ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

How the Proposed UK Cyber Security and Resilience Bill Can Unlock Growth in the Nation's Cyber Insurance Market

SAMUEL AGYARKO KORANTENG AND AYESHA BHATTI | DECEMBER 2025

The UK's proposed Cyber Security and Resilience Bill presents a much-needed opportunity to kickstart the growth of the UK's lagging cyber insurance market, which will make businesses more resilient to the increasing frequency and significance of cyberattacks.

KEY TAKEAWAYS

- Cyber insurance represents a key tool for firms to boost their cybersecurity practices and resiliency during a period of increasingly sophisticated, widespread, and damaging cyber threats.
- A lack of regulatory pressure within the UK's data protection laws and cybersecurity regulations has led to a slow uptake in cyber insurance and an underdeveloped cyber insurance market.
- The UK government's proposed Cyber Security and Resilience (Network and Information Systems) Bill (CSRB) is a promising start to develop the UK's cyber insurance market but requires further improvements to encourage firm adoption of cyber insurance.
- These improvements to the CSRB should include measures to improve information sharing between organizations and institutions, promote the widespread uptake of cyber insurance, and foster innovation in cyber insurance.
- Greater adoption of cyber insurance will reduce interruptions and financial losses from cyber incidents.

CONTENTS

Key Takeaways 1
Introduction 2
The UK Faces More Sophisticated, Frequent, and Expensive CyberAttacks 3
The UK's Underdeveloped Cyber Insurance Market Exacerbates Risks 5
The UK's Cyber Insurance Market is Underdeveloped Because of its Current Regulatory Policies and Inconsistent Industry Practices 6
Limited Regulatory Pressure Contributes to an Underdeveloped UK Market 6
Inconsistent UK Cyber Insurance Industry Practices Have Stifled Insurance Uptake 8
Recommendations 10
Establishing a Confidential Cyber Incident Information Exchange Platform 11
Creating Model Cyber Insurance Wording and an Underwriting Glossary 12
Introducing Clearer, Objective Definitions for Firms the Bill Captures 12
Prioritizing Risk-Based Over Size-Based Classifications 13
Establishing a State-Backed Cyber Reinsurance Pool 14
Launching a Cyber Insurance Sandbox 15
Conclusion 16
Endnotes 17

INTRODUCTION

Cyber insurance is an effective tool to boost the cybersecurity and resiliency of businesses. It shifts cyberattack risk to insurers, allowing businesses to operate normally while aligning their cybersecurity practices with insurer requirements to secure coverage. The UK is experiencing more cyberattacks; however, compared with global peers such as the United States, it has an underdeveloped cyber insurance market with poor demand and adoption, leaving UK businesses exposed and insufficiently protected. This underdevelopment is the result of laws and regulations that have created fragmented cyber risk data, high cyber insurance premium rates, and a lack of common cybersecurity standards.

The UK's proposed Cyber Security and Resilience (Network and Information Systems) Bill (CSRB) presents an opportunity for course correction. This legislation would promote better cyber risk management practices, reduce cyber insurance coverage gaps, ensure that organizations recover more effectively from cyber incidents, and boost the growth of the U.K. cyber insurance market that makes the United Kingdom globally competitive and on par with current cyber insurance leaders such as the United States.

The bill contains deficiencies that will reduce its ability to achieve a thriving U.K. cyber insurance market. These deficiencies include vague criteria that would capture entities beyond the intended scope of the bill and a reliance on size-based enforcement that blurs accountability

for third-party risk. This type of enforcement could introduce hidden vulnerabilities within supply chains, undermining the growth of a much-needed UK cyber insurance sector that undermines the objectives of the bill to boost security and resiliency. With these measures, the CSRB will enhance UK organizational resilience, reduce economic loss from cyber incidents, accelerate the growth of the UK's cyber insurance market, and foster a competitive insurance landscape with accurate risk pricing and broader coverage. Such steps will strengthen national cyber resilience by optimizing risk transfer mechanisms and lowering the country's vulnerability to widespread cyberattacks.

To improve the CSRB to promote the development and adoption of cyber insurance, the UK government should do the following:

- Establish a confidential cyber incident information exchange platform, require firms to participate, and publicly release an anonymized cyber incident dataset
- Create model cyber insurance wording and an underwriting glossary in partnership with key regulators and insurer bodies
- Introduce clearer, objective definitions for firms the bill captures
- Prioritize risk-based over size-based classifications for firms, infrastructure, suppliers, and other entities the bill captures
- Establish a state-backed cyber reinsurance pool to cover catastrophic risk from cyber incidents
- Launch a cyber insurance sandbox overseen by the Regulatory Innovation Office

Adopting these recommendations within the CSRB will address the current limitations of the UK cyber insurance market, thereby reducing underwriting uncertainty, simplifying premium estimation, and avoiding arbitrary blanket exclusions and surcharges.

THE UK FACES MORE SOPHISTICATED, FREQUENT, AND EXPENSIVE CYBERATTACKS

The UK is facing a surge in cyberattacks that are more frequent, costly, and sophisticated than ever before. Businesses across the country are losing billions in revenue to ransomware, phishing, and social engineering campaigns, with nearly half suffering a successful breach in the past year alone. These escalating threats highlight the urgent need for stronger resilience measures and more effective risk transfer mechanisms, making the case for the CSRB.

The UK faces more cyberattacks than does any nation in Europe, with the scale and cost of incidents rising sharply.[1] In 2024, the UK National Cyber Security Centre (NCSC) recorded 1,957 cyber incidents across all sectors, 430 of which were classified as serious—a rise from 371 the previous year—with 89 qualifying as nationally significant.[2] Over the last five years, UK businesses have lost an estimated £253.1 billion in revenue to cyberattacks, while cybercrime cost the UK economy £38.1 billion in 2024, is projected to reach £44.6 billion in 2025, and could climb to £71.9 billion by 2027.[3] The government's own Cyber Security Breaches survey found that about half of UK businesses and nearly a third of charities experienced a breach or attack in 2023, with phishing the most common method, affecting 84 percent of organizations.[4] In 2024 alone, UK firms faced more than 8.5 million attempted attacks—nearly 8 million of

them phishing attempts and almost 600,000 system hacks—with an average financial impact of £1,025 per successful breach, rising to £10,830 for medium-sized and large firms.[5] The scope and financial damage of cyberattacks in the UK is serious, especially on medium-sized and large businesses, where breaches severely impair operational resilience and business continuity.

