Hawsons Chartered Accountants
Latest News

May| 2024

Transport & Logistics Insight

In this issue:

Hawsons

Big firm expertise,
small firm personal attention

Hawsons Chartered Accountants
Latest News

Paul Wormald
Partner

Introduction

Welcome to our latest Transport and Logistics newsletter. Since our last edition of the newsletter the government delivered their 'budget for long-term growth'. The current HGV driver shortage is estimated to be around 35,000 - 40,000 which is significantly lower than 100,000 estimated just after the pandemic ended.

In this edition of the newsletter we discuss the following:

- Digital skills gap found in the logistics sector
- Truck stops to be upgraded
- Network Rail Spending Plans 2024 – 2029
- UK company size thresholds to increase
- 2024 Ransomware Trends
- Small business enrgy standing charge sharply increases

As always we hope you enjoy the contents of this newsletter and as ever please do not hesitate to contact one of our experts if you have any questions about these articles.

Paul Wormald
Partner

Digital skills gap found in logistics sector

Introduction

As the world becomes increasingly digitised, industries are facing a pressing need to adapt to technological advancements. The logistics sector, a cornerstone of the UK economy, is no exception. Recent findings from a report by Neos Networks have unveiled a significant digital skills gap within the logistics industry. This revelation comes hot on the heels of previous challenges faced by the sector, including shortages in drivers and HGV technicians.

The report highlights how this digital skills deficit is impeding companies' efforts towards digital transformation and the adoption of technology-driven initiatives. Through surveying industry leaders nationwide, Neos Networks delves into the crucial role of connectivity in the UK logistics landscape, while also gauging the industry's readiness for broader digital transformations.

In this article, we explore some of research findings and address some of barriers facing investment in digital skills in the logistics industry.

Research findings

The research conducted by Neos Networks highlights a concerning shortage of digital talent within the UK logistics sector, with 63% of companies facing this challenge. Only a minority of logistics companies feel adequately equipped for digital growth, with less than 40% possessing the necessary skill set for tech initiatives. Outdated systems plague a significant portion of the industry, hindering the adoption of digital processes, as reported by 37% of surveyed companies. Additionally, insufficient digital infrastructure poses a substantial barrier, according to 35% of respondents.

Barriers to investment in Digital skills

Experts caution that without sufficient investment, the sector risks stagnating in its digital transformation efforts. We explore some of common barriers preventing logistics companies from investing in digital skills.

Unwillingness to invest

One of the primary obstacles encountered by any organisation seeking to embark on digital transformation is the reluctance to embrace change. Furthermore, the importance of crafting a digital transformation plan may encounter hindrances due to the reluctance to allocate adequate human and financial resources for such projects. This is especially the case in sectors that typically have low profit margins such as logistics.

Continued overleaf

Digital skills gap found in logistics sector (Continued)

Not an attractive career path compared to other sectors

The logistics sector has a need for well-qualified experienced staff with in-depth technical skills. However, this may be difficult to achieve as a career in logistics may not be as appealing to these experts as other sectors.

Outdated technology and systems can be expensive to replace

Many logistics companies have invested a huge amount of money into technology and systems that are now outdated which could be difficult and expensive to replace.

Why is it important for the logistics sector to invest in technology?

Investing in digital education and infrastructure is very important to create a culture of innovation which will ensure that the UK will be at the forefront of the logistics sector. To achieve this their will need to be collaboration between industry leaders, digital experts and the government to overcome the digital skills gap barrier in the logistics sector.

Truck stops to be upgraded

Introduction

Truck stops across England are set to undergo a significant upgrade, thanks to a collaborative effort between industry players and the government. With a combined investment of £16.5 million, 38 HGV rest areas will see substantial improvements aimed at enhancing the facilities available to lorry drivers.

How will truck stops be upgraded?

