relatively low cost and good value it presented. Brokers could focus on raising awareness of cyber risks that are specific to SMEs and demonstrate how insurance provides invaluable assistance.

> **Awareness campaigns can focus on realistic evidence of the impacts of a cyber-attack and details of the prevalence of such attacks, how they are evolving, and the services folded into the products. Example campaigns that provide value include workshops and "drop in" sessions for SMEs to discuss their needs and the insurance product fit in a friendly and social environment.**

Brokers could also consider using bodies such as the ABI and BIBA to facilitate connections with relevant UK industry bodies.

Understanding Cyber Breach Impacts

Some SMEs express concerns that their broker doesn't understand their business and the possible impacts of a breach, so they are unable to understand the need and value of cyber insurance. A fairly common query from SMEs was, "aren't I already covered for this?" Similar concerns are expressed about under-insurance and potential gaps left in insurance coverage.

Brokers may partner with cyber security consultancies to provide cyber security advice and guidance appropriate for the risk posture and realistic concerns of an SME, such as "how do I encrypt my data?" and "is multi-factor authentication (MFA) expensive?". This trend should be expanded and increased. The focus should be on supporting brokers to find reputable consultancies, as there are very few standards and regulations in the cyber space with which to vet partners.

Many SMEs will not have an in-house cyber security expert. A number of brokers, consultancies and insurers are prepared to invest in providing free 'pre-event' consultancy solutions where the SME does not have in-house competence available. These goodwill exercises improve the insurance solution and the quality of the relationship with the broker as a trusted advisor.

Supporting Appropriate Marketing Material

As with insurers, brokers could consider providing realistic case studies illustrating risks and detailed breach information (anonymised) to help prospective clients understand the value of their data, the need for cyber hygiene and the benefits of risk management using cyber insurance, as well as the potential impact/cost of breaches and attacks for SMEs. Case studies could also be issued by insurers and then tailored with brokers for their specific markets.

More brokers can be trained and provided with material to confidently handle questions about cyber policies. This could involve product specific training on how to tailor messaging for SMEs, initial and ongoing refresher training on the evolving threat landscape and how it could impact the business, and policy specifics on coverage, excesses, exclusions etc. This education could assist in overcoming obstacles in selling cyber insurance to SMEs. This is a common focus of insurers and brokers.

Cross Selling and Adding Value to Insurance

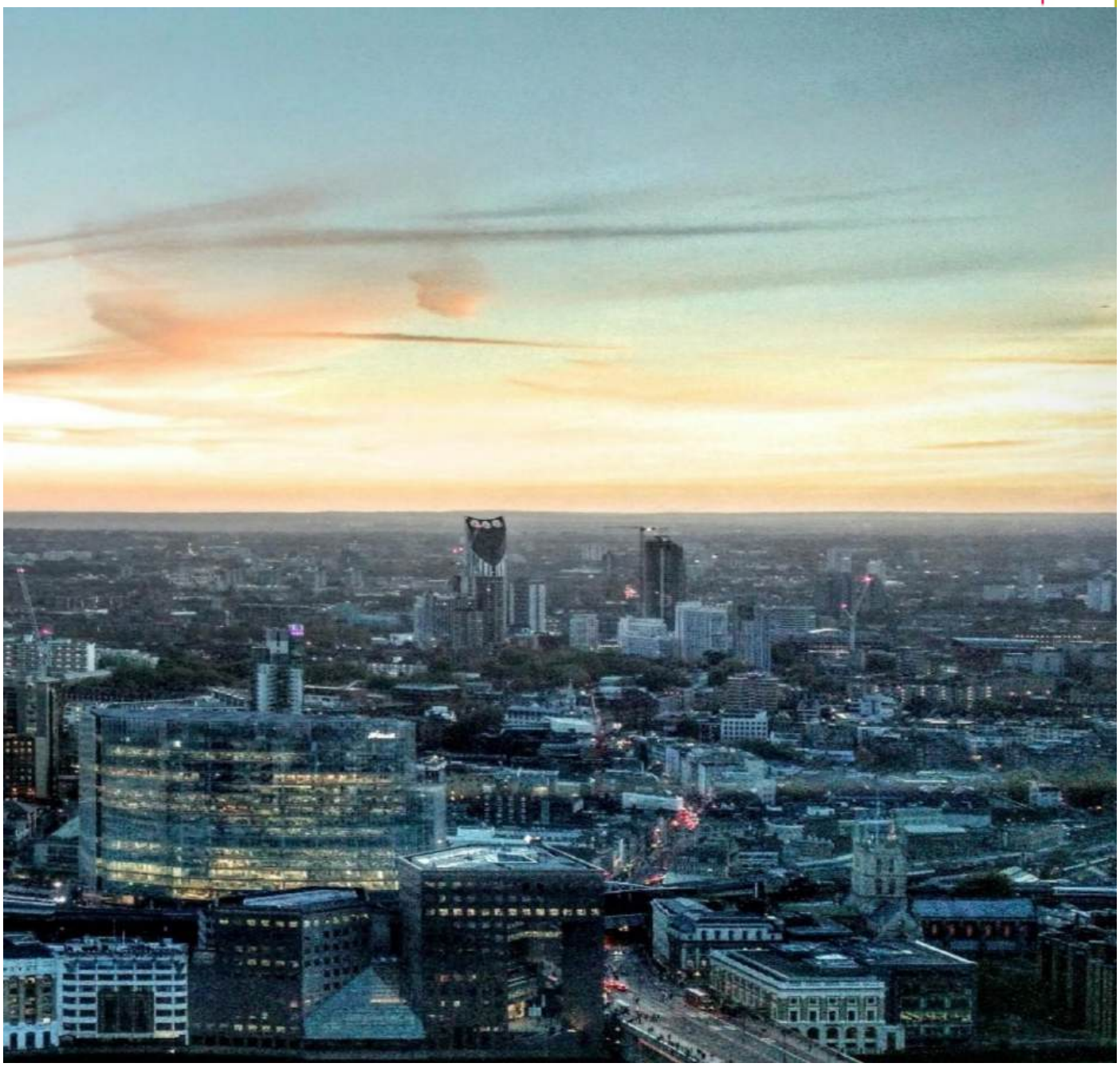
It must be noted that many brokers are perfectly comfortable with the cyber propositions. Some feel there

are insufficient incentives by insurers for them to sell or cross sell cyber insurance to their clients **brokers can partner with insurers to help improve their familiarity with products.** This exchange of insights would also raise the effectiveness of communicating the value proposition to a relatively less informed population of SME businesses.