In recent years, cyberattacks in the UK have become more sophisticated, such as attackers employing artificial intelligence (AI) to assist with attacks.[6] The NCSC has warned that generative AI is driving this trend, allowing attackers to launch hyper-personalized phishing campaigns, create realistic deepfake calls and videos, and automate the identification of system vulnerabilities.[7] These tools are increasingly being utilized by both criminal organizations and state-aligned actors.

The UK faces more cyberattacks than does any nation in Europe, with the scale and cost of incidents rising sharply.

UK businesses have also experienced highly impactful cyberattacks, demonstrating their increasing significance in business operations. Early in 2024, Hong Kong employees for British professional services firm Arup were tricked by a deepfake video call, resulting in the transfer of HK$200 million (£20 million) to scammers.[8] Only months later in April 2024, UK retail giant Marks & Spencer (M&S) had to halt all online orders after a breach of its systems.[9] The cyberattack started with a supply chain vulnerability: hackers attacked Tata Consultancy Services, the third-party supplier running M&S's IT helpdesk. By impersonating internal IT personnel in telephone calls, help desk staff were tricked into resetting passwords and providing network access. The attackers, known as DragonForce, gained access to M&S's systems, encrypted important data, and stole sensitive customer information for extortion.[10] The effect was profound. Automatic ordering and stock systems were shut down, with stores reverting to manual systems, resulting in shortages and agitated customers. Financial harm was put at £300 million in lost revenue, while market capitalization dipped by over £1 billion.[11] While payment information was not compromised, personal data—names, addresses, emails, and purchase histories—was vulnerable, prompting bulk customer notification and password resets. Insurers estimated daily losses at more than £1 million until services ultimately resumed.[12] Shortly afterward, Co-op and Harrods were hit by similar intrusions, taking advantage of online services and IT helpdesks. The frequency and extremity of these attacks underline their increasing sophistication and impact.

Costly cyberattacks have also demonstrated the vulnerability of UK critical infrastructure. In health, a ransomware attack in 2023 on Synnovis, a National Health Service pathology supplier, disrupted essential services at six London hospitals, costing Synnovis about £32.7 million.[13] Thousands of procedures were postponed, illustrating how one cyber event can ripple through linked health systems with serious implications for public well-being. In 2021, the energy sector alone represented 24 percent of all national cyberattacks. Elexon was one such affected UK energy supplier, where attackers obtained access using a compromised user account and installed malware that encrypted internal company systems.[14] Although the intrusion had no direct impact on the national grid, it disrupted Elexon's ability to coordinate settlements between electricity suppliers, demonstrating how even an attack on back-office IT may cause operational and financial pressure. Financial services followed, with 19 percent that same year, as Finastra,

one of the world's leading financial technology businesses, was hit by a severe ransomware attack, forcing it to shut down several of its key servers.[15]

In short, the UK continues to experience a rise in both the prevalence and sophistication of cyberattacks, leaving businesses, public services, and critical infrastructure vulnerable.

THE UK'S UNDERDEVELOPED CYBER INSURANCE MARKET EXACERBATES RISKS

Despite facing one of the most severe cyber threat landscapes in the world, the UK has an underdeveloped cyber insurance market that leaves businesses and critical infrastructure dangerously exposed. Low market penetration, particularly among small and medium-sized enterprises (SMEs), has created a wide protection gap that amplifies the economic and operational fallout of cyber incidents. Without adequate financial safeguards, cyberattacks risk becoming a multiplier of harm across the economy—underscoring the need for policy that supports a thriving cyber insurance sector.

Cyber insurance uptake is still alarmingly low across all business sizes, according to UK adoption data. Only 45 percent of UK businesses had cyber insurance in 2024, primarily as part of larger insurance policies.[16] Stand-alone cyber policies remain uncommon: only 7 percent of all UK businesses had specific cyber coverage in 2024 (down from 8 percent in 2023), with uptake focused among larger entities, with 27 percent of large businesses and 18 percent of medium-sized businesses having had stand-alone cyber insurance.[17] Small businesses lag behind, with the 2025 UK Cyber Security Breaches Survey finding that just 17 percent of small businesses have stand-alone cyber insurance. SMEs in the UK believe that they are too small to be targeted, even though over 43 percent report cyberattacks annually.[18]

Cyber insurance uptake is still alarmingly low across all business sizes, according to UK adoption data.

This persistent coverage gap—despite rising cyber threats and cyberattack frequencies—underscores the significant market opportunity and the need to expand the availability and adoption of cyber insurance across the UK business landscape.

This underdeveloped UK cyber insurance market increases the nation's cyber risks. Cyber insurance functions as a risk transfer tool, providing financial coverage for cyber-related losses, such as ransomware, business interruption, regulatory fines, and legal fees.[19] A common criticism of cyber insurance is that it may provide a perverse incentive to threat actors to initiate certain types of attacks, such as ransomware attacks, knowing that insured organizations can pay. However, cyber insurance also serves as a driver of resilience, as insurers require policyholders to adopt high cybersecurity precautions. Policyholders often receive specialist advice, monitoring services, and incident response support as part of their coverage. In this respect, insurance is not merely a payout mechanism but also an incentive for businesses to strengthen their defenses. With a low cyber insurance penetration in the UK, most companies miss out on these benefits.

For the UK, increasing cyber insurance adoption is both a resilience and an economic move—it has the potential to help the UK match larger markets such as the United States by developing high-value underwriting, actuarial, and cyber services and making the UK a more secure and

stable location to conduct digital business. By contrast, the underdevelopment of the UK's cyber insurance market may result in a dangerous risk multiplier effect, wherein cyber incidents trigger economic harm due to inadequate financial protection.

THE UK'S CYBER INSURANCE MARKET IS UNDERDEVELOPED BECAUSE OF ITS CURRENT REGULATORY POLICIES AND INCONSISTENT INDUSTRY PRACTICES

The UK's underwhelming cyber insurance sector growth and uptake is the result of limited regulatory pressure, reliance on outdated standards and varying industry practices related to premium pricing, complex insurance policy language, lack of data reporting, and inconsistent insurer requirements. This environment reduces the efficacy of cyber insurance as a risk management tool, which in turn threatens the UK's global economic position and puts the UK—as the most cyber-attacked nation in Europe—at even greater risk. Better regulatory policies that also improve industry practices would spur a greater global market share in cyber insurance that would not only provide better safeguards to UK businesses through more fulsome coverage options but also make the UK more competitive in worldwide cyber risk markets.

Increasing cyber insurance adoption is both a resilience and an economic move.

Limited Regulatory Pressure Contributes to an Underdeveloped UK Market

Data protection rules have historically played a role in fostering the uptake and widespread adoption of cyber insurance, such as within the United States where its strong cyber insurance market is linked to effective data protection rules. The UK's data protection regulation, by contrast, has insufficiently incentivized the growth of the sector and cyber insurance uptake.