The Department for Transport (DfT) is allocating £6 million towards this initiative, with an additional £10.5 million contributed by industry partners. The focus of these upgrades is to provide lorry drivers with more parking spaces, improved welfare facilities, and safer rest areas, ensuring their comfort and well-being during breaks. Among the planned enhancements are the installation of new showers, restaurants, better lighting, and secure fencing. Moreover, around 430 new parking spaces will be created for heavy goods vehicles (HGVs), alleviating congestion on local roads.
Notably, the upgrades will also incorporate provisions for sustainable energy solutions, including charge points for electric HGVs and the integration of solar panels on driver facilities.

This investment builds upon previous efforts, with £15 million in funding allocated last year for similar improvements. With a total joint investment of up to £31 million, the government and industry stakeholders are committed to enhancing lorry roadside facilities, ensuring a safer and more comfortable experience for lorry drivers across the country.

Truck stops to be upgraded

Introduction

Truck stops across England are set to undergo a significant upgrade, thanks to a collaborative effort between industry players and the government. With a combined investment of £16.5 million, 38 HGV rest areas will see substantial improvements aimed at enhancing the facilities available to lorry drivers.

How will truck stops be upgraded?

The Department for Transport (DfT) is allocating £6 million towards this initiative, with an additional £10.5 million contributed by industry partners. The focus of these upgrades is to provide lorry drivers with more parking spaces, improved welfare facilities, and safer rest areas, ensuring their comfort and well-being during breaks. Among the planned enhancements are the installation of new showers, restaurants, better lighting, and secure fencing. Moreover, around 430 new parking spaces will be created for heavy goods vehicles (HGVs), alleviating congestion on local roads.
Notably, the upgrades will also incorporate provisions for sustainable energy solutions, including charge points for electric HGVs and the integration of solar panels on driver facilities.

This investment builds upon previous efforts, with £15 million in funding allocated last year for similar improvements. With a total joint investment of up to £31 million, the government and industry stakeholders are committed to enhancing lorry roadside facilities, ensuring a safer and more comfortable experience for lorry drivers across the country.

Network Rail Spending Plans 2024 – 2029

Introduction

As the impacts of climate change continue to pose significant challenges for infrastructure maintenance, Network Rail unveils its comprehensive spending plans for Control Period 7. Spanning from April 2024 to March 2029, this ambitious five-year strategy places a strong emphasis on addressing climate-related issues affecting vital components such as drains, cuttings, and embankments. With an allocated budget of £45.4 billion, Network Rail aims to sustainably operate, maintain, and renew its extensive network, encompassing 20,000 miles of track, 30,000 bridges, tunnels, and viaducts, as well as a multitude of signals, level crossings, and stations.

In this article, we delve into Network Rail's strategic approach to combatting climate change while ensuring the resilience and reliability of the UK's rail infrastructure for years to come.

Where is the funding coming from?

