Cyber Security: The Billion Pound Risk

January 2026

W: www.csa-uk.com / **LinkedIn:** credit-services-association / **LinkedIn:** csa-learning / **YouTube:** Credit Services Association

Introduction

In October 2025, the Cyber Monitoring Centre (CMC), a non-profit organisation that monitors and classifies cyber-security incidents, estimated that the cyber-attack on Jaguar Land Rover caused a UK financial impact of £1.9 billion, making it "the most economically damaging cyber event to hit the UK"[1].

In the same month, a fine of £14 million was levied against Capita for data protection failings following a cyber-attack[2].

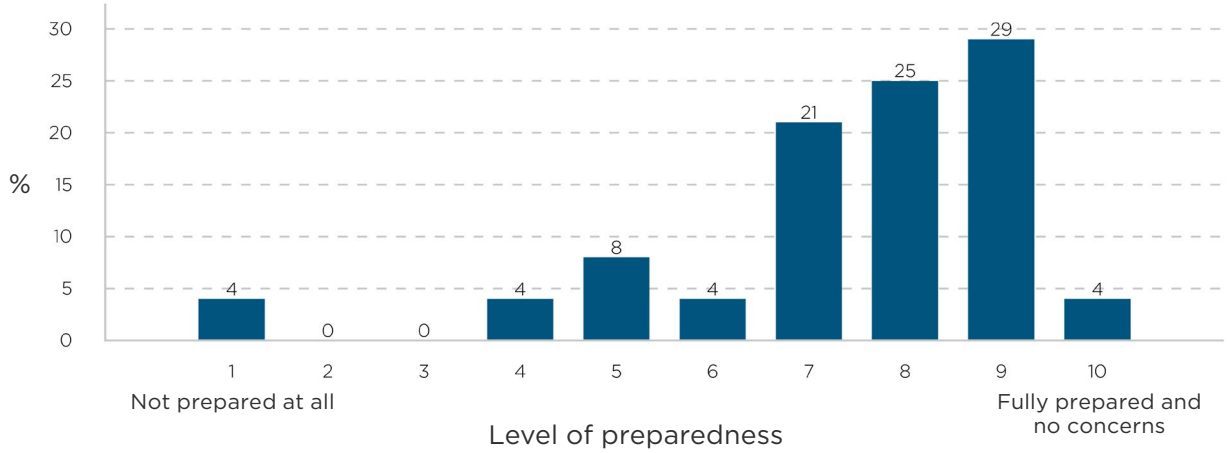
Whether we are talking millions, billions or thousands of pounds, the reality is that cyber-security is an incredibly costly risk for all businesses and it should be treated accordingly. The damage that a firm can be exposed to from a cyber-attack covers a multitude of areas – operational, regulatory, reputational – and could cost firms dearly in each.

And these days, cyber risk does not just mean being exposed to a cyber-attack. Firms have to think about how resilient their cyber capabilities are, as more and more firms rely on many of the same technology providers for their infrastructure and services, bringing with it the risk of widespread damage from a single outage. In October 2025, "errors and connectivity issues" caused an outage at Amazon Web Services, which took down many of its clients' apps and websites in the process, including Lloyds Bank, Starbucks, Snapchat and BT. This particular incident may not have been the result of a cyber-attack but it does show the dependency and interconnectivity between cyber-security and cyber-resilience.

With a reported 50% rise in "highly-significant" cyber-attacks in the last year, the National Cyber Security Centre (NCSC) has urged organisations to make cyber resilience a Board-level responsibility. Dr Richard Horne, Chief Executive at the NCSC, calls cyber-security "a matter of business survival and national resilience"[3].

Preparedness for a cyber attack (scale of 1-10)

Figure 1: CSA survey, Q4 2025



1. Cyber Monitoring Centre: Statement on the Jaguar Land Rover Cyber Incident (October 2025)
2. Information Commissioner's Office: Capita fined £14m for data breach affecting over 6m people (October 2025)
3. National Cyber Security Centre: UK experiencing four 'nationally significant' cyber attacks every week (October 2025)

"Rising numbers of cyber incidents make it critical that firms explore how they can improve their preparations and learn from other incidents, as bad actors are always looking for new avenues to exploit."

The collections and purchase sector may be relatively niche but it holds huge volumes of data and is tightly interwoven with a number of major creditor sectors, including consumer credit, energy and government.