The United States introduced data protection laws such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996 to safeguard individuals' medical information and streamline health care data flows, several statewide data breach notification laws that imposed obligations on companies to notify customers of a data breach, and the California Consumer Privacy Act (CCPA) of 2018 to enhance privacy rights and consumer protection for California residents. These rules—some of which were in response to rising and significant data breaches—imposed tough security and data breach obligations on covered entities, making them liable for the activities of service providers, third-party vendors, and business associates. Such obligations gave rise to the need for cyber insurance.

HIPAA introduced three rules on entities covered by the legislation to protect the privacy and security of sensitive patient data. These rules are the Privacy Rule, which sets standards for how entities should use and disclose protected health information (PHI), the Security Rule, outlining key safeguards for electronic PHI, and the Breach Notification Rule, which requires health care entities to notify affected individuals and authorities whenever a breach occurs. Failure to comply with these rules leads to steep penalties. For example, civil monetary penalties for breaches range from a minimum of $141 at Tier 1 to a maximum of over $2 million at Tier 4 per violation, with the tiers corresponding to the level of culpability for the breach. HIPAA also imposes criminal penalties for violations in which an individual or entity knowingly breaches the Privacy Rule, including fines of up to $250,000 and imprisonment of up to 10 years, based on

intent.[20] Given this framework, entities that engage with sensitive patient data require strong cybersecurity practices, and many use cyber insurance to transfer risk as much as possible.

The third rule of HIPAA—the Breach Notification Rule—represents one of the earliest requirements on entities to notify affected individuals whenever a breach occurs. This notification obligation has been directly linked to the uptake in cyber insurance, most notably with California's data breach notification legislation in 2002, which was one of the first state-wide breach notification laws.[21] Other states soon followed, mandating similar requirements on companies for which the cyber insurance market underwent a shift to indemnify the costs associated with a major data breach.

The CCPA subsequently came into effect to address heightened concerns over data privacy sparked by the Cambridge Analytica scandal. The CCPA imposes liability and heavy fines when covered entities do not cure a CCPA violation within 30 days. The CCPA also created a private right of action for any breach of unencrypted personal data, with high damages.

These types of rules, coupled with notable cyber incidents across the United States, including the TJX Companies hack in 2007 that compromised over 45 million customer credit and debit cards and cost TJX between $1 billion and $4.5 billion, heightened awareness of the need for appropriate cyber insurance coverage to transfer risk.[22] In particular, the cyber insurance industry became a key asset for U.S. businesses that saw the growing threat of cyber incidents.

While U.S. regulations established a clear link between regulatory liability, organizational vulnerability, and insurance adoption, the UK's more liberal and fragmented framework stalled both cyber insurance development and adoption.

By contrast, the UK's legislative structure has consistently failed to sufficiently pressure businesses to adopt cyber insurance, despite the inevitable rise in cyber incidents. The UK Data Protection Act (DPA) 1984 only focused on data registration and access rights rather than third-party liability or data breach notification.[23] Its emphasis on procedural transparency over risk containment left UK companies with scant regulatory motivation to underwrite against third-party cyber exposures. In practice, the DPA only promoted access rights, diverging from HIPAA and the CCPA, which explicitly impose liability on covered entities for their service providers' and business associates' actions.

HIPAA and the CCPA mandate organizations not only to secure data internally but also to monitor their entire vendor ecosystem—a clear connection between regulatory requirements and the business case for cyber insurance as a means of transferring that external risk. UK laws did not establish this chain of liability. Therefore, UK insurers had less demand for cyber coverage and less actuarial loss data with which to underwrite, price, and scale such policies successfully.

In the event of a data breach, breach notification regimes established under HIPAA and the CCPA increased reputational and financial exposure for non-compliant organizations. These standards often demand disclosure within specific deadlines and provide for civil penalties and private litigation, even if the breach is caused by a third-party vendor. In contrast, the UK's early data protection rules did not include a comparable breach reporting mandate, nor was there any incentive for businesses to quantify or hedge cyber exposure through insurance.

While U.S. regulations established a clear link between regulatory liability, organizational vulnerability, and insurance adoption, the UK's more liberal and fragmented framework stalled both cyber insurance development and adoption. Without the threat of downstream liability, businesses viewed risk transfer tools such as standalone cyber insurance as discretionary rather than essential business instruments.

The advent of the EU's General Data Protection Regulation (GDPR) in 2018 raised awareness and drove some uptake of cyber insurance in the UK, however it did little to foster widespread adoption. Following the GDPR's implementation, larger UK businesses saw a moderate increase in standalone cyber insurance coverage, from 33 percent to 41 percent in 2019.[24] And an overwhelming majority of the UK insurance sector felt that the GDPR drove demand for cyber insurance even prior to its launch.[25]

But while the GDPR drove demand for cyber insurance, this demand was localized to larger firms, with smaller firms far less responsive. For example, between the announcement of the GDPR in 2012 and its adoption in 2018, over 30 percent of businesses made modifications to their cybersecurity policies, with most of the adjustments coming from large (62 percent) and medium-sized (51 percent) firms.[26] Only 18 percent of micro and small businesses reported changes.[27] Therefore, the GDPR had only a limited impact on the uptake of cyber insurance in the UK, and the UK still needs additional reforms to promote cyber insurance adoption on par with leading adopters such as the United States.

Unfortunately, the UK continues to work from its outdated 2018 transposition of the EU Network and Information Systems (NIS) Directive—designed to achieve a higher common level of cybersecurity across the EU by mandating essential service operators and digital service providers to improve the security of their networks and information systems and report significant incidents. Its limited scope and weak liability provisions have failed to address rising cyber threats. The 2018 NIS Directive covers a handful of critical sectors (energy, transport, health, water supply, and digital infrastructure) and some digital services (cloud, marketplaces, and search).[28]

Conversely, the EU's NIS2 Directive 2024, an update of the 2018 NIS Directive, substantially broadens the scope. It now applies across 18 sectors—including information and communications technology (ICT) providers such as managed service providers and data centers—and imposes clearer, stricter security requirements.[29] Evidence already suggests that this broader scope and imposed obligations incentivizes firms to adopt cyber insurance, with one study explicitly identifying the EU's NIS2 as a key driver of the global cyber insurance market.[30]

This lack of regulatory pressure that has led to the slow growth and adoption of cyber insurance in the UK is an indication that the new CSRB needs to deliver a fresh regulatory drive to stimulate quicker uptake.

