eye.

Cyber in Logistics 2024


C2

Introduction

Hello, new growth! Hello, new risks...

Cyber in Logistics 2024

Sustainability. Growth. Digitalisation. These are the words everyone's using about the logistics landscape of 2024. But what do they mean for individual businesses – and for security?

First, the good news. Post-pandemic, the logistics industry has recovered well, achieving a market size of 10.41 trillion USD in 2020. Statista projects that by 2028, the market size will grow to 14.08 trillion.[1] Thanks to what Kearney calls the 'twin transition' – the alignment of digital and sustainability goals – the sustainable transformation is picking up speed.[2] A wave of initiatives, from automation, predictive maintenance, IoT applications, to intelligent transport systems and demand-based supply, are helping businesses across the sector improve efficiency and reduce waste.

The downside? The same factors improving operations and acceleration towards sustainability are opening the door to increased security risks. In 2020, alarmingly, cyber attacks soared by as much as 700%. The logistics sector was especially impacted, with attacks on operational technology in the maritime industry rising by as much as 900% in 2020[3].

Hot on the heels of increased cyber crime are new regulations designed for resilience. Under NIS2 – the Network & Information Security Directive coming into place next year – company directors can be held personally liable for failing to implement sufficient security.

With the uptick in cyber threats, NIS2, and the high cost of attacks themselves, every business in the logistics sector should be fortifying their defences right now.

1 Size of the logistics industry worldwide 2018-2028 (Statista Research Department, 2023)

2 State of Logistics 2023: The great reset (Kearney, 2023)

3 'Maritime Cyber Attacks Increase 900%' (Maritime Professional, 2020)

Eye Security offers non-enterprise businesses the essential tools of high-grade security, ensuring their data stays safe and their infrastructure compliant. In this e-book, we'll explore the risks and challenges particular to the logistics sector. We'll break down the upcoming NIS2 and help you think about your own state of resilience. Cyber risk may be on the rise, but we're rising to meet it – and together, we can safeguard your business.

From e-commerce, to cyber crime

How industry changes are opening the door

COVID may no longer be closing borders, but long-term effects are still impacting the logistics industry. The meteoric rise of e-commerce, with easy return and refund policies, has driven corresponding demand for flexible delivery services. Fast growth is turning up the pressure for more sustainable transport solutions.

The result? Rapid innovation and digitisation across the industry, driven by new technologies. An explosion of new players and challengers, with flexible and data-led offers. Increasing digital footprints, even as carbon aims are centred. And soaring cyber crime.

Digitalisation, the double-edged sword

Machine-driven process changes have transformed today's supply chain. Transportation and logistics companies now use Edge and IoT to track the location of goods, monitor temperature, and check stock levels. With so much real-time data to hand, companies can make informed decisions that reduce spoilage, minimise waste and optimise supply and demand.

These improvements dovetail happily with sustainability goals – a seeming win-win situation.

By 2025, the World Economic Forum forecasts that digitalisation in logistics may unlock as much as $1.5 trillion in value for the industry.[4]

But there's a downside.

These advances require companies to store large amounts of data in the cloud. Automation across the supply chain means operations are connected in invisible, complex ways. The huge data sets generated by these processes can only be analysed by AI.

In the resulting tangle of vendors and opaque operations, maintaining a holistic view is more difficult – and necessary – than ever.

4 Digital Transformation of Industries (World Economic Forum, 2016)

Cyber risk is real – and rising

As one of the most profitable industries, logistics has long been a target for organised cyber crime. And the more it relies on digital infrastructure, the more susceptible it is to attacks.

With the advancement of vast data sets from IoT, attackers have a ready supply of data to sell or exploit. And just as AI and automation are helping logistics companies be more efficient, cyber criminals are using these tools in attacks which are increasingly hard to detect and manage.

A high proportion of phishing attacks are made on logistics companies. The highly-connected nature of the sector makes it especially vulnerable to criminals who pose as legitimate professionals, gaining access to passwords and data.

