LOGISTICS UK

Cyber Security

Insight Report 2024

Executive Membership

LOGISTICS UK

We support, shape and stand up for safe and efficient logistics

Logistics UK is one of the biggest business groups in the UK, supporting, shaping and standing up for efficient logistics. We are the only organisation in the UK that represents all of logistics, with members from the road, rail, water and air industries, as well as the buyers of freight services such as retailers and manufacturers whose businesses depend on the efficient movement of goods.

An effective supply chain is vital to keep Britain trading, directly impacting over seven million people employed in making, selling and moving the goods that affect everyone everywhere.

With EU exit, technology and other disruptive forces driving changes in the way goods move across borders and through the supply chain, logistics has never been more important to UK plc.

As champions and challengers, Logistics UK speaks to government with one voice on behalf of the whole sector, greatly increasing the impact of our messages and achieving amazing results for members.

T: 03717 11 22 22
W: www.logistics.org.uk/executivemembership

Contents

Foreword

Logistics acts as an enabler for trade and commerce, and it would be hard to find a business sector that is more inextricably intertwined with so many other parts of the global economy. This very interconnectedness, and the increasing digitalisation of supply chains, places the logistics sector – and its customers and suppliers – at a far higher risk in the event of a cyber attack.

In this Insight Report, we have blended insights gleaned from in-depth interviews with senior experts from industry, government, law enforcement and academia with the latest research from Logistics UK, to present a comprehensive picture of how the sector can combat the rising tide of cyber attacks, both from criminal and nation-state actors.

Capturing a broad range of comment and insight on a topic that is fast climbing the boardroom's agenda, the report explores many aspects of cyber security, from the types of cyber attacks logistics businesses may encounter to the peculiar risks associated with nation-state cyber attacks. It also touches on the legal implications of cyber security and the perspective of the UK government and police, as well as the importance of engaging your board and maintaining business continuity in the event of an attack.

Finally, the report offers practical guidance on how to protect your business from a cyber attack, including through the use of cyber insurance, as well as insights on which future trends in cyber security you should keep firmly on your risk radar.

I do hope you take the opportunity to read and absorb some of the key findings of this report and consider how your business can benefit from increasing and enhancing its cyber defences.

Phil Roe
President
Logistics UK

Executive summary

This report captures many aspects of cyber security in logistics, through a series of in-depth interviews with experts from across the industry, public sector and academia.

1 Types of cyber attacks that are of concern to the logistics industry.

Interviewees: Nigel Smart, Director of IT & Development, Logistics UK; James Bore, Managing Director, Bores Group Ltd; Professor Ciaran Martin, Professor of Practice, Blavatnik School of Government, University of Oxford

1.1 According to Logistics UK's Logistics Performance Tracker Q1 2024, when respondents were asked about the frequency of cyber security risk assessments, 56.9% reported their organisations run a risk assessment every six months. This highlights a heightened awareness of evolving threats.

1.2 Just under a quarter (24.4%) reported they 'didn't know', which may stem from inadequate processes or communication.

1.3 When considering future investments, approximately half (49.2%) of respondents plan to increase their investment in cyber security measures over the next 12 months, highlighting the growing priority placed on cyber security.

1.4 By contrast 44.3% of respondents were uncertain about their level of future investment, possibly indicative of budget constraints, lack of skilled personnel or lack of strategic direction in some organisations.

1.5 Over the next 12 months, 49.2% of respondents plan to increase their investment in cyber security measures, with 44.3% not planning to increase their investment in cyber security measures, and 6.6% of respondents did not know whether to increase their investment in cyber security measures.

1.6 Keeping up with rapidly evolving threats was the most commonly reported challenges in terms of the organisation maintaining cyber security, followed by ensuring employee compliance with policies and then budget restraints and lack of skilled personnel.