Inconsistent UK Cyber Insurance Industry Practices Have Stifled Insurance Uptake

Current industry practices in the UK cyber insurance market—such as high premiums, complex insurance policy language, and inconsistent insurer requirements—undermine the widespread uptake of insurance. UK firms pay some of the highest cyber insurance premiums in the world, as compared with global counterparts such as the United States. Recent data shows that UK SMEs pay an average of £3,715 annually in premiums, while larger firms pay between £15,000

and £100,000.[31] In comparison, U.S. small businesses pay about $1,740 per year (roughly £1,380) on average. Higher pricing reflects a less established market with higher uncertainty, making coverage expensive for UK firms. The high-priced cyber insurance premium regime in the UK is a result of uncertainties created by current regulatory deficiencies and inconsistent industry practices.

The UK lacks a centralized reporting framework for cyber insurance, a crucial element of a thriving cybersecurity regime. In the United States for example, state regulators require insurers to submit detailed cyber data (premiums, claims, policies, and loss indicators) using the National Association of Insurance Commissioners cyber supplement.[32] Such records provide insurers with valuable datasets for risk modeling, pricing, and product development. There is no comparable obligatory data collection in the UK. Therefore, regulators and insurers lack reliable market-wide loss statistics. This lack of data impedes actuarial modeling and product innovation, driving high premium rates.

UK cyber insurance policies rely heavily on complex and technical language such as "operator of essential services" and "relevant digital service provider" (RDSP)—adopted from the EU 2018 NIS Directive—hampering the understanding of coverage underwriting. Moreover, following the NIS Directive limits the scope of policy coverage and introduces legal ambiguity on policy wording where the directive remains silent, such as what constitutes an "essential service" or "relevant digital service." Insurers can each interpret the same cyber incident differently according to their own definitions or risk frameworks, which makes it difficult for businesses to effectively compare policies or plan on whether claims will be covered.

In the absence of government-mandated definitions or baseline risk criteria, insurers rely on internally designed questionnaires and risk assessment techniques.

Varying definitions lead to disagreements about coverage eligibility, delayed payouts, and even litigation. This ambiguity undermines policyholders' trust in cyber insurance as a dependable risk transfer tool, particularly for responding to incidents such as state-sponsored cyberattacks. For example, in March 2019, the London-headquartered global law firm DLA Piper was struck by NotPetya malware that encrypted thousands of its servers.[33] Hiscox, the insurer, declined to pay the ensuing claim, citing the "act of war" exclusion on the basis that the UK government had concluded that NotPetya was "almost certainly" conducted by Russia's military. The law firm publicly threatened to sue over this interpretation, contending that NotPetya was a criminal act and not a warlike act and should therefore be covered.[34]

Another fundamental structural flaw of the UK's cyber insurance market is its fragmented and unregulated underwriting system, leading to a lack of consistent insurer requirements. In the absence of government-mandated definitions or baseline risk criteria, insurers rely on internally designed questionnaires and risk assessment techniques. This patchwork of approaches leads to varied methodologies across the market and variations in how insurers assess and price risk. As a result, businesses' expectations differ depending on the insurer, making it difficult to compare policies or make informed coverage decisions and deterring widespread uptake in necessary coverage. Standard requirements are necessary for the insurance industry, as they give insurers

and businesses flexibility in risk assessment while agreeing on common assumptions and indicators.

RECOMMENDATIONS

The CSRB represents a major step forward in addressing the United Kingdom's escalating cyber risks and strengthening its underdeveloped cyber insurance ecosystem. By introducing stricter statutory baselines for certain security measures, enhancing incident reporting, and establishing a supply chain resiliency focus, the bill corrects many of the shortcomings of the 2018 NIS Directive, as well as addresses some of the barriers to developing the cyber insurance market. However, the bill could go further to encourage the widespread uptake of cyber insurance, as it misses opportunities to promote insurer data access, develop policy standardization, adopt a size-neutral, risk-based approach to enforcement, and establish a reinsurance backstop to address catastrophic risk. Embracing these measures would go far to incentivize cyber insurance adoption across all firm sizes, creating a more secure and resilient UK business environment.

The CSRB is not without its merits. Most notably, it corrects the failings of the UK's present cybersecurity framework, influenced by the EU's 2018 NIS Directive. The most significant contribution is the creation of a consistent baseline for cyber risk assessments. This baseline implements the NCSC Cyber Assessment Framework (CAF) as the baseline security standard, regulated by the Information Commissioner's Office. CAF is a set of principles created to help businesses achieve and demonstrate robust cybersecurity, the purpose of which is to maintain a predictable and harmonized cyber risk environment while also conducting regular incident response planning, supply chain management, and vulnerability assessments.[35] By codifying CAF, the bill compels firms to go beyond written policies and routinely test and demonstrate operational capabilities, including incident response, vulnerability management, and supplier assurance. For the UK economy, this consistency provides a harmonized and predictable baseline, minimizing weak links in key sectors.

The bill misses opportunities to promote insurer data access, develop policy standardization, adopt a size-neutral, risk-based approach to enforcement, and establish a reinsurance backstop to address catastrophic risk.

Similarly, the bill expands regulatory scope to capture more entities, including more Managed Service Providers (MSPs), critical suppliers, and infrastructure such as data centers. This expanded scope creates clearer duties for firms, especially suppliers, which contributes to better supply chain resiliency and less third-party risk. By expanding its regulatory scope to include more MSPs, and other digital service providers, the bill also creates an urgent demand for cyber insurance among previously unregulated sectors of the UK digital economy, including the estimated 900–1,100 uncovered MSPs, directly affecting growth of the insurance market. MSPs have regularly served as conduits for cascading breaches, resulting in concentrated and correlated exposures across multiple organizations.[36] Therefore, bringing these digital service providers fully into regulatory purview decreases systemic tail risk, making losses more predictable and significantly improving insurability and capital planning for insurers.

Finally, the bill enhances the data environment that underpins actuarial modelling, with stricter incident reporting to regulators and the NCSC. Its two-stage reporting obligation to both the

relevant regulator and the NCSC, as well as broader incident definitions, produces richer, timelier data for risk modelling. This enhanced data addresses the current data vacuum that drives wide pricing dispersion of insurance premiums.