When a less-protected third-party down the supply chain is breached, even companies with a high level of cyber defence can find themselves at risk. In 2021, a logistics company involved in the COVID vaccine chain was compromised in just this way.[5]

Ransomware – when hackers infiltrate a company's IT infrastructure and encrypt files or whole systems, making them inaccessible unless the business pays a ransom – is one of the fastest-growing threats. In 2020, reported ransomware incidents grew by 700%, with transport and logistics firms a key target.[6] According to figures from the UK's Information Commissioner's Office (ICO), 1 in 3 cyber breaches are now ransomware attacks.[7] Given that not all such attacks are reported, the number could be even higher.

Such attacks are devastating for any business, but in logistics, where continuity is all-important, some businesses never recover. Earlier this month, major UK company KNP Logistics declared insolvency, citing its inability to recover from a ransomware attack as the cause.[8]

1 in 5 businesses in logistics and transport are likely to experience a cyber incident

4.45 million dollars is the global average cost of a data breach in 2023

~ 5% of new customers at Eye Security had already been breached before onboarding

Source: 'Cost of a Data Breach Report' (IBM, 2023)

5 'How one email took down a logistic company' (Darktrace, 2021)

6 Mid-Year Threat Landscape Report (Bitdefender, 2020)

7 Data Security Incident Trends (Information Commissioner's Office, 2022)

8 'UK logistics firm blames ransomware for insolvency, 730 redundancies' (The Record, 2023)

The likelihood of the threat, the potential of losses running into millions, and the impact on reputation, customer satisfaction, and competitive edge, all make it more urgent than ever for logistics and transport businesses to defend their IT and OT systems.

While logistic companies see...		Cyber criminals see...
Rapid industry growth and profitability	>	More to gain from potential attacks
More data on goods and services	>	More data to harvest and sell for profit
Greater sharing of data across partnerships	>	Greater chance of finding weak links
More remote working, driving e-commerce	>	More unsecured devices to hack
Greater headcount to service a growing business	>	More untrained targets for phishing
More opportunities for end to end automation	>	A larger surface to attack

Exploring your security landscape

While the impact of an attack is almost always greater than expected, a security upgrade reaps rewards. By preventing attacks in the first place, organisations can save up to $1.4m.[9]

- Are your employees trained in identifying phishing emails?
- Are your HR onboarding and leaving processes secure?
- Are your IoT endpoints and networks segmented?
- Are your encryption and authentication methods robust?
- How safe are your third-party connections?
- Are you staying up-to-date against new forms of attack?

9 'Study: Preventing Cyberattack Penetration Can Save Enterprises Up To $1.4 Million Per Incident' (Businesswire, 2020)

A case of ransomware, resolved

How Eye Security and Van Mieghem handled a cyber attack

Van Mieghem Logistics has over 350 vehicles and more than 700 employees. The family-run transport company has been in operation for 65 years, with seven Belgian branches and another four across Europe.

Like many businesses, Van Mieghem Logistics depends on its IT infrastructure, built almost entirely in-house. One Saturday morning, strange things began happening to the company's servers. They had fallen victim to a cyber attack in the form of ransomware – by far the biggest cyber threat to logistics companies worldwide.

Van Mieghem turned to Eye Security for help. Within hours, two Incident Responders were on site, rebuilding systems and rolling out security software before bringing the business back online.

Eye Security's cyber experts determined that the business' former external IT partner had made a wrong configuration in its firewalls, enabling the attack.

The first systems were back online in days, but 'the 150-plus links to customers, suppliers, and partners were still closed to the internal systems, as was the internet,' recalls van Mieghem. The company reconnected all external sites one by one, while vetting and taking security measures.

Eye Security was able to reassure Van Mieghem that the attackers had not captured any data to resell. The attack still cost the company a staggering 1.3 million Euros (much of which was fortunately covered by its cyber insurance).