1.7 Despite challenges, most organisations (67.5%) report compliance with cyber security regulations, reflecting robust adherence to standards. Yet there is high uncertainty (30.9%), suggesting insufficient awareness or clarity regarding compliance.

1.8 Confidence in incident response averages at 6.9 out of 10, indicating moderate assurance but room for improvement.

1.9 The main types of cyber attacks that affect the logistics industry are ransomware, supply chain cyber attacks and phishing attempts.

1.10 Supply chain cyber attacks take many forms but the ones that affect the logistics industry the most are third-party software compromise, hardware attacks, vendor credential compromise, dependency chain exploitation, counterfeit and malicious components, man in the middle attacks and physical security breaches.

2 The risks to the logistics industry from nation state cyber attacks.

Interviewees: Ian Thornton-Trump, Chief Information Security Officer, Cyjax Ltd; Professor Ciaran Martin, Professor of Practice, Blavatnik School of Government, University of Oxford

2.1 Nation-state cyber attacks are a significant and growing threat to the logistics industry.

2.2 Some of the most common types of nation-state cyber attacks include advanced persistent threats, zero-day exploits and supply chain infiltration.

2.3 Ian Thornton-Trump stated that adversary nations such as China, Russia, Iran and North Korea have an opportunity to get inside organisations, as a logistics organisation of any size tends to have a wealth of data that bad actors will be interested in getting their hands on.

2.4 Colonial Pipeline and NotPetya are two of the most prolific nation-state cyber attacks seen to date.

2.5 The London NHS cyber attack in 2024 brought parts of the healthcare system to a standstill and processing lab testing results for blood tests was unable to be carried out as a result of a cyber attack.

2.6 Piracy on the high seas is a common problem when it comes to nation-state cyber attacks.

2.7 The potential for a cyber attack from a nation state is huge because of there being so many different points of entry from criminal and advanced persistent threat actors.

2.8 The potential for a cyber attack from a nation state increases if bad actors get hold of some sensitive technology that they can exploit.

2.9 An example of a nation-state cyber attack took place in June 2024, according to Ian Thornton-Trump, when Italian authorities intercepted and seized two Chinese-made military drones that were destined for Libya.

2.10 The Italians acted on intelligence received, provided to them by the USA, to foil the potential nation-state cyber attack, which meant they were able to intercept the drone shipment. This shows how important sharing threat intelligence is globally and how greater collaboration in cyber security needs to be fostered.

3 The legal implications of cyber security.

Interviewees: Sasha Henry, Senior Managing Consultant, CyXel; Edward Lewis, Managing Partner, CyXel

3.1 The intersection of technology and law is increasingly complex, with regulatory frameworks struggling to keep pace with rapid advancements in cyber security capabilities.

3.2 Lewis stated that there are many different frameworks for cyber security and data safety, but from a UK perspective, the General Data Protection Regulation (GDPR) act is one that most organisations are aware of.

3.3 GDPR states that organisations must process data in a manner that ensures appropriate security using appropriate technical and organisational measures.

3.4 Lewis states that when it comes to GDPR there is no hard and fast criteria, and there is no framework against which your appropriateness with security or otherwise can be benchmarked, because it is incredibly subjective.

3.5 Maintaining a secure backup environment is crucial, and there are many different approaches that can be taken when it comes to backing up data.

3.6 Many in the legal field anticipated scenarios in which the Information Commissioner's Office (ICO) would issue fines of up to 10% of an organisation's global turnover for a data breach, but the reality is very few fines have been issued.

3.7 Typically speaking, fines that have been issued range from between £5k ranging up to £10k-£15k.

3.8 The full weight and power of the law is available in terms of monetary award if an organisation suffers a data breach.

3.9 Data breaches tend to fall in terms of responsibility onto the Chief Information Security Officer (CISO) who takes the brunt of what happens.

3.10 As the logistics industry relies heavily on technology, cyber security needs to be a big priority as many organisations won't be able to operate in the event of a cyber attack.