Bandwidth of Expertise

A broker may not have adequate capacity of cyber security experts to deal with a rapid increase in cyber insurance policy take up to advise prospective Insureds properly on the risks, the impact of a breach and the benefits of a cyber insurance policy.

Likewise, trained cyber responders may be costly to acquire, to train, and to keep trained on evolving threats. Breach response is perceived to be expensive and time consuming, especially compared to other categories of risk. It may be especially true for those outsourcing cyber expertise rather than using in-house capabilities.



Appendix D: Definitions and Terminology

Definitions

It is helpful to 'speak a common language' when communicating cyber insurance concepts to potential SME buyers. Differences in drafting, policy language, and exclusions, make purchasing decisions challenging for SMEs seeking to compare products.

Industry bodies are making efforts to have more coherent language. See for example the recent efforts to establish a consistent framework to define a major cyber event[57].

The SME Segment – defining the addressable population

[57] Components of a major cyber event:;

According to Statistica there are 219,900 small businesses and 37,750 medium businesses in the UK[58]. This means that the potential market for cyber insurance (omitting micro businesses) is in the region of 219,900 + 37,750 = 257,650.

With approximately 90% of SMEs currently not obtaining cyber insurance, the addressable cyber insurance market for this group may be over 230,000 SMEs.

Even within this population, some of those with cyber insurance will not have appropriate or adequate cover for their current and evolving risks.

The FSB statistics for SME cyber insurance take-up notes:

- 10% of small businesses and the self-employed say they have cyber insurance (therefore 90% do not); and
- Of those small businesses that do have cyber insurance, 38% do not know what their policy includes.[59]

There are many definitions for SMEs, computer systems and "cyber crime". There is currently no "standard" language and definitions for many terms. This confusion can make a complex technical area even more challenging to communicate about.

UK Government Definitions of SME

The UK Government defines an SME in three categories:

- Micro Business – fewer than 10 employees and a turnover of less than or equal to €2 million or a balance sheet total of less than or equal to €2 million;
- Small Business – 10 – 49 employees and a turnover of less than or equal to €10 million or a balance sheet total of less than or equal to €10 million; and
- Medium Business – 50 – 249 employees and a turnover of less than or equal to €50 million or a balance sheet total of less than or equal to €43 million[60].

Note: This is the same as the EU definition as defined in EU recommendation 2003/61 (concerning the definition of micro, small and medium-sized enterprises)[61].

Companies Act 2006

This definition is essential as it defines the type of business accounts that the entity can file with Companies House. Similar to the UK Government. It defines an SME as a business that meets at least two of the following criteria:

- Turnover – no more than £36 million;
- Balance sheet total – no more than £18 million; or
- Number of employees – no more than 250.

[58] Number of small and medium-sized enterprises (SMEs) in the UK;
[59] FSB-Policy-Paying-a-premium (Page 7);
[60] Small to Medium Enterprise Action Plan, Foreign, Commonwealth and Development Office, HMG, Updated 2 May 2023
[61] Definition of micro, small and medium-sized enterprises;

Insurance Market Definitions of SME

Many insurers do not agree on criteria to define business size. Some insurers focus exclusively on a company's turnover, whilst others place emphasis on its employee headcount. For some insurers, the key issue is whether the company is owner-run, or whether it is a subsidiary branch of a larger company group.

Different insurers may be using a variety of parameters to define the SME class. However, of greater importance to the potential insureds is crafting solutions that fit their specific commercial criteria. These definitions are important as technical insurance details are often reliant on the insurer's assessment of the company size.

Towergate defines an SME as:

- Micro Business – fewer than 10 employees and a turnover of less than £2 million;
- Small Business – 10 – 50 employees and a turnover more than £2 million but less than £10 million; and
- Medium Business – 50 – 249 employees and a turnover above £10 million but below £50 million.

Hiscox uses the UK government definition above.[62]

The Definition of "Computer System"

The Federation of Small Business report 'Paying a Premium'[63] illustrated lack of common terminology by disclosing that there were around fifty definitions of 'Computer System,' in cyber policies in use in the London Market.

The Definition of "Cyber Crime"

There are a number of definitions for 'Cyber Crime'. Some are outlined below.

Crown Prosecution Service

Cybercrime is an umbrella term used to describe two closely linked, but distinct ranges of criminal activity. Government's National Cyber Security Strategy defines these as:

- Cyber-dependent crimes - crimes that can be committed only through the use of Information and Communications Technology (ICT') devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g. developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity); and
- Cyber-enabled crimes - traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft).'[64]

Note 1: This has been sourced from the National Cyber Security Strategy 2022 - 2030.
Note 2: This definition has also been used in 'Cybercrime: A review of the Evidence Research Report 75', Home Office, October 2013.[65]

EU Definitions of Cyber Crime[66]

Cyber crime does not respect international borders.

It can be classified in three broad definitions:

- crimes specific to the internet, such as attacks against information systems or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' bank accounts);
- online fraud and forgery: large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code; and
- illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia.