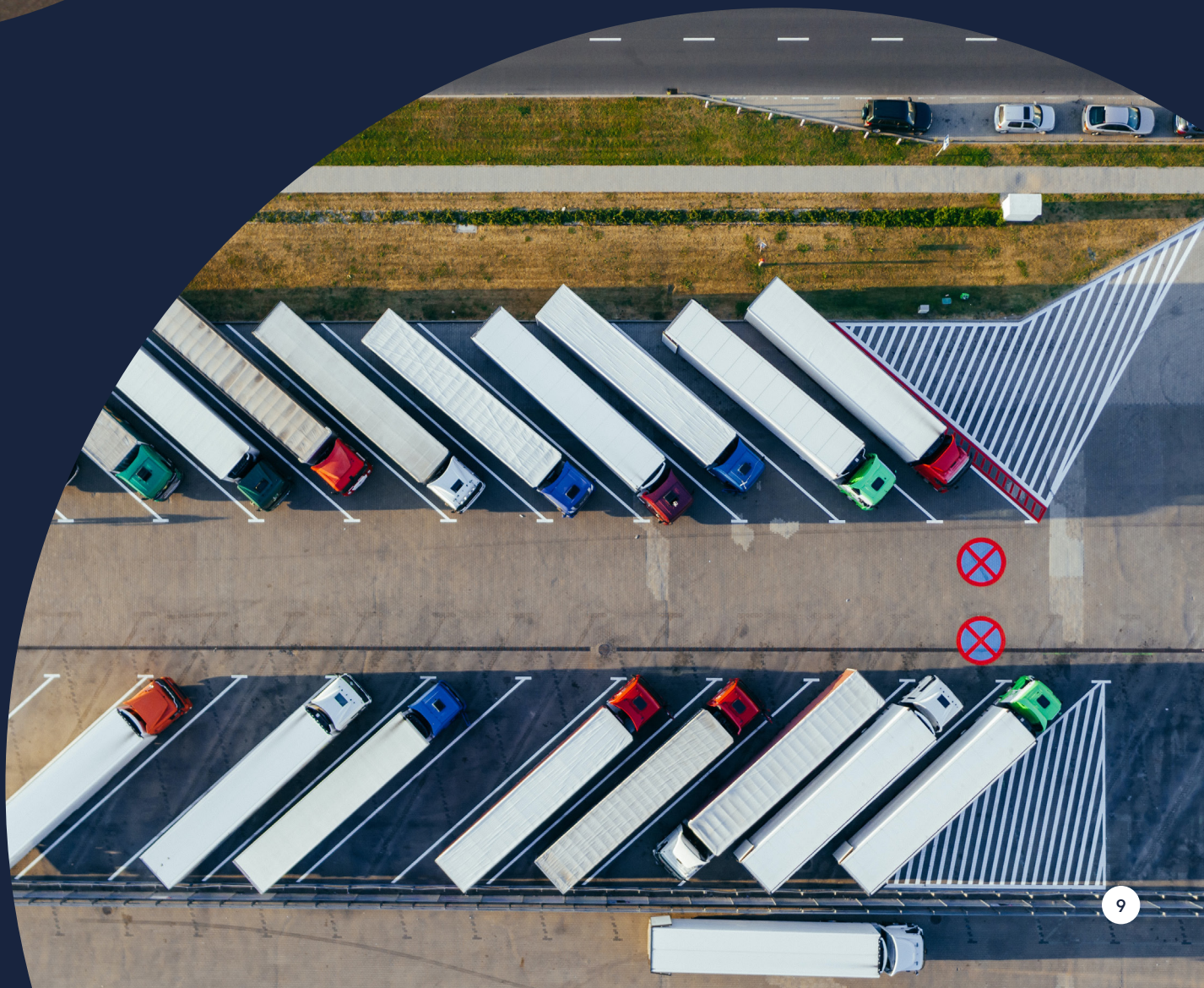
It was almost a year before the business was fully operational again – now with fortified IT infrastructure.

'Today, we remain constantly alert. Is the entire infrastructure secure? Are employees trained on how to recognise phishing? Have we missed any critical patches? It's a process.'

Van Mieghem received additional advice from Eye Security, benefiting from their local knowledge. As Anne Masson, CEO of Eye Security Belgium, says: 'We are able to solve large-scale challenges with personal attention and to the full satisfaction of our customers [...] We know the Belgian market inside out. We advise Belgian companies on process improvements to make their infrastructure more secure, and what solutions they can deploy to be sufficiently secure in the future.'

Meanwhile, Eye Security has rolled out its Cyber Guard solution across Van Mieghem's systems, using Managed Extended Detection & Response technology (mXDR) combined with cloud detection.

'We always thought we had our security in place,' says Van Mieghem. The ransomware attack cost the company €1.3m.



Building cyber resilience with NIS2

Why compliance is more urgent than ever

NIS2, the new version of Network & Information Security Directive, aims to strengthen the overall level of cyber security across the EU. The guideline is a milestone in cyber defence – and a challenge for most non-enterprise businesses.