It is therefore a potential target for bad actors. Even the smallest DCA could hold a considerable number of consumer records. While having state-of-the-art security measures may not be viable for a smaller firm, there are a range of tools and practices firms can employ to keep themselves secure.

In a recent survey of the CSA membership, members rated their preparedness for a cyber-attack on average around 8 or 9 out of 10 (see Fig.1), suggesting that there is a great deal of assuredness among respondents, but there is also a recognition that there is scope to enhance preparations. Rising numbers of cyber incidents make it critical that firms explore how they can improve their preparations and learn from other incidents, as bad actors are always looking for new avenues to exploit.

Does your organisation hold cyber insurance?

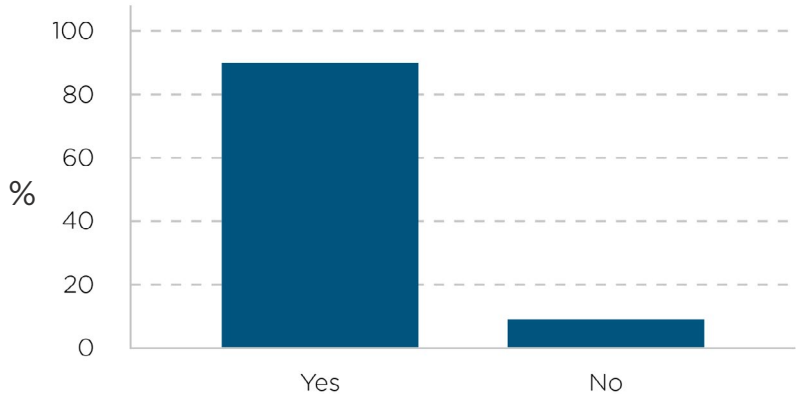


Figure 2: CSA member survey, Q4 2025

In terms of protecting themselves against the consequences of a cyber-attack, almost 90% of respondents to the survey reported having cyber insurance in place. But it is not enough to simply cover yourself. In the same way that a home insurance provider isn't going to pay out on a burglary where you left the front door wide open, businesses have to do as much as they can to protect themselves if their cyber insurance is ever to be worth the paper it's written on.

In the face of mounting numbers of cyber-attacks, we are encouraging CSA members to prioritise their cyber-security.

- Make sure you understand your business' cyber-security risks.
- Continually review your cyber resilience.
- Ensure that you or your IT provider are monitoring developments and risks.
- Incorporate cyber-security into your governance.

Investing now in security and resilience measures will better protect you in the future. Cyber-criminals are only getting more and more sophisticated, while the ability for even amateurs to carry out cyber-attacks is made even easier by artificial intelligence tools.

But, to return to Dr Richard Horne's comments, cyber-security is a matter of "national resilience" and, with that in mind, it should not just be for firms to defend themselves alone. Policymakers, stakeholders and regulators must provide essential support and measures to keep UK organisations secure. That means setting clear expectations for all firms especially around data retention and security requirements; ensuring that organisations and sectors are protected from critical third-party failures; and maintaining awareness across businesses about emerging cyber risks.

Threat Landscape

There is a growing array of cyber threats in the UK collections and purchase sector, many of which mirror those that the wider financial services sector face. The specific details of an individual cyber-attack may vary but some of the most common attacks tend to be:

Phishing/Social engineering

This can come in two different forms – on the one hand, criminals can attempt to extract information from staff by pretending to be the customer, using already-obtained partial details; or they can target consumers themselves, impersonating collections firms or creditors, in order to secure information. In its 2025 Global Threat Report[4], cyber-security solutions provider, CrowdStrike, reported a 442% increase in vishing (voice phishing) between the first and second half of 2024. The goal is ultimately to extract sensitive information about individuals which can then be exploited for financial gain, in many cases for identity theft.

Traditionally, phishing communications contained various red flags such as grammatical and spelling errors, but recent reports indicate that AI is enabling perpetrators to fix these issues, making it trickier for recipients to spot phishing communications.

Malware/Ransomware

Malware, where malicious software is used as part of the attack, is one of the most common types of cyber-attack, largely because it encompasses a range of different types of attacks.

But in recent years, ransomware has become one of the key malware threats, with the NCSC describing ransomware as "one of the most acute and pervasive cyber threats to UK organisations"[5]. Ransomware involves malicious installations on business devices which allow cyber criminals access – key data is then encrypted and/or stolen, with hackers demanding payment for its release.