These measures go far to boost the growth of the cyber insurance industry, but not far enough to incentivize the adoption of cyber insurance by firms of all sizes. It lacks a necessary insurance data collection framework to boost its enhanced incident reporting scheme, fails to alleviate issues related to complex insurance policy language, takes an indirect approach to the uptake of cyber insurance across all businesses, and maintains a size-based view to certain entities and cyber requirements that undermine the bill's objectives of better overall UK security and resiliency. The UK government should adopt the following recommendations to address these gaps:

1. Establish a confidential cyber incident information exchange platform, require firms to participate, and publicly release an anonymized cyber incident dataset.
2. Create model cyber insurance wording and an underwriting glossary in partnership with key regulators and insurer bodies.
3. Introduce clearer, objective definitions for firms the bill captures.
4. Prioritize risk-based over size-based classifications for firms, infrastructure, suppliers, and other entities the bill captures.
5. Establish a state-backed cyber reinsurance pool to cover catastrophic risk from cyber incidents.
6. Launch a cyber insurance sandbox overseen by the Regulatory Innovation Office.

These recommendations will incentivize the adoption of cyber insurance, working in tandem with the CSRB's other proposed measures, which will encourage the industry's development.

Establishing a Confidential Cyber Incident Information Exchange Platform

While the bill mandates firms to simultaneously report to relevant regulators as well as the NCSC, it lacks an appropriate mechanism to streamline this incident data into a single repository that could feed into insurer premium calculations and improvements. This is a lost opportunity, as insufficient loss data is a major impediment to cyber insurance market development.[37]

The dual-reporting approach as proposed in the CSRB risks producing data silos, impeding the development of an integrated intelligence system required by a mature insurance market. The simultaneous reporting between the sectoral regulator and the NCSC runs the risk of duplicative data as well as overburdens the NCSC as the single point of contact to both receive and manage and subsequently share incident data with relevant parties. Without formal data-sharing agreements with the insurance industry, critical incident data becomes locked within regulatory channels, restricting insurers' ability to develop accurate models and competitive pricing. This lock-in, in turn, limits the creation of more accessible and affordable coverage, preventing the broad adoption of cyber insurance.

Unfortunately, the NCSC has decommissioned the platform for cybersecurity information sharing—Connect, Inform, Share, Protect (CISP)—leaving a significant gap for how government

and industry can streamline cyber incident reporting to a single source. To better support the CSRB's proposed enhanced incident reporting obligations on firms, the bill should establish a new information sharing platform housed within the NCSC, such as creating a new information sharing service within the NCSC's Active Cyber Defence 2.0 (ACD 2.0).

ACD 2.0 aims to build the next generation of services in partnership with industry and academia to help organizations protect themselves against cyber threats. ACD 2.0 comprises several services organizations it can leverage, some of which are developed in house by the NCSC, to address security vulnerability and detect and disrupt attacks. As part of this package of services, the NCSC should introduce a CISP-style framework that all entities—industry, academia, and government—should feed into in order to satisfy their reporting obligations, ensuring a secure and confidential information exchange. Such a platform could be accessed by government regulators, facilitating firm obligations to report to both the relevant regulator and the NCSC.

To support this incident data feeding into the calculation of insurer premiums, the bill should require the NCSC to release and maintain an anonymized, publicly accessible cyber incident dataset. Such a dataset would provide crucial, up-to-date information for the calculation of premiums, acting as a strong foundation for actuarial modelling that leads to more accurate, relevant insurance premiums.

Creating Model Cyber Insurance Wording and an Underwriting Glossary

The bill fails to address ambiguous policy language, which leads to coverage disputes and market uncertainty.[38] An example is the dilemma of silent cyber risk, wherein traditional insurance policies (e.g., property or liability) do not expressly include or exclude cyber incidents.[39] This ambiguity makes businesses uncertain whether they are protected after an attack and exposes insurers to unpriced liabilities, weakening trust on both sides.

The bill misses a golden opportunity to enhance the fundamentals of a sustainable and transparent cyber insurance industry by failing to clarify and standardize policy wording. Indeed, the Organization for Economic Co-operation and Development (OECD) has underlined that imprecise policy language increases the possibility of conflicts between policyholders and insurers.[40]

The bill should address these issues by provisioning model cyber insurance wording and an underwriting glossary, such as introducing both through secondary legislation after working with key regulators and insurer bodies to agree on standard terms. Clear, standard policy language would promote insurance adoption, as companies have better certainty over their coverage.

Introducing Clearer, Objective Definitions for Firms the Bill Captures

The bill is right to expand the scope of cybersecurity obligations to more MSPs, as doing so brings more firms into compliance; however, policymakers should ensure that this coverage remains relevant and not overly broad. A lack of definitional clarity over what constitutes an MSP runs the risk of capturing more entities than is needed, leading to increased unnecessary compliance burdens and confusion over insurer coverage.

The bill defines managed services as those that provide "ongoing management of information technology systems for the customer (whether in the form of support and maintenance, monitoring, active administration or other activities)" and "connecting to or otherwise obtaining

access to network and information systems relied on by the customer in connection with a business or other activity carried on by the customer."[41] These definitions fail to establish objective thresholds or clear exclusion criteria—issues currently faced by the UK cyber insurance market.

This definitional ambiguity poses serious challenges to the approximately 1,000 new MSPs set to be captured under the bill because providers cannot accurately assess their regulatory status, compliance requirements, or associated penalties. The vague language risks inadvertently capturing low-risk firms while potentially excluding true high-risk providers. To address this ambiguity in defining MSPs, the bill should draw on objective definitions from the U.S. Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).

CIRCIA defines an MSP as any entity providing network, application, infrastructure, or security services via continuous, active monitoring and management—whether on a customer's premises, in the provider's own data center, or at a third-party facility.[42] CIRCIA's explicit statutory definition of MSPs ensures that only entities with significant access to and management over critical infrastructure systems are subject to federal oversight and incident reporting. This targeted scope eliminates uncertainty by bringing all 16 critical infrastructure sectors in the United States under one compliance framework.

The standardization allows the Cybersecurity and Infrastructure Security Agency (CISA) to apply consistent risk assessments, incident analysis, and supply chain management. It also improves compliance, simplifies information exchange and data gathering, and supports the adoption of frameworks such as the National Institute of Standards and Technology (NIST) Risk Management Framework, ultimately boosting the national cybersecurity baseline through standardized third-party risk management. Therefore, the CSRB should adopt the CIRCIA approach that quantifies MSPs based on key operational and service delivery parameters to ensure tight scoping of captured entities. These parameters should include the scope of service offered (e.g., network, application, infrastructure, or security) and the type of support (active administration on a regular and ongoing basis).

Furthermore, the bill should specify quantitative thresholds for MSPs, such as level of network access and degree of system control or administrative rights. These thresholds would help delineate between entities offering significant management and operational control and those providing more limited or ad hoc services that do not require extra cybersecurity. This level of clarity would ensure consistent regulatory application and also allow insurers to develop standardized risk assessment frameworks based on consistent definitions, which are critical for market growth.