Critical infrastructure – our electricity, water, healthcare system, the way we move from place to place – is the number one target for malicious attacks. It's not hard to understand why: a large-scale attack on transport systems can bring a city to a halt.

NIS2 – a little like GDPR, but for cyber security – is necessary for the protection of critical infrastructure. The guidelines, which must be adopted by all EU member states by October 2024, require businesses to adopt more stringent cyber defence and reporting than the previous NIS1.

Like its predecessor, NIS2 should be considered a guide, with compliance being the minimum. Businesses should be proactive in protecting their sensitive data and critical systems, because the impact of a cyberattack extends far beyond the financial.

In logistics, prolonged downtime erodes customer satisfaction and trust, disrupts business continuity, reduces competitive advantage, and hinders growth. In today's growing marketplace – with new challengers around every corner – few businesses can afford to lose their edge.

●●●

'By acting on NIS2 now, companies can take the opportunity to assess their operations, get a better understanding of their systems and integrations, and fortify any weaknesses.'

What's new in NIS2

Broader and more stringent

NIS2 broadens the scope of NIS1 from 7 to 18 industries (including transport, postal and courier services, food production, and manufacturing), while introducing stronger cyber security standards and precise incident reporting requirements.

More impact on logistics

In logistics, IT and OT have become more entwined. To meet the new standards, businesses in this sector need a holistic overview of interdependencies and weaknesses. They will have to monitor areas of risk, with measures in place to act on any incidents.

Increased personal liability

Not complying with NIS2 carries heavy penalties. From 2024, company directors can be held personally liable for failing to implement sufficient security, with fines of up to €10 million.

How Eye Security can help

Most non-enterprise businesses won't have resources to dedicate to understanding NIS2 requirements, and implementing them holistically across operations.

We can put our expertise to work for you, from initial cyber risk assessment, to rolling out a robust cyber resilience framework.

We see NIS2 as an opportunity, rather than a hindrance. By putting measures in place for cyber attack monitoring, such as Managed XDR, we can help you avoid such attacks in the first place.

Instead of dealing with the consequences of an attack, you can focus on opportunities for growth.

Interview

Q&A with Danny Zegger of QFirst

What's your role in cybersecurity?

I'm a Cybersecurity Officer at QFirst, which helps companies prepare for certification – particularly around the new European NIS2 legislation. Specifically, I bridge the gap between the theoretical and the practical, helping people translate regulations into their actual operations.

How has cybersecurity changed in recent years – and where's it headed?

Every IT company thinks they're doing a good job – they've strengthened their firewalls, their procedures and processes. Most already have set up ISO27k (international guidelines for managing risks around data), or are in the process of setting it up.

The main thing businesses are facing in the next 3-5 years is levelling up to a Zero Trust approach (in which everyone is verified every time they request access, even if they were authenticated earlier). National law will require this to be absolutely waterproof. And if not, it will require constant monitoring by a company like Eye Security.

How do you get companies certification-ready?

We have a 5-stage process. The first step is to screen them, and see what they do already in terms of cybersecurity. Then we test it – a Black Hat Penetration Test on all the levels. Then we make an advisory report, which is used to develop a solutions roadmap. Finally, we look at ongoing monitoring and reporting. With NIS2, the moment there is an incident, the company has only 72 hours to report and register the incident. They have to report it, so that other companies can know there is an exploit and take action.

What's the biggest cybersecurity challenge for logistics?

Logistic companies have many divisions and moving parts – they're like a Rubik's cube. And every division is focused on what needs to be done right then. Continuously monitoring endpoints isn't their priority. So monitoring and getting an overview is a big challenge.

Also, from 2024, logistics companies will have to ensure that all their supply chain are also NIS2 certified. This includes anyone providing them with APIs – drivers, everyone who connects to the applications and services the ICT infrastructure. It's a huge challenge. But a framework can be developed to help them do this more easily.

Any advice for companies exploring cybersecurity upgrades?

Don't let yourself (or your budget) be swamped by solutions. Focus on getting the right solutions in place from the start. Don't just know the regulations -- know how to implement them in practice for your business. And provide yourself with a centralised ISMS NIS2 framework, where you have a link between incident management, risk analysis, digital assets and divisions.