Cyber Security Breaches Survey 2024[67]

The breaches survey covers the following range of cybercrimes:

- ransomware - that breached an organisation's defences (i.e. it was not stopped by software);
- hacking - unauthorised access of files or data, as well as online takeovers (e.g. of websites, social media accounts or email accounts and hacking of online bank accounts that did not lead to fraud) that was carried out intentionally, including attacks that led to extortion);
- denial of service attacks - that breached an organisation's defences and were carried out intentionally, including attacks that led to extortion;
- other computer viruses or malware - that breached an organisation's defences; and
- phishing attacks - those individuals engaged with (e.g. by opening an attachment) or that were targeted towards a specific organisation/recipient (e.g. containing personal data) and did not lead to any further crimes being committed'.

There are a number of different definitions, making a "standard" definition of a cyber-crime difficult.

[62] What is an SME?;
[63] Paying a premium?
[64] National Cyber Security Strategy 2016 to 2021, Section 3.2;
[65] Cyber crime: A review of the evidence;
[66] Cybercrime;
[67] Cyber security breaches survey 2024;

Appendix E: Approach and Methodology

Approach and Methodology

Analysis for this report utilised a combination of 15 face-to-face interviews and broader discussions with relevant stakeholders, and desk-based research of pertinent source material.

Interviews covered a wide range of UK SME buyers including prospective insureds, those that currently have cyber insurance, and several who had had cyber insurance but turned away from it. UK Insurers and Brokers were also interviewed in this research report.

Desk research assessed material generated by other industry bodies, press and media reporting, evolving law and regulations and industry speeches, among other sources.

Desk research

Research and material was sourced from a variety of sources including:

- UK Government, various departments;
- Trade bodies relating to insurance and SMEs;
- Press articles relating to cyber-crime;
- Details of services and case studies from specialist cyber security consultancies;
- Case studies from specialist cyber incident response teams;
- Insurance company and Intermediate documentation; and
- Law firms and professional services businesses.

Interviews

Face to face interviews were carried out with several insurers ranging from large carriers to insurtechs, professional insurance institutes, brokers and Grant Thornton SME clients. These included those who had cyber insurance, those that had a claim and did not renew, those that had cyber insurance and had not made a claim and those without cyber insurance.

Questionnaires

Standard questionnaires were used for the discussions with each of the categories above.

For insurers and brokers, the following high-level areas were covered with detailed questionnaires encompassing inter alia:

- Level of cyber expertise in the business;
- General categories of claims seen, including most common types;
- What is the process for determining the risks to be covered?
- What are your views on why there is a lack of take up of cyber insurance by SMEs?
- How do you market cyber insurance to SMEs; do you think it has been successful?
- Do you think that there is sufficient government marketing / awareness to SMEs on the need for cyber insurance?
- Additional comments and observations?

The answers to questions dictated what other questions were asked.

The questionnaire to Grant Thornton clients asked how they rated the process of gaining cyber insurance, the support during the life of the policy and experience dealing with claims on an insured incident. Questions were also asked about their preparedness for a cyber-attack, areas of internal investment and cyber and data governance.

Appendix F: Evaluating the Cost of Breaches

Cost of Breaches

There are a variety of different sources for estimating the cost of a breach.

Cyber Security Breaches Survey 2024

This detailed survey looked at the most disruptive breach suffered by an organisation and the direct financial impact, staff time and other indirect costs[68].

For businesses identifying breaches or attacks, the most disruptive breach during the previous 12 months cost businesses (of all sizes) an average of approximately £1,205. For medium and large businesses, this was approximately £10,830.

Federation of Small Businesses (FSB)

The FSB reports that 73% of small businesses say that they have experienced a financial cost following the most impactful cyber-crime.

- 44% say that it cost up to £1,000;
- 24% say that the financial cost was between £1,001 and £10,000;
- 3% say that it cost between £10,001 and £25,000;
- 2% say that it cost between £25,001 and £100,000;
- 1% say that it cost over £100,000.[69]

Statistica

As of 11 September 2024, the average data breach cost in the United Kingdom (UK) was around $4.53 million. In the measured period, 2022 registered the highest cost for breached data, more than $5 million[70]. This is an average across all businesses and does not differentiate for SMEs.

The Independent

The Independent, dated 28 June 2024, stated that the 'average short-term costs of cyber-attacks or breaches' was £1,630, with 29% of small businesses and 19% of micro businesses affected.

Sky Business

Sky Business research[71] indicates that SMEs will lose approximately £31,000 for each day they are forced to close after a cyber-attack.

UK SME business decision makers estimate they would be forced to stop trading for an average of four days following a cyber-attack.

8% of businesses who have not been victims think an offline period would last eight days or longer compared to 24% of those who have experienced one before.

Micro businesses (those with 1-9 employees) were more likely to underestimate the impact of a cyber-attack on their business, with nearly a third (29%) saying an attack would not cause their business to close. Only one in ten (10%) of medium businesses (with 100-249 employees) said an attack would not cause business closure.

Lloyds

At 'Lloyds Cyber Summit', 2022 Bruce Carnegie-Brown (chairman of Lloyds) stated that the cost of a breach for small businesses was $139,000[72]. It was not determined what the scope of this was (i.e. UK / Worldwide or business size)

Cost of Data Breach Report 2024

The IBM ''Cost of Breaches Report, 2024'[73] covered the period of March 2023 and February 2024. This survey covered 17 industries in 16 countries and interviewed 3,556 security and C-suite business leaders, of which 50 were in the UK.