In July 2025, the UK Government announced plans to prohibit payment to hackers, in order to deter the practice – if you can't get the money from firms, it may become less desirable to carry out, or at the very least, the crime won't be worth the initial cost of carrying it out. However, the proposals have been met with some concern[6], with some warning that it risks the collapse of essential services if organisations have no viable route to negotiation with criminals. In its reporting, the Financial Times cited the State of Ransomware 2025 report from cyber security firm, Sophos, as stating that almost 50 per cent of companies hacked in 2024 paid a ransom, so such a change would require a significant reversal in current practices. The proposal also carries the risk of cross-border firms off-shoring operations to permit them to take a different approach should the need arise, potentially creating a two-tier approach – thereby undermining the very goal of the change.

85%

of businesses attacked in the last 12 months experienced a phishing attack, making it the most prevalent and disruptive type of breach.

Figure 3: Cyber security breaches survey 2025 - Department for Science, Innovation & Technology[7]

4. Crowdstrike: Global Threat Report 2025 (August 2025)
5. National Cyber Security Centre: NCSC Annual Report 2025 (October 2025)
6. Financial Times: UK cyber ransom ban risks collapse of essential services (November 2025)
7. Gov.uk: Cyber security breaches survey 2025 (June 2025)

Other factors amplifying the risk

Data breaches: A cyber-attack can often result in a breach of data protection law. This means that along with the cyber-attack itself, the firm in question may have to contend with the consequences of a data breach too. For consumers, a data breach could lead to identity theft and fraud; for firms it can bring regulatory consequences and costs, which are considerable when it comes to data protection, not to mention the inevitable reputational damage. In the collections and purchase sector, a sector that is extremely reliant on outsourcing, the kind of reputational damage caused by a data breach could seriously damage a firm's credibility if clients think their data is exposed to significant risk.

More routes in: Technological advancement and innovation have been key focuses for many firms in recent decades and has arguably gone into overdrive as firms look to capitalise on the explosion of AI-powered tools. This rapid digital transformation has huge benefits in terms of efficiencies and consumer journey – but it also introduces new risks to the business. Each digital touchpoint becomes a potential entry point for cyber-criminals and it is often the case that firms focus on bringing in the new system first and the security measures to protect that system later.

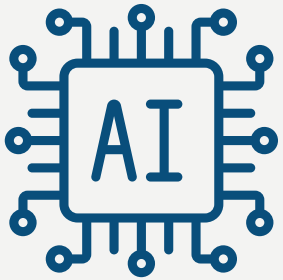
Legacy infrastructure: One of the most widely-cited challenges to cyber resilience and cyber-security is reliance on legacy systems. It is not just that they may lack modern security features but that they are not designed to integrate effectively into newer systems. It can also be difficult to retain the necessary institutional knowledge for managing legacy systems, exposing them further to attack. While moving away from legacy systems may appear the simplest and most effective way to build up cyber resilience, it can be debilitatingly costly for firms, especially SMEs, making it a challenging solution for many.

Reliance on cloud infrastructure: Cloud storage makes a lot of sense as it is a cost-effective route to large-scale data storage and accessing more sophisticated digital tools that may otherwise be inaccessible. But misconfiguration when migrating to or storing data in cloud environments can be a major risk for data breaches. Cloud infrastructure is often underpinned by a critical third-party supplier, where a single issue could cause problems at hundreds or thousands of organisations.

Investment: Cyber-security can be incredibly complex and explaining the risks involved can require a large amount of technical detail, which may not always be the forte of senior management. If senior managers cannot grasp the scale or significance of the underlying risks – whether down to their own understanding of the risk, or the manner in which it is being articulated – they are less likely to approve the investment required to protect the business.

Governance: Investment is closely linked with the extent to which organisations have effective cyber-security governance. Board directors and senior management may lack the necessary cyber expertise to digest all business security risks and associated mitigations, which can leave firms exposed.

AI: The growing use of AI presents plenty of opportunities for businesses, but at the same time the growth in its wider public use can represent a threat to firms as it effectively makes it easier for individuals to carry out cyber-attacks. Research carried out as part of Infosecurity Europe's 2025 report on cyber-security trends[8] found that 64% of cyber-security professionals agree that AI will result in increased cyber-attacks on their organisation, with 78% reporting that AI will force them to overhaul their security strategy.