Prioritizing Risk-Based Over Size-Based Classifications

Despite the partial acknowledgment of size-neutral risk, the bill continues to adopt various problematic size-based thresholds that are inconsistent with risk-based regulatory ideals. While the bill correctly includes data centers in its scope due to their growing role as critical national infrastructure, it employs a capacity-based threshold, resulting in a tiered regime: ordinary facilities are regulated at 1 megawatt (MW) of capacity, whereas "enterprise" data centers are only regulated once they exceed 10 MW. This tenfold disparity incorrectly assumes that enterprise sites represent less systemic risk since they are primarily internal-facing—a notion that does not reflect the reality of modern, interconnected service dependencies.

The bill also overlooks the fact that cyber risk does not relate to physical capacity—a smaller data center supporting critical infrastructure may present more systemic risk than does a larger enterprise facility with minimal external connectivity. The size-based enforcement reflects the UK's flawed attempt to model the CSRB after the EU's NIS2 Directive, which adopts size-based thresholds to determine regulatory scope. Exempting micro and small RDSPs automatically leads to regulatory loopholes. While regulators may recognize these firms as critical suppliers, doing so requires special action, meaning size is still considered as a baseline rather than actual risk. As a result, smaller entities below regulatory thresholds—yet critical to digital supply chains—become attractive targets for cyberattacks. The bill should adopt a risk-based classification for captured entities, avoiding modelling the CSRB on the NIS2 Directive's size-based approach. A risk-based enforcement focused predominantly on firm activities such as the types of data a firm handles will ensure effective cybersecurity practices based on the threat an attack would pose to an organization, while avoiding prejudicing based on ambiguous classifiers such as firm size.

As part of this risk-based classification, the bill could impose smaller obligations across the board that make an immediate difference to the security of a firm. For example, the bill should explicitly mandate low-cost phishing-resistant technologies such as multi-factor authentication (MFA) to address the UK's most common attack vector.[43] Including an explicit MFA requirement would ensure that all organizations have a consistent baseline of strict access control, reducing the risk of unauthorized access due to compromised or stolen credentials—a leading cause of cyber incidents.[44]

Establishing a State-Backed Cyber Reinsurance Pool

Although modernizing the UK's cybersecurity framework will promote the adoption of cyber insurance indirectly, the bill does little to connect CSRB requirements directly with insurance adoption mechanisms. Most importantly, the bill does not tackle the increasing exclusion of state-sponsored cyberattacks from insurance policies—exactly the space where government involvement is most required.

Insurance firms such as Lloyd's of London have now made exclusions mandatory for losses stemming from state-sponsored cyberattacks that "significantly impair the ability of a state to function," leaving considerable uninsured risk exposure.[45] This exclusion impacts standalone cyber policies as well as traditional insurance lines, leaving organizations financially vulnerable to the most impactful threat vectors recognized by the bill.

The bill should create a state-backed cyber reinsurance pool to address catastrophic risks from state-sponsored cyberattacks as well as other large-scale cyberattacks that overwhelm private insurance capacity, modelled after the 1993 Pool Re framework. The Pool Re program was created after commercial insurers withdrew from terrorism coverage during the Irish Republican Army (IRA) bombing campaign in London.[46] The program allowed insurers to pool their resources to collaboratively cover terrorism risks, backed by an unlimited government guarantee to pay claims even if Pool Re depleted its reserves. This structure reassured insurers that they could offer terrorism coverage without fearing financial ruin, therefore maintaining market stability and saving the UK economy from the financial impact of terrorism-related losses.

A reinsurance pool for catastrophic cyberattacks, structured in a similar fashion to Pool Re that allows insurers to pool resources backed by government, would address current gaps in insurance coverage for losses that exceed insurer capacity. Of course, the reinsurance pool would not need

to completely mirror Pool Re, and could instead be structured with linear triggers based on incident type, coverage for intangible losses such as data loss, business interruption, and liability, and reliance on specialized underwriting and models that reflect fast-moving technical, supply-chain, and geopolitical risks.

A reinsurance pool for cyber-related losses would provide UK insurers with the confidence to cover cyber incidents irrespective of the attack vector. It would minimize volatility in the cyber insurance market, support insurers suffering large-scale losses, and stimulate broader uptake of cyber insurance through government coinsurance for damages exceeding defined thresholds.

Launching a Cyber Insurance Sandbox

The bill should establish Financial Conduct Authority (FCA)-style regulatory sandboxes for cyber insurance innovation, drawing on the proven model that has been adopted by more than 70 countries since the FCA's inception in 2016.[47]

An FCA-style "regulatory sandboxes" offer supervised, controlled spaces for companies to test innovative products, services, or technologies with actual customers while temporarily relaxing certain regulatory requirements. This sandbox technique is particularly advantageous to new entrants and established firms looking to test cutting-edge technologies.

The regulatory sandbox should be standalone, operated jointly by the FCA and the Prudential Regulation Authority (PRA). Cyber insurance innovation encompasses both conduct and prudential risks—the FCA's mandate addresses market conduct, consumer protection, and policy clarity, whereas the PRA regulates insurer safety, solvency, and capital adequacy.[48] The FCA's existing sandbox focuses on fintech and conduct issues, but cyber insurance also necessitates PRA expertise on severe loss modelling, systemic risk, and capital requirements—supervisory priorities the PRA has already identified.

A joint sandbox would utilize the FCA-PRA Memorandum of Understanding (MOU) to deliver a single entry point, coordinated supervision, and clear delineation of responsibilities (FCA on conduct, PRA on prudential safety), preventing duplicated processes and regulatory uncertainty.[49] The FCA-PRA MOU is a high-level framework that outlines how the FCA and the PRA will collaborate, coordinate, and share information when carrying out their respective regulatory and supervisory responsibilities, particularly wherever their remits overlap. This combined testing environment would deliver innovation while protecting policyholders and the financial system against the distinctive risks of cyber insurance products.

The regulatory sandbox is a strong model for cyber insurance because it would allow UK cyber insurers to test cutting-edge technologies, such as AI-driven underwriting models, dynamic pricing platforms, and real-time risk analysis tools, without imposing up-front full regulatory compliance costs. The framework should prioritize AI-led innovations that promote ongoing risk monitoring and behavior-linked pricing models where premiums vary based on cybersecurity posture—for example, adopting multi-factor authentication, keeping security patches up to date, or demonstrating improved incident response capabilities.

The approval process should include expedited pathways for technologies that address new cyber threats and market gaps. It should also include clear criteria that require genuine innovation, regulatory uncertainty justification, and sufficient product development readiness to allow live

testing with actual customers. This structured approach ensures that successful innovations can move quickly from testing to full market deployment while maintaining appropriate consumer protection safeguards.