[68] Cyber security breaches survey 2024, Department for Science, Innovation and Technology, 9 April 2024, Section 4.6 and Tables 4.1 and 4.2
[69] Cracking the Case, FSB, December 2023;
[70] Statistica.com
[71] SMEs miscalculate the cost of cyber-attacks on their business;
[72] youtube
[73] IBM 'Cost of Breaches Report, 2024'

Although this report primarily focuses on larger organisations, the themes and trends will closely follow the behaviours of cyber-criminals and their general focus on businesses of all sizes.

This Report noted that the cost of a data breach had risen '10% over the past year reaching $4.88M, the biggest jump since the pandemic. Business disruption and post-breach customer support and remediation drove this cost spike'.

46% of breaches involved PII and the average cost of a malicious insider attack was $4.99M.

The 'cost of a data breach' in the UK was $4.53M in 2024 with over a quarter of the costs of cyber-attacks due to 'lost business cost'. These will be skewed towards larger organisations, and especially those that publicly declared a breach.

Skills Gaps

The cyber skills shortage is a growing issue that is impacting all areas of the UK, and the situation is similar internationally.

Businesses that don't have access to skilled cyber practitioners will generally suffer more expensive cyber incidents. Cyber insurance offers a solution to this skills gap.

The 'Cyber security skills in the UK labour market 2024'[74] states:

'Over the six years this survey has run, we have consistently found that around half of businesses have a basic skills gap and around three in ten have an advanced skills gap.'

In 2024, the average cost of breaches associated with a **high-level skills** shortage jumped to $5.74 million from $5.36 million in 2023, a 7.1% rise. This increase was $860,000 higher than the global average breach cost[75].

The 'Cyber security skills in the UK labour market 2023' Report[76] states:

'A high proportion of UK businesses continue to lack staff with the technical skills, incident response skills and governance skills needed to manage their cyber security. We estimate that:

- Approximately 739,000 businesses (50%) have a basic skills gap: the people in charge of cyber security in those businesses lack the confidence to carry out the kinds of basic tasks laid out in the government-endorsed Cyber Essentials scheme and are not getting support from external cyber security providers. The most common of these skills gaps are in setting up configured firewalls, storing or transferring personal data, and detecting and removing malware;
- Approximately 487,000 businesses (33%) have more advanced skills gaps, most commonly in forensic analysis of breaches, security architecture, interpreting malicious code and penetration testing; and
- 41% have an internal skills gap when it comes to incident response and recovery, and do not have this aspect of cyber security resourced externally.

Nevertheless, skills gaps are also common in the cyber sector:

- 49% of all cyber firms have faced problems with technical cyber security skills gaps, either among existing staff or among job applicants;
- 22% of cyber sector employers report having existing employees who lack necessary technical skills and 44% say that the job applicants they have seen lack necessary technical skills; and
- Technical skills gaps were most often cited in these 3 areas: security testing (35%), cyber security governance and risk management (31%) and secure system architecture and design (30%).'[77]

[74] Cyber security skills in the UK labour market 2023;
[75] IBM 'Cost of Breaches Report, 2024'
[76] Cyber security skills in the UK labour market 2023;
[77] Cyber security skills in the UK labour market 2023;

Appendix G: External Cyber Advice and Guidance

A wide variety of resources are available from a broad range of sources. These will generally agree on high level concepts but may contain differences or indeed contradictory recommendations on more technical areas.

As noted earlier in this report, there can be a plethora of material available to SMEs. Feedback in interviews suggested that many were overwhelmed and unable to stay up to date. This report calls out opportunities for insurers and brokers to provide some coherent and contemporaneous messaging that is approachable to an SME audience.

In particular efforts by BIBA, the ABI and the FSB have worked to provide harmonious and approachable guidance to potential insureds, insurers and brokers that aligns with government.

Commercial

The most frequently used source of advice in the 'Cyber Security Breaches Survey 2024' was external / third-party cyber consultants and IT consultants from IT service providers, mentioned by 23% of businesses[78].

There was no mention of any advice being sought from insurers or brokers.

The most common source for micro businesses was also external cyber or IT consultants at 21%, with online searching at 4%.

Government

Government or public sector sources, including government websites, regulators and other public bodies were only used by 3% of businesses[79].

It is of note that the Foreign, Commonwealth and Development Office (FCDO) published the 'Small to Medium Sized Enterprise (SME) Action Plan', updated in May 2023[80]. This mentions neither cyber nor cyber insurance.

The FSB document 'Paying a Premium'[81] notes: "We propose that governments across the UK raise awareness through key stakeholder bodies on cyber risk and signpost to relevant information."

There are also a number of sources of cyber advice, grants and loans available that cover implementing / increasing cyber security. Some examples are given below.

NCSC

Only 1% of businesses mentioned the National Cyber Security Centre (NCSC) by name[82].

12% of micro and 13% small businesses had heard of the 'Small Business Guide'.

The NCSC publishes highly helpful guidance for businesses of all sizes. It promotes a"Cyber Assessment Framework[83]" (CAF), audited by independent "Cyber Resilience Audit" suppliers. The NCSC CAF cyber security and resilience objective and principles have four high-level objectives and 14 principles, which are themselves detailed further in a collection of 39 "Indicators of Good Practice".