78%

of cybersecurity professionals report that AI will force them to overhaul their security strategy.

8. Infosecurity Europe: Cybersecurity Trends Report 2025 (March 2025)

What steps can firms take?

Whether you are a micro-enterprise, an SME or a large organisation, there are a wide range of steps you can take to protect your organisation, accredit your security measures and provide reassurance to both consumers and counterparties.

Make sure it is taken seriously throughout the organisation: Cyber-security does not start and end with the IT department. It affects everyone and demands appropriate governance. The NCSC has advocated for cyber governance training for boards of directors. Director-level comprehension of the risks posed and the mitigations taken by the business is key to ensuring there is adequate investment in cyber-security and necessary precautions are taken across the business. It also sets a standard across the organisation.

Be proactive: In the same way that firms are expected to design systems and processes with 'data protection by design', firms should be doing the same with their cyber-security. And with the increasing volume and sophistication of attacks, firms cannot rest on their laurels; they must be proactive in identifying and tackling cyber-security risks, if they are to remain resilient.

Training: All staff should be routinely trained on cyber-security awareness. They should understand the different types of cyber-attack, particularly the kinds they are most likely to encounter, such as phishing and social engineering. Regular training will also ensure employees are up-to-speed on developments, as cyber risks and attacks change, especially as perpetrators refine their approaches and address some of the more identifiable red flags, such as spelling and grammar errors.

Preparation and testing: Organisations should have a comprehensive cyber incident plan. And that plan should be tested with appropriate regularity. Staff preparedness and awareness, as well as the adequacy of other controls, can be assessed through security audits and penetration testing. These should look at all points of exposure and firms should act swiftly and effectively on the findings.

Consider relevant accreditations: The Cyber Essentials and Cyber Essentials Plus schemes assess firms against a set of minimum security standards and are designed to be implemented by organisations, big or small. Successful accreditation also comes with free cyber liability insurance for UK-based organisations with turnover under £20m. The NCSC also provides a range of schemes[9] to support firms in demonstrating their cyber resilience. The financial services regulators operate certain testing schemes as part of their supervisory toolkit (CBEST; STAR-FS) but the scale, nature and cost of those schemes mean that they are generally aimed at the largest of financial institutions.

9. National Cyber Security Centre: NCSC assured services (accessed November 2025)

Effective security measures: There are a number of measures advocated by cyber-security professionals. For example, whether you have data sitting in your systems or you're sending it elsewhere, ensuring that it is protected with encryption is widely recommended, so that if it falls into the wrong hands, it is at far lower risk of exposure.

Firms should also limit access where appropriate, and put in place sensible access controls and permissions across the business. Securing systems – both those managed internally and those supplied externally – with multi-factor authentication is now a standard expectation; in fact, the Cyber Essentials scheme now requires firms to have MFA of some sort for any system storing data.

Ensuring that critical data is backed up effectively will also be key, whether that is the organisation's own back-up solutions or those of a third-party provider. Firms may want to consider multiple back-ups of critical data to mitigate many of the cyber-security threats.

Explore external tools and solutions: There are various tools, often available free of charge, to support firms in protecting themselves. The following are examples of some of the free solutions available to firms which may be of use, especially for smaller firms that may not be able to access more expensive solutions:

- **GoPhish**

  A tool for carrying out phishing simulations within the organisation to test staff awareness