The growth and sophistication of the UK's cyber insurance market through regulatory sandbox innovation would position the nation at the forefront of global cyber resilience, complementing the government's ambitions to stimulate economic growth while securing critical national infrastructure. Establishing homogeneous criteria would equip insurers with adequate data to price risk accurately and compete on a level playing field.

CONCLUSION

The CSRB aims to strengthen the UK's national cyber defenses by modernizing outdated frameworks. A bill that supports a thriving cyber insurance market will deliver economic benefits by enhancing organizational resilience, reducing operational interruptions from cyber incidents and minimizing financial losses from cyber incidents as more firms obtain financial protection. By adding specific provisions to the CSRB to support cyber insurance, the UK will realize major advancements in its cyber insurance industry, contributing to the nation's overall cyber resilience. The growth of the cyber insurance market in the UK will position the nation at the forefront of global cyber resilience, complementing the government's ambitions to stimulate economic growth while securing critical national infrastructure. Furthermore, a thriving UK cyber insurance market has the potential to contribute to the national economy, fostering job creation and innovation in addition to providing critical support to other industries seeking security and risk mitigation.

About the Authors

Samuel Agyarko Koranteng is a candidate for the Master of Science in Cybersecurity and Public Policy at The Fletcher School, Tufts University, with complementary legal training in technology and cybersecurity from Harvard Law School. He focuses on cyber risk management, privacy policy, and the governance of emerging technologies, particularly artificial intelligence.

Ayesha Bhatti is head of digital policy for the United Kingdom and EU at ITIF's Center for Data Innovation. Prior to joining, she worked as a data scientist at a technology consulting firm in London. She has an LL.B. from the University of Nottingham, and an M.Sc. in Computer Science from Birkbeck, University of London. She is also a licensed attorney in the state of New York.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent 501(c)(3) nonprofit, nonpartisan research and educational institute that has been recognized repeatedly as the world's leading think tank for science and technology policy. Its mission is to formulate, evaluate, and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. For more information, visit itif.org/about.

ENDNOTES

1. IBM, "2025 IBM X-Force Threat Index: UK Remains Most-Attacked Country in Europe as Large-Scale Credential Theft Escalates," IBM Newsroom, April 17, 2025, https://uk.newsroom.ibm.com/2025-IBM-X-force-threat-index-uk-remains-most-attacked-country-in-europe.
2. National Cyber Security Center, "NCSC Annual Review," UK Government, December 2024, https://www.ncsc.gov.uk/files/NCSC_Annual_Review_2024.pdf.
3. Ani Petrosyan, "Estimated annual cost of cybercrime in the United Kingdom (UK) from 2017 to 2028," *Statista*, July 2, 2025, https://www.statista.com/forecasts/1425776/uk-cybercrime-cost-annual#statisticContainer.
4. Department for Science, Innovation & Technology, "Cyber security breaches survey 2024," UK Government, April 9, 2024, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024.
5. Department for Science, Innovation & Technology, "Cyber security breaches survey 2025," UK Government, June 19, 2025, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025.
6. Amy Dawson, "87% of UK organisations are vulnerable to cyberattacks in the age of AI, research reveals," Microsoft UK, March 18, 2024, https://ukstories.microsoft.com/features/87-of-uk-organisations-are-vulnerable-to-cyberattacks-in-the-age-of-ai-research-reveals/.
7. Anna Ribeiro, "NCSC warns UK critical systems face rising threats from AI-driven vulnerabilities," Industrial Cyber, May 9, 2025, https://industrialcyber.co/threats-attacks/ncsc-warns-uk-critical-systems-face-rising-threats-from-ai-driven-vulnerabilities/.
8. Kathleen Magramo, "British engineering giant Arup revealed as $25 million deepfake scam victim," CNN Business, May 17, 2024, https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk.
9. Ravie Lakshmanan, "Scattered Spider Behind Cyberattacks on M&S and Co-op, Causing Up to $592M in Damages," *The Hacker News*, June 21, 2025, https://thehackernews.com/2025/06/scattered-spider-behind-cyberattacks-on.html.
10. Ed Williams, "A chain reaction: inside the cyberattack that brought M&S to its knees," Tech radar, July 22, 2025, https://www.yahoo.com/news/articles/chain-reaction-inside-cyberattack-brought-084444657.html.
11. Laura Onita, "M&S turned to FBI for help after 'traumatic' cyber attack'," *Financial Times*, July 8, 2025, https://www.ft.com/content/83d362a3-7c11-4c8f-bd33-ff45454cea72.
12. Maria Ward-Brennan, "M&S, Co-op and Harrods attacks drive demand for cyber insurance," City AM, May 12, 2025, https://www.cityam.com/ms-co-op-and-harrods-attacks-drive-demand-for-cyber-insurance/.
13. Jordan Sollof, "Cyber attack cost Synnovis estimated £32.7m in 2024," Digital Health, January 20, 2025, https://www.digitalhealth.net/2025/01/cyber-attack-cost-synnovis-estimated-32-7m-in-2024/.
14. Molly Lempriere, "Elexon files posted online following May's ransomware attack," Solar Power Portal, June 8, 2020, https://www.solarpowerportal.co.uk/solar-technology/elexon-files-posted-online-following-may-s-ransomware-attack.
15. IBM, "IBM Security Report: Energy Sector Becomes UK's Top Target for Cyberattacks as Adversaries Take Aim at Nation's Critical Industries," IBM Newsroom, February 23, 2022, https://uk.newsroom.ibm.com/2022-02-23-IBM-Security-Report-Energy-Sector-Becomes-UKs-Top-Target-for-Cyberattacks-as-Adversaries-Take-Aim-at-Nations-Critical-Industries; Finastra, "Finastra Statement on Cyberattack," April 3, 2020, https://www.finastra.com/sites/default/files/2020-04/Finastra-customer-letter_040420_BR_FIN.pdf.