A1.a: Board Direction
A1.b: Roles & Responsibilities
A1.c: Decision-making
A2.a: Risk Management Process
A2.b: Assurance
A3.a: Asset Management
A4.a: Supply Chain

B1.a: Policy & Process Development
B1.b: Policy & Process Implementation
B2.a: Identity Verification, Authentication and Authorisation
B2.b: Identity Verification
B2.c: IDAC Management & Maintenance
B2.c: Privileged User Management
B3.a: Understanding Data
B3.b: Data in Transit
B3.c: Stored Data
B3.d: Mobile Data
B3.e: Media/Equipment Sanitization
B4.b: Secure Configuration
B4.c: Secure Management
B4.d: Vulnerability Management

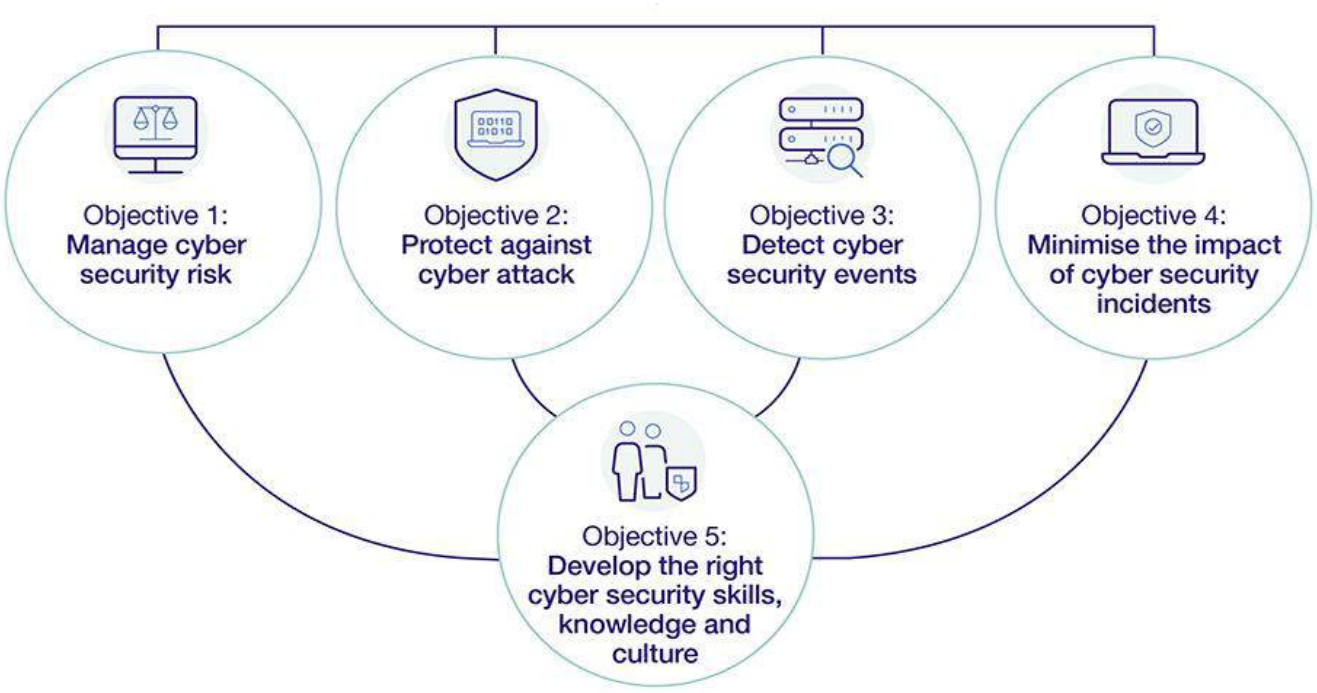
[78] Cyber security breaches survey 2024, Department for Science, Innovation and Technology, 9 April 2024;
[79] Cyber security breaches survey 2024, Department for Science, Innovation and Technology, 9 April 2024;
[80] Small and medium sized enterprises;
[81] Paying a premium?

[82] It is noted that this was an unprompted answer, i.e. not mentioning the NCSC by name and asking if they used their services. However, when prompted 39% of businesses recalled seeing at least one government communication of guidance advice.
[83] Cyber Assessment Framework

B4.a: Secure by Design
B5.a: Resilience Preparation
B5.b: Design for Resilience
B5.c: Backups
B6.a: Cyber Security Culture
B6.b: Cyber Security Training
C1.a: Monitoring Coverage
C1.b: Securing Logs
C1.c: Generating Alerts
C1.d: Identifying Security Incidents
C1.e: Monitoring Tools & Skills
C2.a: System Abnormalities for Attack Detection
C2.b: Proactive Attack Discovery

D1.a: Response Plan
D1.b: Response & Recovery Capability
D1.c: Testing and Exercising
D2.a: Incident Root Cause Analysis
D2.b: Using Incidents to Drive Improvements

An illustration of the Government Cyber Security Strategy is shown below[84]:



[84] Government Cyber Security Strategy:

National Cyber Resilience Centre Group (NCRCG)[85]

Whilst the NCRCG was mentioned in the 2023 Breaches survey, it was not mentioned in the 2024 survey. Inspection of its web site shows that it is still active.

NCRCG has nine regional centres in the UK and provides cyber security podcasts, cyber resilience services, free resources and a 'cyber path'.

The NCRCG website defines a number of services it provides, which include:

- Security Awareness Training;
- First Step Web Assessment;
- Corporate Internet Discovery;
- Internal Vulnerability Assessment;
- Individual Internet Discovery;
- Web App Vulnerability Assessment;
- Remote vulnerability Assessment;
- Security Policy Review; and
- Cyber Business Continuity Review.

There are a number of free resources for SMEs available on the NCRCG websites[86].

Their website states 'Each of the nine Cyber Resilience Centres (CRCs) across England and Wales works closely with its local universities to handpick a unique and talented cadre of students, who work alongside senior Cyber Security Practitioners and police officers to deliver high-quality and tailored cyber resilience services to smaller organisations.'

Cyber Aware[87]

Cyber Aware is part of the NCSC and offers tips and assistance to a variety of people and organisations, including SMEs.

45% of medium businesses had heard of Cyber Aware[88].

Growth Guarantee Scheme (GGS)[89]

This is a government backed loan managed by the Funding Circle and British Business Bank since 2013 through the Growth Guarantee Scheme (GCS), designed to support access to finance for UK small businesses seeking to invest and grow.