4 The UK government and police perspective on cyber security.

Interviewees: Andrew Elliot, Director of Cyber Security, Department for Science, Innovation and Technology (UK Government); Detective Superintendent Martin Peters, City of London Police; Lisa Ventura MBE, Founder, Cyber Security Unity Limited

4.1 Cyber security has emerged as a cornerstone of national security, economic stability and public safety.

4.2 In December 2022, the UK government published its updated national cyber strategy, which is the government's plan to ensure the UK remains confident, capable and resilient in today's fast-moving digital world.

4.3 The UK's national cyber strategy exists to ensure the UK is a resilient nation against cyber attacks.

4.4 Andrew Elliot from the Department of Science, Innovation and Technology stated that it is important to recognise that the UK is a country that deals with cyber security very seriously.

4.5 The supply chain to the rest of the critical national infrastructure, including the private sector, is critical and must be protected from cyber attacks as such.

4.6 The five pillars of the UK's national cyber strategy are strengthening the UK's cyber ecosystem, building a resilient and prosperous digital UK, taking the lead in the technologies vital to cyber power, advancing UK global leadership and influence for a secure and prosperous international order and detecting, disrupting and deterring our adversaries to enhance UK security in and through cyberspace.

4.7 The UK has the new Cyber Security and Resilience Bill, which was announced during the State Opening of Parliament by King Charles III on 17 July 2024.

4.8 From the police perspective, basic cyber hygiene is critical to maintain a good cyber security posture.

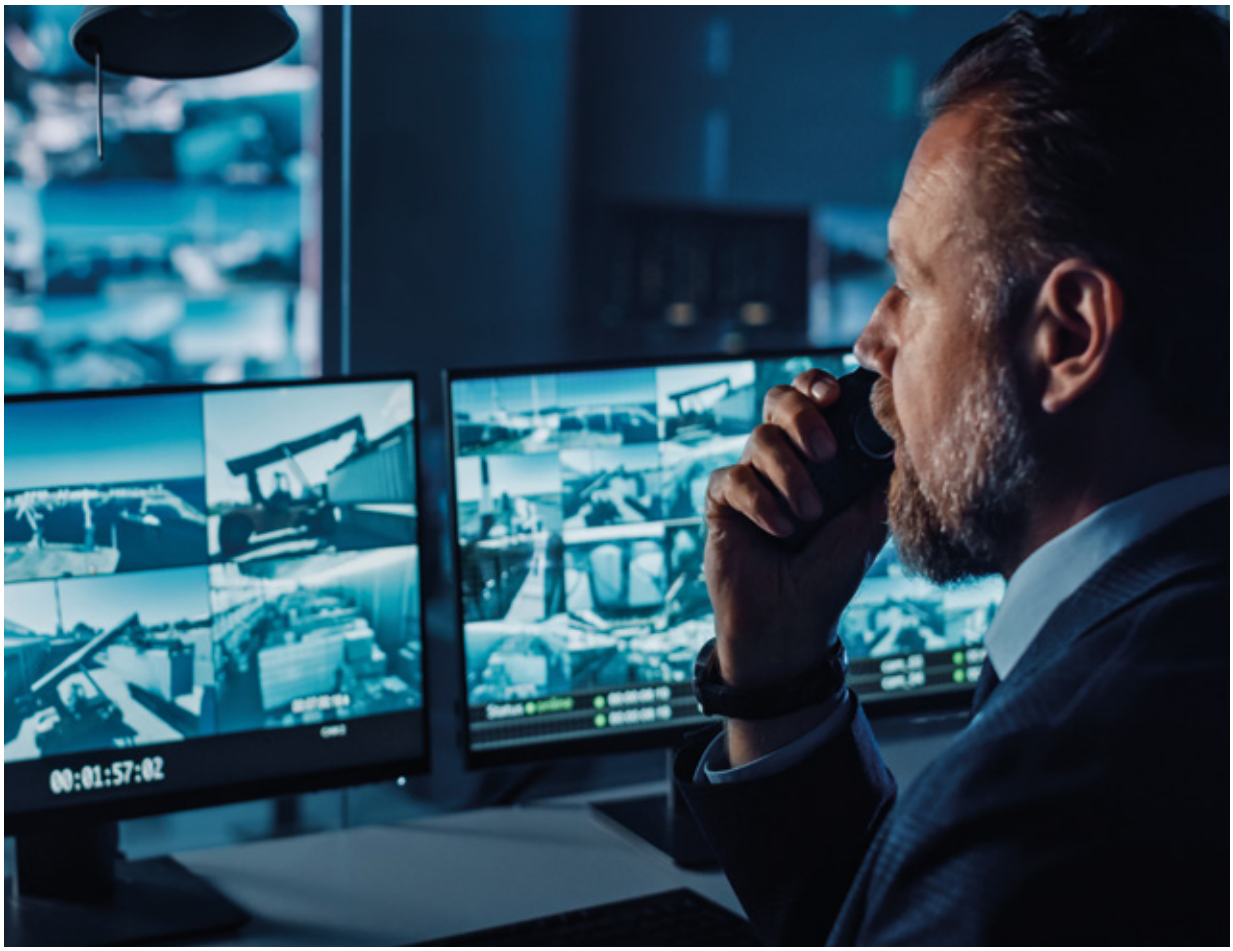
4.9 Lisa Ventura MBE stated that global collaboration when it comes to cyber security is critical. Governments, trade associations and other groups within the cyber security industry must work closely together to share threat intelligence information to help combat the growing cyber threat.