- **Haveibeenpwned.com**

  A tool for checking if your credentials have been part of a data breach

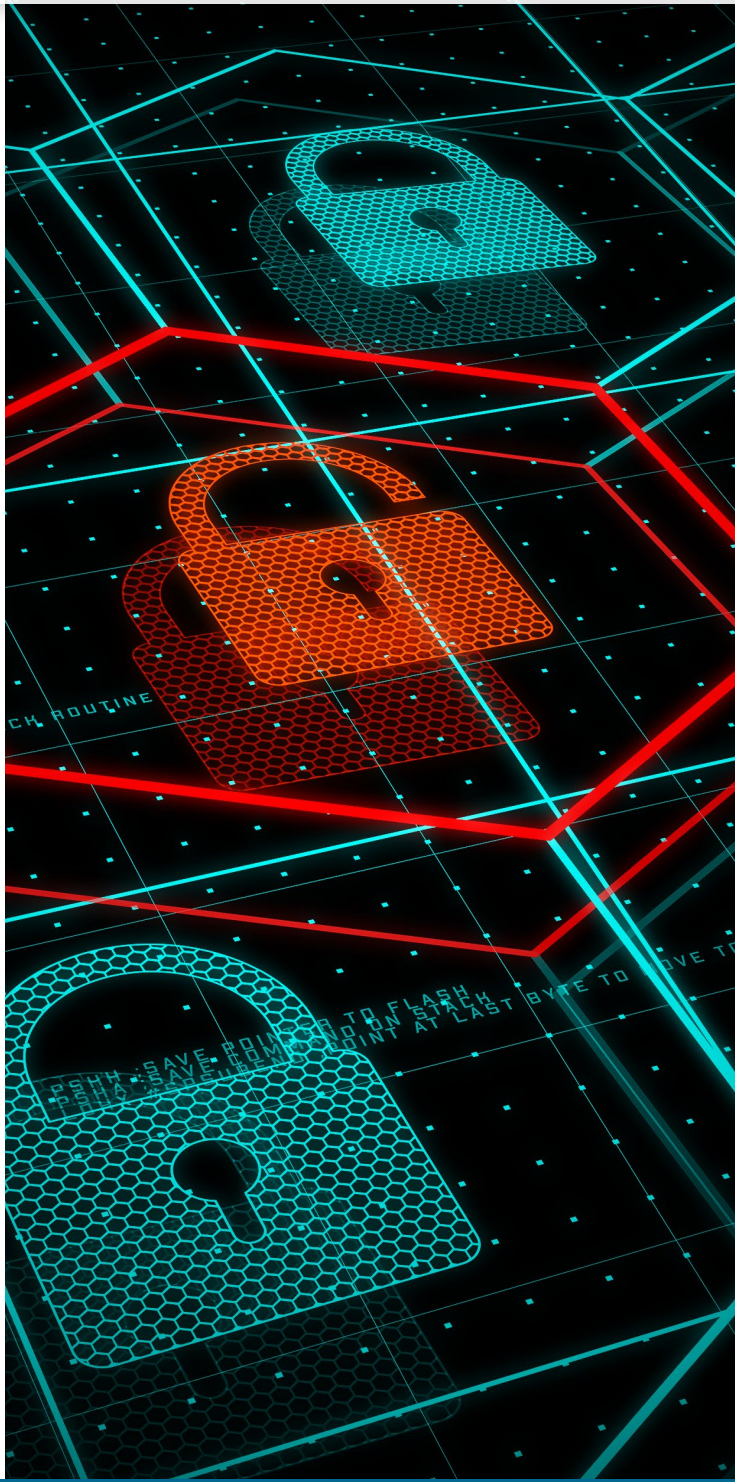
- **VirusTotal.com**

  A tool to scan any downloaded file prior to opening it

- **uBlock Origin**

  An ad-blocker tool that will obscure fake download buttons and malicious advertisements

Review NCSC guidance: While the above is a non-exhaustive list of steps firms should consider taking, we would also advocate reviewing the NCSC's wide range of guidance materials, which set out a host of measures available to firms of all different sizes.



Recommendations

Organisations should consider board-level oversight of cyber-security

All organisations should consider appointing a board director or senior manager with oversight for cyber-security within their organisation.

Stronger regulatory oversight for critical third parties

As critical third parties present a growing risk to all organisations, and even entire sectors, regulators must step up and use the powers afforded to them to ensure that firms and sectors are suitably protected.

Clearer regulatory guidance on data retention and minimisation conflicts

Regulators must work cooperatively and provide clear guidance on conflicts between data storage expectations and data minimisation expectations – recent proposals in the motor finance redress scheme have raised serious questions about the balance that needs to be struck between the two, with firms caught in the middle.

Greater clarity on the use of artificial intelligence in cyber-security

In the absence of specific statutory or regulatory requirements, policymakers and regulators should provide more clarity on expectations around uses of artificial intelligence both in prevention and identification of cyber-security risks.

Government must address the risks of a ransomware payment ban

While we support the underlying goal of prohibiting payment in a ransomware attack, the Government must take steps to address the associated risks of any such prohibition, to ensure the public are protected, essential services remain operational and firms are not pressured to seek workarounds.

2 Esh Plaza
Sir Bobby Robson Way
Great Park
Newcastle upon Tyne
NE13 9BA

T: +44 (0)191 217 0775

E: info@csa-uk.com
W: www.csa-uk.com

voice of the collections industry