To be eligible to apply for the GCS with Funding Circle, the following criteria apply:

- Have a turnover of less than £45 million;
- Be trading in the UK for a minimum of 2 years;
- Be a limited company;
- Use the loan for a business purpose such as working capital or investment; and
- Not be in difficulty or have any collective insolvency proceedings ongoing.

Loans of up to £250,000 are available on meeting application criteria and could support investment in cyber skills and infrastructure.

Funded CES Advice

The National Cyber Security Centre (NCSC) is providing a funded Cyber Essentials programme[90] to help small businesses in certain sectors across the UK implement essential security controls.

The funding will provide 20 hours of free remote support from an NCSC-assured cyber security advisor. The advisor will focus on implementing the controls and ensuring they are effective.

Micro or small businesses (1 – 49 employees) registered in the UK and working on the development of fundamental AI technologies are eligible to apply for the funded Cyber Essentials Programme.

20 hours is very little time to address complex concepts such as cyber security and the value of cyber insurance to SMEs. However, raising the level of awareness for businesses might help some SMEs start a journey towards more effective cyber resilience.

Cyber insurers and brokers can offer similar knowledge and consultancy services to demonstrate the value of insurance solutions. Drop in "cyber surgeries" and similar workshops have been found to be very effective at reaching SME stakeholders.

[85] Nationalcrcgroup
[86] Free Information Pack
[87] https://www.ncsc.gov.uk/cyberaware/home
[88] Cyber security breaches survey 2024, Department for Science, Innovation and Technology, 9 April 2024,
[89] fundingcircle
[90] ross-brooke

Workforce Upskilling Grant

This scheme[91] will give businesses a grant if they are looking to make improvements in the following areas:

- Advanced Manufacturing
- Lean/Six Sigma
- Cyber Security
- Using Hybrid/Virtual Reality in the Workplace
- Leadership
- Project Management
- Computer-Aided Draughting and Design

Trade Bodies and Organisations

It is evident that there are many sources of information available to SMEs to gather information, guidance, and indeed actual cyber consultancy, all at no cost. However, the challenge may be lack of cohesion between the bodies, an overload of information without a centralised "source of truth", which indeed may be impractical, and differing terminology between sources.

Many SMEs are not aware of the risk, and thus even less aware of the resources available, often for free, to help mitigate the risks. Insurers and brokers can do much to help raise this awareness both before placing a product, and during the lifecycle of the insurance.

Examples of insurer and broker driven cyber insurance resources aimed at, or to support SMEs, include:

British Insurers Brokers' Association (BIBA)

The BIBA website[92] points to several resources, including:

- CFC Underwriting Ltd as a BIBA Official Scheme Provider – for cyber insurance;
- Details of the CES Scheme; and
- Guidance from the NCSC on ransomware.

The Chartered Insurance Institute (CII)

The CII makes available multiple courses available to insurance and risk professionals[93].

An example course on cyber security covers is aimed at those:

- looking to build knowledge and understanding of cyber risk and insurance to inform their day-to-day roles;
- influencing the wider business activities; and
- serving customers facing challenging cyber threats.

It covers how to:

Describe
the nature and types of cyber threat

Explain
how legal and regulatory developments impact cyber exposure

Identify
how different insurance policies can impact cyber coverage

Summarise
the principal considerations of underwriters and brokers in relation to cyber insurance policies

Describe
the claims handling process for cyber insurance

Such courses are clearly very encouraging and aimed at raising the level of familiarity with cyber concepts for insurers and brokers.

[91] https://smallbusiness.co.uk/small-business-grants-uk-2548113/
[92] https://www.biba.org.uk
[93] https://www.cii.co.uk

Immersive Labs[94]

This training platform is widely used and well regarded by cyber experts across many fields and has been trusted for many years by world leading cyber security professionals. The platform relies on real-time measurement of human cyber capabilities across technical and non-technical teams—any role within the organisation, including cyber teams, developers, engineers and executives.

Cyber Insurance Academy

The Cyber Insurance Academy website[95] was recently set-up and provides benefits for cyber insurance professionals from over 40 countries worldwide, including:

- Certification course - the Certified Cyber Insurance Specialist (CCIS) is accredited by the CII);
- Foundation courses;
- Premium content library on cyber issues;
- Real time newsroom; and
- Powerful networking opportunities for cyber insurance professionals.

Federation of Small Businesses (FSB)

The FSB website[96] provides a range of cyber security advice aimed at small businesses. These resources are highly valuable for SMEs and communicate concepts that Insurers and Brokers would be well placed to become familiar with.

A selection of recent posts include:

- Eight benefits of a cyber security policy
- Nine cyber and data security documents your business needs
- 10 ways to protect your cyber security as a small business
- Cyber Resilience - How to protect small firms in the digital economy.
- How to prevent employee cyber breaches
- How to Protect Your Business from Cyber Fraud

The Institute of Chartered Accountants in England and Wales (ICAEW)

The ICAEW website[97] provides support to its members for a variety of resources for managing cyber risk, but not specifically for cyber insurance.

Chartered Institute of Information Security (CIISec)

The CIISec website[98] contains a variety of resources relating to cyber security, but not specifically for cyber insurance.

Insurers and Brokers

In many cases insurers and brokers provide cyber security advice and other related services from pre-inception stage throughout the life of the policy. This includes consultancy, training and the use of cyber security tools, depending on the insurer or broker. Some provide continuous monitoring and the ability of the insured to log in via a portal to access their scanned data or undertake scans 'on demand'.

Free Cyber Security Tools

There are a number of these available on the internet. Many are tailored via self-assessment questionnaires that cover some critical questions and give high level advice on system security issues. Several are highlighted below.