4.10 There are various ways the police will help organisations which are the victim of cyber crime, including working with Action Fraud and the National Crime Agency, according to Detective Superintendent Martin Peters from the City of London Police.

5 The importance of maintaining business continuity.

Interviewees: Simon Newman, Co-Founder, Cyber London; Sarah Armstrong-Smith, Chief Security Advisor, Microsoft; Ian Kirby, CEO, National Cyber Resilience Centre Group

5.1 In July 2024, although not the result of a cyber attack, a huge IT systems failure globally led to significant disruption across the globe, which originated from cyber security organisation CrowdStrike.



5.2 According to Simon Newman from Cyber London, business continuity in the event of a cyber attack needs to be right up there as a number one priority.

5.3 The impact of a cyber attack on the supply chain of things like fresh fruit, vegetables and other produce is huge, as if people can't get hold of food or other basic goods, it won't take long for them to become disruptive.

5.4 Ian Kirby from the National Cyber Security Resilience Centre Group said that before organisations look at their business continuity plans, they need to understand where their assets are and map networks and endpoints.

5.5 If an organisation does suffer a cyber attack, it is crucial not to panic and to deploy your business continuity plan.

5.6 Cyber crime is widely underreported, and incidents should be reported to Action Fraud as well as the Information Commissioner's Office (ICO), especially if it is a data breach.

5.7 Communication is vital to staff in the event of a cyber attack, as is releasing clear and transparent information as to what happened, and what is being done to protect the organisation from further harm.

5.8 Microsoft provides a myriad of different solutions for ensuring business continuity in the event of a cyber attack, and has over 300 data centres globally, with a further 500 in the process of being launched.

5.9 There are multiple layers at Microsoft in terms of how it builds its data centres from power networking to services in the cloud.

5.10 Updating a business continuity plan is crucial and this should be done ideally every six months or annually.

6 Involving the board with cyber security.

Interviewees: Nigel Smart, Director of IT and Development, Logistics UK; Simon Newman, Co-Founder, Cyber London; James Bore, Managing Director, Bores Group Ltd

6.1 Cyber security is no longer just an IT issue, but a critical component of an overall business strategy and risk management.

6.2 When the board is on board with cyber security, it sends a strong message throughout an organisation about the importance of protecting it against cyber attacks.