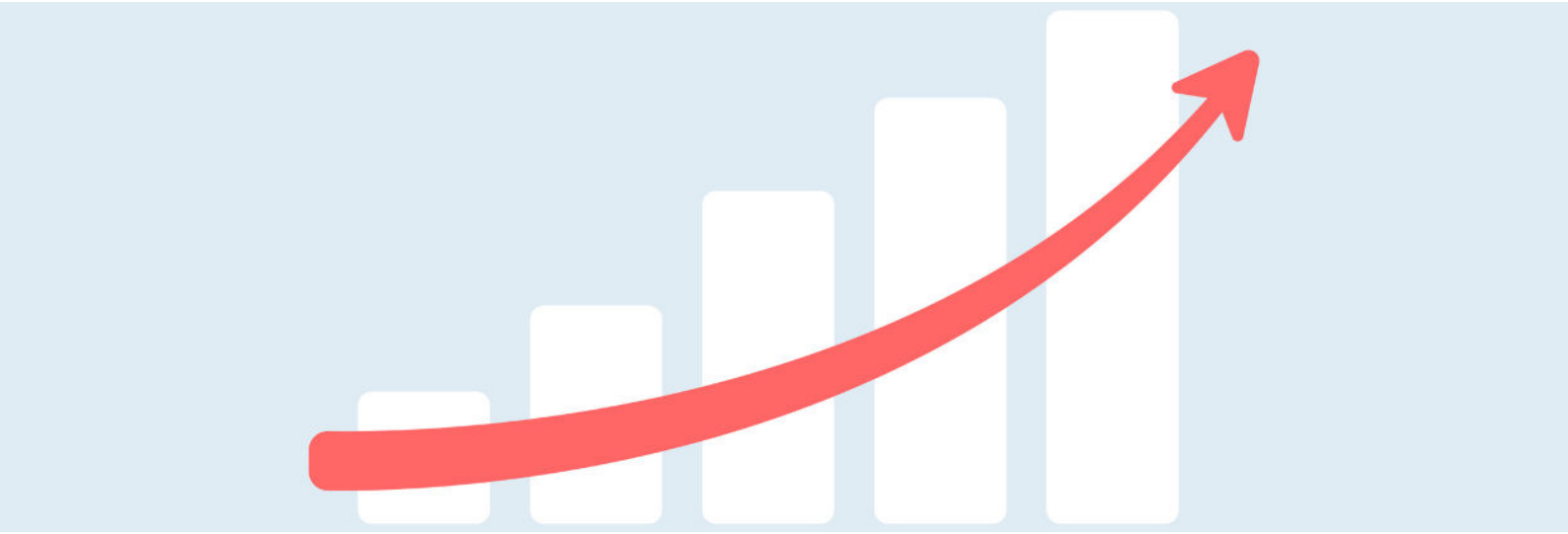
The funding for Network Rail's ambitious spending plans primarily stems from multiple sources, reflecting a diverse financial landscape. The Department for Transport (DfT) shoulders a substantial portion of the financial burden, contributing £27.5 billion towards the allocated budget. Transport Scotland (TS) is committing £2.3 billion to support Network Rail's initiatives within their jurisdiction. In addition to governmental contributions, access charges levied on train and freight operators contribute significantly, amounting to £13.8 billion. Network Rail further supplements its funding through commercial income streams, generating £1.7 billion.

What will the funding be spend on?

The funding has been divided into categories which are as follows:

- Operations (£4.4bn)
- Support (£5.3bn)
- Maintenance (£12.6bn)
- Renewals (£19.3bn)
- Industry costs (£2.0bn)
- Risk Funding (£1.8bn)

When the Statement of Funds was first announced the figures demonstrated that CP7 (2024-2029) had a small real terms increase in funding than CP6 (2019-2024). However, recent inflation means that Network Rail now has slightly less funding in real terms than it did in CP6.



UK company size thresholds to increase

To cut complexity and burdens from legislative reporting requirements, the thresholds for company sizes in the UK are being increased by 50%.

Following the Spring Budget, it has been announced by the Prime Minister Rishi Sunak that the company size thresholds will be changing in order to relieve the UK's regulatory burden.

The Government intends for companies with financial years starting on or after 1 October 2024 to benefit from the changes being made to the thresholds. The ICAEW provided their own input into the consultation process with the clear message to ministers that the thresholds should become more simplified.

Company size thresholds UK

The new measures will mean micro entity thresholds will increase to turnover of not more than £1m, as compared to not more than £632,000 previously. Small company thresholds will now become £15m of turnover as opposed to £10.2m and the upper medium threshold will now be no more than £54m of turnover. Anything above this level will now be classed as a large company. The balance sheet total assets threshold will rise to £500,000 (micro), £7.5m (small), £27m (medium) and anything exceeding £27m (large).

The company size thresholds increasing is a step closer towards modernising the model for UK corporate reporting. The Government intends for 132,000 businesses to be taken out of non-financial reporting requirements. The measures also plan to simplify the process for filing reports digitally and to remove certain requirements relating to what companies are required to disclose in their annual reports.

Medium sized companies

The Government intends to look at the definition for medium sized companies and how this impacts on the required reporting.

There is a proposal to increase the medium sized companies average number of employees limit to 500 from 250. Medium companies may also become exempt from the requirement to prepare a strategic report. Furthermore, smaller public interest entities may be removed from their audit tender and rotation requirements.

Fully funded apprenticeships

The Prime minister also announced in his speech that the government intends to fully fund apprenticeships for small businesses from 1 April for trainees under the age of 21. The government will also increase the amount of funding that can be passed on to other businesses from employers that are paying the apprenticeship levy. Apprenticeships can currently be funded by a levy-paying employer transferring up to 25% of their unused levy to a different employer.