Experian provides a very well received Data Breach Response Guide[99], providing guidance on cyber security issues and a template Incident Response Plan. A prepared and tested Incident Response Plan is one of the most cost-effective ways to reduce the impact of a cyber incident.

Hiscox provides a free, online, Cyber Maturity Assessment. Six fairly simple questions allow a business to assess its cyber posture compared to its peers, "*to help you understand your company's cyber security strengths and weaknesses*"[100].

The questions query how the business structures itself across six areas:

- Governance and assurance
- Operational readiness
- Policies and standards
- Process and procedures
- Suitably qualified and experienced people (SQEP)
- Tools and technologies

AIG offers a free Cyber Resiliency Program to its Insureds.

[94] Immersivelabs
[95] Cyber Insurance Academy
[96] FSB
[97] Cyber-security
[98] https://www.ciisec.org/
[99] Why it's essential to put your consumer response plan to the test;
[100] What's your cyber readiness score?;

This presents a high water mark for value add solutions for businesses, including:

- Real-Time Threat Intelligence
- Cyber Risk Assessments - clients receive cyber risk assessments and guidance from AIG's Cyber Risk Advisors to understand their current cyber security posture and identify loss control gaps using best practices.
- CyberMatics - helps clients verify their cyber risk posture, prioritize implementation of controls that reduce risk.
- CyberEdge Communications Platform - provides clients an off-network collaboration platform to efficiently prepare for and manage incident response and report claims to AIG.

Law Firms may offer free news bulletins, webinars, cyber war games and advice on evolving cyber threats. An example is Reynolds Porter Chamberlain LLP's Cyber_Bytes[101].

The **ABI's online Cyber Safety Tool**[102], as well as webpage on:

- What does cyber insurance cover?
- Common exclusions to look out for |
- Cyber insurance in action
- How to buy cyber insurance |
- Advice for improving cybersecurity

helps businesses. The Tool helps generate a tailored action plan with low cost and relatively easy to implement actions to improve their risk posture.

[101] Data and privacy

[102] https://abi.cyber-safety.org.uk/

Online Resources

Some of these include:

- Association of British Insurers (ABI);[103]
- Oryxalign;[104]
- Own Your Own Online;[105]
- Twenty Four[106];
- Cyber Aware; and[107]
- NCSC – Exercise in a Box[108]

These provide online questionnaires that produce high level cyber hygiene action plans to improve a business's cyber security posture. Cyber Aware's questions are specifically aimed at micro and small businesses.

Paper Based Resources

Some of these include:

- Cyber Essentials Scheme (CES);[109]
- 10 Steps;[110]
- Centre for Internet Security (CIS) Controls;[111]
- Axa -10 Quick Wins to reduce your cyber risk[112]
- NCSC Cyber Security Board Toolkit for boards[113]
- NCSC Small Business Guide: Cyber Security[114]

Note: Undertaking CES or CES+ through the Information Assurance Security Management Association (IASME), who is the NCSC's official cyber essentials delivery partner, can provide basic cyber insurance cover. Although beneficial, this only provides up to £25,000 of cover, which will not provide very broad assistance on a complex breach when one considers the professionals needed to address the breach. These include:

Several insurers will provide external system scans and non-invasive security tests to help better understand and inform the Insured. These are excellent examples of the Insurance industry demonstrating value add solutions to enrich the value of insurance.

Free Cyber Security Training Courses

There are a number of free training courses available online. These include, but are not limited to:

- Free courses in England (Government funded and provides a certificate)[115]
- Reed (Some are government funded and some have certificates)[116]
- Oxford Home Study (with certificates)[117]
- Forbes (with certificates)[118]
- NCSC[119]
- Coursera (many free courses and some have certificates – some are 'paid for' courses)[120];
- Microsoft Security Academy[121]

In addition, there are a number of sites giving details of multiple suppliers offering free cyber security training (e.g. Skill for Careers, DfE).[122]

Further education and apprenticeships are available, but these must keep pace with technological advances to provide appropriate cyber guidance to SMEs.

If potential and current insureds are not already made aware of these resources, insurers and brokers in the cyber market should familiarise themselves with the materials, and also direct SMEs towards them. This will help strengthen awareness of the value proposition of cyber insurance products, and also reduce the risk of the insured through more effective implementation of mitigation measures.

[103] https://abi.cyber-safety.org.uk/
[104] cybersecurity-score
[105] Business-online-security-assessment-tool
[106] Cyber-health-check
[107] Action plan
[108] Exercise-in-a-box
[109] https://www.ncsc.gov.uk/cyberessentials/overview
[110] https://www.ncsc.gov.uk/collection/10-steps
[111] https://www.cisecurity.org/controls
[112] https://axaxl.com/-/media/axaxl/files/pdfs/insurance/cyber-north-america/axa-xl_cyber_quick-wins-to-reduce-cyber-risk_marketing-sheet_srm.pdf?sc_lang=en&hash=E580E5841E86B587498F98149F0C5591
[113] https://www.ncsc.gov.uk/collection/board-toolkit/toolkits-toolbox/downloads
[114] https://www.ncsc.gov.uk/collection/small-business-guide
[115] https://freecoursesinengland.co.uk/cyber-security-course-free/
[116] https://www.reed.co.uk/courses/free/cyber-security
[117] https://www.oxfordhomestudy.com/courses/cyber-security-courses/free-cyber-security-courses
[118] https://www.forbes.com/sites/rachelwells/2024/07/14/free-online-cybersecurity-courses-with-certificates/
[119] https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available
[120] https://www.coursera.org/business?utm_content=corp-to-home-for-enterprise&utm_campaign=website&utm_medium=coursera&utm_source=header&utm_term=b-in
[121] https://microsoft.github.io/PartnerResources/skilling/microsoft-security-academy
[122] Skills-bootcamp

Appendix H: The FCA and PRA

Financial Conduct Authority (FCA)

The FCA has an obligation to regulate Insurers and their conduct. Regulation is a moving target as threats and the market evolve.