6.3 It is the responsibility of the board to be aware of and monitor organisational risk, but the risk of a cyber attack has somewhat escaped from the board's agenda today, according to Nigel Smart at Logistics UK.

6.4 Cyber security is a crucial element of overall business strategy and risk management, extending beyond an IT issue to involve the entire organisation.

6.5 Active involvement and support from the board of directors are essential for effective cyber security measures, ensuring adequate resources and a clear organisational message about the importance of protecting against cyber threats.

6.6 Board prioritisation of cyber security helps secure necessary funding, skilled personnel, and ongoing training to counter emerging threats effectively.

6.7 Establishing governance sub-boards focused on cyber risk and regulatory requirements helps in detailed risk assessments and contingency planning.

6.8 Organisations should continually monitor cyber threats, leveraging intelligence from suppliers and national security centres, and keep the board informed of evolving risks.

6.9 Boards play a key role in aligning cyber security strategies with business objectives, protecting critical assets, maintaining customer trust, and ensuring regulatory compliance.

7 How can logistics organisations protect themselves from cyber attacks?

Interviewees: Ian Kirby, Chief Executive, National Cyber Resilience Centre Group; Simon Newman, Co-Founder, Cyber London; Dr Emma Philpott, CEO, The IASME Consortium

7.1 Preventing cyber attacks in the logistics industry is essential for maintaining supply chain functionality, protecting sensitive information, and preserving company reputation and customer satisfaction.

7.2 The exponential growth in cyber threats poses significant financial risks, with potential losses in the millions, underscoring the urgent need for robust cyber defence mechanisms.

7.3 The National Cyber Security Centre's (NCSC) *Ten Steps to Cyber Security* provides a comprehensive framework for building cyber resilience, focusing on risk management, secure configuration, incident management, and user education among other critical areas.

7.4 Cyber Essentials and Cyber Essentials Plus are government-backed certifications that are designed to ensure organisations implement basic technical controls to defend against cyber attacks. Cyber Essentials is a self assessment, while Cyber Essentials Plus involves a more rigorous external assessment.

7.5 The wealth management firm saw an 80% reduction in cyber incidents after requiring its network to achieve Cyber Essentials Plus certification, illustrating the efficacy of these controls.

7.6 Support from the National Cyber Resilience Centre network is available UK wide and offers free cyber security advice and support to organisations, particularly small and medium enterprises, helping them improve their cyber resilience through training and expert guidance.

7.7 The EU's NIS2 Directive broadens the scope of covered sectors and strengthens security requirements, ensuring better risk management, incident response, and supply chain security across the EU.

7.8 The Digital Operational Resilience Act (DORA) enhances digital resilience through stringent ICT risk management, incident reporting, and regular resilience testing, ensuring financial entities can withstand and recover from digital disruptions.

7.9 Both NIS2 and DORA emphasise the need for clear governance structures and accountability in cyber security practices, ensuring senior management is directly involved in overseeing and managing cyber risks.

7.10 Continuous investment in cyber security awareness and training is vital. Programmes like those from the National Cyber Resilience Centre Network and the guidelines from Cyber Essentials ensure that organisations are equipped to handle evolving cyber threats.

8 Can cyber insurance help protect against cyber attacks?

Interviewees: Professor Ciaran Martin, Professor of Practice, Blavatnik School of Government, University of Oxford; Ian Kirby, Chief Executive, National Cyber Resilience Centre Group

8.1 Cyber security insurance, also known as cyber liability insurance, is designed to protect businesses from financial losses resulting from cyber attacks, including data breaches, ransomware attacks, cyber extortion, business interruption, and cyber crime.

8.2 Cyber security insurance covers costs associated with incident response, legal fees, potential damages, and business interruption, minimising financial losses and helping restore operations post attack.