Where we started, where we're going... ...and where your business fits in

Eye Security was founded in 2020 to make national intelligence-grade cyber security available to organisations large and small. Just three years later, we're proud to have a board with five former national security experts, a team of 80 skilled employees (and growing), and offices in the Netherlands, Belgium, and Germany.

At Eye Security, we understand people who build business. We know the years of work that go into turning an idea into a successful company. We know that when an organisation falls victim to an attack, there's more than financial and reputational damage – livelihoods are at stake.

Our clients trust us as their security partner. We earned that trust by making the knowledge of our experts available to organisations of all sizes and at all times. Our work won't be finished until every business in Europe has the protection they need.

'We're not selling technology or software. We're selling the security of expertise.'

Our products

Enterprise-level security, for the non-enterprise business

Hundreds of businesses rely on Eye Security – from one of the largest carriers in the Netherlands, to a producer for some of the most well-known Dutch food brands.

Developed by security experts, our subscription-based service provides comprehensive protection and support, without the unnecessary products so often bundled with cyber protection.

Our all-in-1 package offers cyber monitoring and detection, 24/7 cyber response in the case of an incident, and most recently, cyber insurance. A streamlined package of the most impactful security measures, it's simple, compliant, robust – and the first of its kind to be made accessible.

●●●

'Eye Security has the specialist knowledge we need to protect our systems, because they are constantly working on cyber crime and security. This allows us to focus on what we are good at: deep-sea container transport through Western Europe.'

Gertjan van der Most, founder of Van der Most Transport

What's included – *and why it matters*

1

Managed XDR

Our Managed Extended Detection and Response (XDR) service offers 24/7 monitoring and detection of abnormal behaviour by a team of human cyber experts to swiftly identify and mitigate potential threats.

Cyber criminals operate 24 hours a day, 7 days a week and only 20% of threats can be dealt with by technology alone – 80% need human judgement and intervention.

2

Cyber Awareness Training

We offer interactive training programs to educate your staff on best practices, empowering them to recognise and respond effectively to cyber risks, such as phishing emails.

Phishing attacks are increasing in volume and sophistication – it only takes one negligent or unaware employee to release an attack chain that could cost your business millions.

3

Incident Response

Our Incident Response team is here for you, in person, 24/7 in case of a cyber incident to limit damage and get you back to business as soon as possible.

Even one day of downtime can cost hundreds of thousands of euros. In that event, you need to deal with real people, not a ticketing system, an email instruction or a global call centre.

4

Intelligence

Through our customer portal, we provide you with clear and specific recommendations for how you can strengthen your cyber security measures.

This value-added intelligence takes the guesswork out of what needs to be done to improve your cyber resilience – and potentially reduce your insurance premiums – without the burden of consultancy hours and extra charges.

5

Threat hunting

Our intelligence team is constantly hunting for new threats. When we identify them, we work with our customers to make sure they are secure.

We are proactively looking for every opportunity to keep your systems resilient and stay one step ahead of cyber criminals.

6

Cyber Insurance

We offer a quick and painless process to buy or renew cyber insurance, so you can mitigate the financial impact of a cyber incident.

1 in 5 non-enterprise businesses are hacked, costing on average €400,000. Cyber insurance is crucial in helping protect your business from the potentially high cost of attacks.

‘Every company, of every size, deserves access to high-quality cyber security.’

– Job Kuijpers,
CEO and Founder
of Eye Security

Get ready for tomorrow’s demands, today.

We know our transport and logistics customers face a wide range of risks. For these customers, we offer a tailor-made quote for each risk category. And – even as major insurers wind down their transport and logistics insurance policies – we’re able to offer a fully-fledged solution through Eye Underwriting that takes into account the complexity of third-party relationships in this sector.

Visit our website to schedule a consultation with one of our experts. We’ll help you understand your threat landscape, fortify your infrastructure, and get to grips with NIS2.

Eye Security makes cyber security simple.

www.eye.security


CẢNG CÔNG-TEN-NƠ QUỐC TẾ HẢI PHÒNG
MAERSK SARAT

Do you want more information?

Please contact us for a no-obligation conversation with an Eye Security cyber specialist. After all, it is now more important that ever to ensure your business' security.

Visit www.eye.security or contact us on
+31 88 644 4888