The FCA has encouraged the development of healthy consumer-facing responsibilities, including in particular, the Consumer Duty obligations.

It is of note that the FCA Insurance Code of Conduct of Business (ICOBS) specifies rules as to how insurers, re-insurers and brokers could interact with customers, but it does not specifically cover cyber insurance.

Communication with customers is specifically covered in ICOBS Chapter 6. Chapter 6.1.5 (R) specifically states:

'A firm must ensure that a customer is given appropriate information about a policy in good time and in a comprehensible form so that the customer can make an informed decision about the arrangements proposed'.

Chapter 6.1.6B (R) states:

'A firm must ensure that the level of appropriate information provided takes into account the complexity of the policy and the type of customer'.

Annex 3 defines the product information that must be provided 'by way of a 'standardised insurance information document' (the Insurance Product Information Document (IPID)) to allow a customer to make an informed decision.

Matt Brewis, the Director of the Insurance at the FCA, wrote to insurers in September 2023 with an update on the FCA's priorities for 2023-2025.[2] Within its letter, the FCA flags the risks with **uncertain policy wordings** which may not meet customers' needs.

The regulator will also obligate insurers to maintain their own strong cyber security standards.

The FCA website publishes a 'Good cyber security – the foundations' infographic[123], which, although dated, shows good intentions by the regulator to help educate the market. Guidance must be up to date for it to be effective, and to not provide a false sense of security.

Information security requirements are also covered in SYSC 13.7[124] and other parts of FCA documentation.

It is noted that the FCA sends out regular 'Dear CEO' letters to regulated businesses, and some of those will include themes on maintaining appropriate levels of operational resilience and cyber hygiene.

Prudential Regulation Authority (PRA)

The PRA has produced SS4/17 – Cyber insurance underwriting risk[125].

The PRA wrote to insurers on 11 January 2024 to define its priorities for 2024, singling out cyber insurance.

The PRA has identified cyber insurance as a priority for 2024[126].

They have published their "Insurance Supervision: 2025 priorities" letter127, specifically calling out "Operational resilience, cyber security and third-party risk". It notes: "The cyber threat landscape facing the UK's financial system continues to evolve rapidly, and we view the ability of firms to detect, respond to and in particular recover from cyber-attacks to be a cornerstone of the financial system's resilience."

Examples of large events

In 2022 the PRA asked the cyber market to model losses for a sustained systemic incident caused by a three-month cloud provider outage in their stress test exercising. There is still controversy about the likelihood of an event of this magnitude and impact taking place, and the level of latency that this might create vs full loss of cloud access. It is difficult to articulate this to an SME in terms of how likely large scale events are to occur, and what their coverage expectations should be, with insurers choosing to apply exclusions for this type of large-scale event in order to be in line with prudential *expectations.*

There is increasing concern around the use of cloud service providers (CSPs), and 'concentration risk' for IT services, where an attack on a major technology provider can impact thousands of businesses for indeterminate time periods.

[123] Cyber-security-infographic
[124] Handbook
[125] Cyber-insurance-underwriting-risk
[126] The PRA identifies cyber insurance as a priority for 2024
[127] Insurance Supervision: 2025 priorities;

Reliance upon core outsourced or centralised infrastructure such as deep sea cabling and cloud providers, for example, are key areas of concern, even though they are not typically covered in the market.

Popular platforms can also create systemic risks that could impact multiple entities simultaneously. The potential impacts of these large events makes it challenging to offer and communicate cover, and exclusions are in place to ensure prudent coverage.

Cyber Insurance solutions provide much needed advice, crisis investigation and containment, and potentially remediation skills that most SMEs lack, however there are certain events which are likely to be excluded such as large low-likelihood, high-impact cyber events.

The recent "CrowdStrike" incident caused by a faulty update on a popular cyber security solution caused global IT failures. Many SMEs were particularly badly impacted by this incident, either directly or as a knock-on impact on supply chains above and below them. For example, banks that were unable to process transactions impacted SMEs that found themselves unable to trade online. An SME coffee shop that relies upon an outsourced Point of Sale system could find itself unable to process payments from customers, causing business failure.

Smaller businesses may also lack the ability to remediate and repair their systems in a timely fashion, causing further delays, potentially deepening and lengthening the impact of the event. Media quotes from SMEs during CrowdStrike reinforce the risks to smaller businesses with more limited operational resilience:

"If I were part of a big company, then I would be able to delegate and get support from computer science or security services… but as a small business owner, I am depending only on myself. It's pretty devastating."

Small businesses are not immune to large cyber events. Indeed, they are more likely to be impacted, potentially catastrophically, by these wide-spread attacks. Industry estimates indicate that around 8.5 million computers, globally, were impacted by the CrowdStrike incident. A significant portion of these were used by SMEs across various industries such as healthcare, transportation, banking, and media, estimated to be around 30-40% of the affected systems. This translates to approximately 2.5 to 3.4 million SMEs globally experiencing significant operational disruptions during this single event.

Amidst headline grabbing large cyber events and their seemingly random origin and spread, the noise can make it hard to explain what the cyber insurance product offers and why. This report offers examples throughout, of the product value and ways to articulate value despite this noise. This is a challenging thing to achieve and may explain some of the apathy of SMEs to act, and the challenges of explaining their exposure to them, as the problem can seem overwhelming and impossible to tackle. However, this is not the case. There are many meaningful actions that businesses can take with the support of insurance to protect themselves, given that the human crisis-response is completely critical to how events play out. SMEs must understand that they can be impacted and are not immune just because they are small.