16. Department for Science, Innovation & Technology, "Cyber security breaches survey 2025."
17. Department for Science, Innovation & Technology, "Cyber security breaches survey 2024."
18. Association of British Insurers, "SMEs consider themselves 'too small' to fall victim to cyber-attacks - according to new ABI report," The ABI, January 1, 2025, https://www.abi.org.uk/news/news-articles/2025/1/abi-launches-new-cyber-guide-for-smes/.
19. Josephine Wolff, "Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks," *The MIT Press*, 2022, https://direct.mit.edu/books/oa-monograph/5373/Cyberinsurance-PolicyRethinking-Risk-in-an-Age-of.
20. Steve Alder, "HIPAA Violation Fines – Updated for 2025," *The HIPAA Journal*, accessed August 3, 2025, https://www.hipaajournal.com/hipaa-violation-fines/.
21. Mark Camillo, "Cyber risk and the changing role of insurance," *Journal of Cyber Policy Vol 2, NO 1*, 53–63, 2017, https://www.tandfonline.com/doi/epdf/10.1080/23738871.2017.1296878.
22. Ibid.
23. UK Parliament, "Data Protection Act 1984, c. 35," accessed July 26, 2025, https://www.legislation.gov.uk/ukpga/1984/35/enacted.
24. Hiscox, "Hiscox Cyber Readiness Report 2019," accessed August 3, 2025, https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf.
25. Jennifer Frost, "GDPR leading to increased cyber insurance uptake," *Insurance Times*, December 15, 2017, https://www.insurancetimes.co.uk/gdpr-leading-to-increased-cyber-insurance-uptake/1425849.article.
26. Oxera Consulting LLP, "The Value of Cyber Insurance to the UK Economy" (prepared for the Association of British Insurers), November 2020, https://www.abi.org.uk/globalassets/files/subject/public/cyber/the-value-of-cyber-insurance-to-the-uk-economy-november.pdf.
27. Ibid.
28. The Network and Information Systems Regulations of 2018, accessed July, 26, 2025, https://www.legislation.gov.uk/uksi/2018/506/regulation/1/2018-05-10.
29. "Understanding the NIS2 Directive: Strengthening Cybersecurity Across the EU," ENISA, accessed July 26, 2025, https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/raising-awareness-campaigns/network-and-information-systems-directive-2-nis2.
30. "Cybersecurity Insurance Market worth $32.19 billion by 2030," Markets and Markets, July 18, 2025, https://www.marketsandmarkets.com/PressReleases/cyber-insurance.asp.
31. "Cyber security measures 'cost SMEs £60,000 a year," *CIR Magazine*, July 25, 2024, https://www.cirmagazine.com/cir/c2024072502.php; Get Indemnity, "Compare active cyber insurance quotes for small business and corporates," accessed July 26, 2025, https://getindemnity.co.uk/business-insurance/cyber/how-much-does-cyber-insurance-cost.
32. National Association of Insurance Commissioners (NAIC), "NAIC 2024 Cyber Insurance Market Report (Cyber Insurance Report to Property & Casualty and Innovation, Cybersecurity & Technology Committees)," October 15, 2024, accessed August 3, 2025, https://content.naic.org/sites/default/files/cmte-h-cyber-wg-2024-cyber-ins-report.pdf.
33. Jonathan Crowe, "How One of the World's Largest Law Firms Was Paralyzed by Petya," Barkly Protects Inc., July 2017, https://harryphillipsaic.com/wp-content/uploads/2018/10/How-One-of-the-World%E2%80%99s-Largest-Law-Firms-Was-Paralyzed-by-Petya-01810088.pdf.

34. "Law firm sues Hiscox over ransomware attack claim," Business Insurance, March 26, 2019, accessed August 3, 2025, https://www.businessinsurance.com/law-firm-sues-hiscox-over-ransomware-attack-claim/.
35. National Cyber Security Center, "Introduction to the Cyber Assessment Framework," UK Government, accessed August 5, 2025, https://www.ncsc.gov.uk/collection/cyber-assessment-framework/introduction-to-caf.
36. SOC Radar, "How Are MSPs (Managed Service Providers) at Risk of Data Breaches?" SOC, October 11, 2023, https://socradar.io/how-are-msps-managed-service-providers-at-risk-of-data-breaches/.
37. Cybersecurity and Infrastructure Security Agency, "Assessment of the Cyber Insurance Market," CISA, December 2018, https://www.cisa.gov/sites/default/files/2024-10/OCE%20Cyber%20Insurance%20Market%20Assessment_508.pdf.
38. International Association of Insurance Supervisors, "Cyber Risk Underwriting Identified Challenges and Supervisory Considerations for Sustainable Market Development," IAIS, December 2020, https://www.iais.org/uploads/2022/01/201229-Cyber-Risk-Underwriting_-Identified-Challenges-and-Supervisory-Considerations-for-Sustainable-Market-Development.pdf.
39. Bethan Moorcraft, "What is silent cyber risk?" *Insurance Business*, November 26, 2018, https://www.insurancebusinessmag.com/us/guides/what-is-silent-cyber-risk-117150.aspx.
40. "Encouraging Clarity in Cyber Insurance Coverage; The Role Of Public Policy And Regulation," OECD, 2020, https://www.oecd.org/daf/fin/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf.
41. Cyber Security and Resilience (Network and Information Systems) Bill, UK Government, accessed December 2025, https://bills.parliament.uk/bills/4035.
42. Cyber Incident Reporting for Critical Infrastructure Act of 2022, H.R.5440, 117th Cong. (2021–2022), accessed August 2, 2025, https://www.cisa.gov/sites/default/files/2023-01/Cyber-Incident-Reporting-ForCriticalInfrastructure-Act-o-f2022_508.pdf.
43. Charles Griffiths, "The Latest 2025 Phishing Statistics," AAG IT Solutions, June 1, 2025, https://aag-it.com/the-latest-phishing-statistics/.
44. Alexander Petrovski, "10 Biggest Data Breaches in the UK [2025]," Corbado, May 11, 2025 [Updated: August 8, 2025], https://www.corbado.com/blog/data-breaches-UK.
45. Tony Chaudhry, "State backed cyber-attack exclusions," Lloyd's of London, August 16, 2022, https://assets.lloyds.com/media/35926dc8-c885-497b-aed8-6d2f87c1415d/Y5381%20Market%20Bulletin%20-%20Cyber-attack%20exclusions.pdf.
46. Reinsurance (Acts of Terrorism) Act of 1993, UK Public General Acts1993 c. 18, accessed August 2, 2025, https://www.legislation.gov.uk/ukpga/1993/18/introduction.
47. Financial Conduct Authority, "Digital Sandbox," accessed July 26, 2025, https://www.fca.org.uk/firms/innovation/digital-sandbox.
48. Prudential Regulation Authority, "Cyber insurance underwriting risk," The Bank of England, November 2024, https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2024/ss417-november-2024-update.pdf.
49. Financial Conduct Authority & Prudential Regulation Authority, "Memorandum of Understanding between the Financial Conduct Authority and the Prudential Regulation Authority," Bank of England, April 2024, https://www.bankofengland.co.uk/-/media/boe/files/memoranda-of-understanding/fca-and-pra.pdf.