2024 Ransomware Trends

The cyber security criminals aren't giving up, and they're not just doubling down either. They are now tripling down. They even have virtual "ransomware supermarkets" for criminals to pop in and buy ransomware in a box with a set of instructions so even more criminals can lurk inside your network for weeks on end, planning their attack to maximise the havoc to your business. In this article, we look at some of the ransomware attack trends of 2024.

Current ransomware attack trends that will continue into 2024

In this section, we identify current ransomware attack trends that are expected to continue into 2024.

Supply chain attacks

Supply chain attacks do not just attack a single victim, they usually infiltrate an entire organisation compromising its suppliers or service providers. These attacks exploit the interconnected nature of modern supply chains, leveraging trusted relationships to gain unauthorised access to valuable data and systems. Once inside, attackers deploy ransomware, a type of malicious software that encrypts files or systems, rendering them inaccessible until a ransom is paid. Whilst this is not a new trend these types of ransomware attacks will likely continue. This is because the attackers will usually demand a large ransom because of the types of organisations they target, making it a very lucrative type of ransomware attack.

Triple extortion ransomware attacks

Triple extortion ransomware attacks operate on a three-pronged strategy, combining traditional encryption-based ransomware tactics with additional methods of extortion. The three elements typically include:

- Data encryption
- Data theft
- Reputational damage

In this type of attack, the attackers will seek to infiltrate the victim's network to disrupt operations before stealing sensitive information and demanding huge ransoms knowing that the threat of public exposure could tarnish the reputation of the organisation.

Continued overleaf

2024 Ransomware Trends (continued overleaf)

Ransomware as a service (RaaS)

These days, ransomware attackers don't even need to code their ransomware. RaaS is a pay-for-use malware that provides attackers the correct coding to launch and maintain a ransomware attack which now gives more individuals the opportunity to launch a ransomware attack.

Attacking unpatched systems

Ransomware attacks exploit vulnerabilities in computer systems to infiltrate networks and encrypt critical data, rendering it inaccessible until a ransom is paid. Software companies announce the vulnerabilities they have fixed including the background to what the problem is, and the criminals use that information to set up automated scans across the internet for vulnerabilities.

Phishing attacks continue and are even more sophisticated

Phishing ransomware attacks typically begin with a deceptive email or message designed to lure unsuspecting users into clicking on a malicious link or downloading an infected attachment. Once the victim interacts with the phishing content, an innocent-looking payload is deployed onto their system which can then download the ransomware and set it up without the user knowing anything about it.

After a period of planning, the criminals set the ransomware off encrypting critical files and locking users out of their data. In some cases, ransomware variants may also exfiltrate sensitive information before encryption, providing the criminals with additional leverage to coerce victims into paying a ransom. Whilst this is now a very well-known method of ransomware attack it is still one that is used regularly by attackers and there are no signs of phishing attacks ending.

Ransomware trends for 2024 and beyond

We are now going to explore some new ransomware trends that are expected to evolve into 2024 and beyond.

Attack methods that will evolve to exploit cloud and VPN infrastructure

It is to be expected that ransomware attacks on VPN infrastructure exploitation will become more sophisticated. This will present significant challenges for organisations that use VPNs for remote working and secure communications. The likely attack methods will be on outdated software with security vulnerabilities, weak passwords and multi-factor authentication.

2024 Ransomware Trends (continued overleaf)

Generative AI could become a huge issue

It is predicted that 2024 will be a huge year for the implementation of AI to help organisations operate more efficiently. However, the rise of generative AI could make it easier for attackers to create more advanced phishing campaigns more efficiently, which means they will be able to target more individuals and organisations with their attacks.

How to mitigate against ransomware attacks?

1.Employee education and awareness

One of the most critical components of ransomware mitigation is educating employees about the risks of cyber threats, including phishing scams and social engineering tactics commonly used by ransomware operators. Regular training sessions and awareness programs can help employees recognise suspicious emails, links, and attachments, empowering them to take proactive measures to prevent ransomware infections.