8.3 Cyber security insurance encourages proactive measures to protect against cyber threats, thereby reducing the likelihood and impact of cyber incidents.

8.4 Support is provided for crisis communication and public relations, helping to manage and mitigate damage to the company's reputation following a cyber incident.

8.5 Cyber insurance assists organisations in meeting regulatory requirements for data protection, ensuring they adhere to legal standards and avoid penalties.

8.6 Cyber security insurance is not a substitute for robust cyber security measures. Strong security practices are essential to prevent attacks and mitigate potential losses. Insurers may also set specific security requirements for policyholders.

8.7 Ian Kirby emphasises the importance of combining insurance with cyber resilience education. Professor Ciaran Martin highlights the need for organisations to understand their risk profiles and work with knowledgeable advisors when purchasing insurance.

8.8 Before purchasing a policy, organisations should conduct a comprehensive risk assessment to understand the most critical assets and potential losses. This ensures that the selected insurance policy addresses the specific risks faced by the business.

8.9 When selecting a cyber security insurance policy, key considerations include assessing the business's risk profile, understanding coverage needs (eg, data breach response, cyber extortion, business interruption), comparing policy features and costs, considering the insurer's reputation, and potentially working with a broker.

8.10 When purchasing cyber security insurance, provide details about the organisation's security measures, potentially leverage cyber security certifications for discounts, and continuously update coverage to align with the evolving security landscape. The National Cyber Security Centre (NCSC) offers resources and guidance for this process.

9 The future of cyber security/future trends to be aware of.

Interviewees: James Bore, Managing Director, Bores Group Ltd; Ian Kirby, Chief Executive, National Cyber Resilience Centre Group; Ian Thornton-Trump, Chief Information Security Officer, Cyjax Ltd; Lisa Ventura MBE, Founder, Cyber Security Unity Limited; Sarah Armstrong-Smith, Chief Security Advisor, Microsoft

9.1 Artificial intelligence and machine learning are revolutionising cyber security by enhancing real-time threat detection, response, and automation of routine security tasks.

9.2 As reliance on cloud-based services grows, securing sensitive data, ensuring data privacy, and protecting against cloud-based threats are critical.

9.3 The proliferation of IoT devices introduces new vulnerabilities. Securing these interconnected devices to prevent them from becoming entry points for cyber attacks is a significant challenge for future cyber security efforts.

9.4 The advent of quantum computing poses a threat to current encryption standards, necessitating the development of quantum-resistant cryptographic algorithms.

9.5 Deep fake technology, which creates realistic but fake audio, video, or images, poses cyber security threats. It can be used for misinformation, identity fraud, and social manipulation.

9.6 Cryptocurrencies present unique cyber security challenges, including theft of digital assets and compliance with regulatory measures.

9.7 AI is increasingly used to develop and deploy ransomware attacks, making them more sophisticated and widespread. Organisations must enhance their defences against AI-driven ransomware to protect their operations and data.

9.8 With advancements in AI, traditional cues for detecting phishing emails (eg, poor spelling and grammar) are becoming less reliable. Continuous and updated cyber security awareness training is vital to equip individuals with the skills to recognise and respond to modern cyber threats.

9.9 Maintaining legacy infrastructure poses security risks due to outdated technologies. Organisations should invest in modernising their infrastructure to meet current security standards and reduce vulnerabilities.

9.10 The rapidly evolving cyber threat landscape requires continuous innovation, collaboration, and vigilance. Organisations must adapt their cyber security strategies to leverage new tools and methodologies while addressing emerging threats.

LOGISTICS UK

Executive
Membership

T: 01892 526171*
F: 01892 534989
www.logistics.org.uk

Logistics UK is a trading name of Freight Transport Association Limited
Registered office: Hermes House, St John's Road, Tunbridge Wells, Kent TN4 9UZ
Registered in England Number 391957

*Calls may be recorded for training purposes. Correct at time of publishing but subject to change.
 13.09.24/SW 001115