2.Implement robust email security measures

Since many ransomware attacks originate from phishing emails, organisations should deploy robust email security solutions to detect and block malicious messages before they reach end-users inboxes. Advanced threat detection mechanisms, such as machine learning algorithms and sender authentication protocols, can help identify and neutralise phishing attempts in real time, reducing the likelihood of successful ransomware infections.

3.Regular Software Patching and Updates

Keeping software and operating systems up to date with the latest security patches and updates is essential for mitigating the risk of ransomware attacks. Vulnerabilities in software applications are often exploited by threat actors to gain unauthorised access to systems, making timely patching updates a critical defense mechanism against ransomware exploits. Organisations should establish robust patch management processes to identify, prioritise, and apply security updates promptly.

4.Implement Access Controls and Privilege Principles

Limiting access to sensitive data and systems through access controls and privilege principles can help prevent unauthorised users from modifying or encrypting critical files in the event of a ransomware attack. By restricting access to only those individuals who require it to perform their job functions, organisations can reduce the attack surface and mitigate the potential impact of ransomware infections.

2024 Ransomware Trends (continued overleaf)

5. Backup and Disaster Recovery Planning

Implementing robust data backup and disaster recovery mechanisms is essential for mitigating the impact of ransomware attacks. Organisations should regularly back up critical data to offline or cloud-based storage repositories and test their backup restoration procedures to ensure data integrity and availability in the event of an attack. A comprehensive disaster recovery plan should outline the steps to be taken to restore operations and minimise downtime following a ransomware incident.

6. Network Segmentation and Intrusion Detection

Segmenting networks and implementing intrusion detection systems can help contain the spread of ransomware within an organisation's infrastructure and detect anomalous behaviour indicative of a ransomware attack. By isolating critical systems and monitoring network traffic for signs of malicious activity, organisations can identify and respond to ransomware threats more effectively, minimising the impact on their operations.

Cyber insurance

Even if you've protected your business to the highest level your budget will allow, that protection can still be breached. The mindset has to be one of planning both to prevent the criminals from accessing your network and planning for what happens if they do. Cyber insurance coverage needs to be checked annually to make sure you have the right type and level of coverage so that if your data is exposed your business is protected. As an example, if customer records are exposed, buying identity theft insurance can be very expensive.

Conclusion

To conclude, the ransomware criminals aren't giving up and A.I will only help criminals to work smarter and faster and make phishing attacks more plausible. It doesn't take much imagination to see how criminals could use A.I to take the voice from a YouTube video of your CEO and use that in a social engineering phone call to one of your employees so, if you haven't done it recently, now is the time to review your protection and recovery against ransomware.

Small business energy standing charge sharply increases

Small businesses across the UK have seen energy standing charges increase very sharply over the past few months with some reporting increasing of over 1000%. Furthermore, 62% of small businesses have said that the ever increasing cost of utilities continues to one of the main drivers for increased business costs.

Ofgem (energy regulator) are yet to take any serious action against energy companies hiking up standing charge prices. The Federation of Small Business has called for Ofgem to take some action and address this issue more transparently.

What is an energy standing charge?

The energy standing charge is a fixed daily fee imposed by energy suppliers to cover the cost of supplying energy to a property, regardless of the amount of energy consumed.

How are the high energy standing charges affecting small businesses?

This is having a huge impact on small businesses energy bills because there is nothing they can do to reduce energy suppliers standing charge. SME's can choose to limit their energy consumption to reduce their bills, however, forcing small businesses to reduce their energy consumption can lead to reduced growth, confidence and the ability to invest.

What about the energy price cap?

Unfortunately, business energy customers are not covered by the energy price cap as this only applies to domestic use. Therefore, business energy tariffs can increase standing charges and consumption rates at any time if the business is not on a fixed tariff. Some businesses believe that this is the reason they have seen their standing charge increase because energy suppliers are unable to increase standing charges for domestic customers.

Continued overleaf

Small business energy standing charge sharply increases (Continued)

What are standing charges used to fund?

Energy firms use standing charges to fund the maintenance and upkeep of the energy infrastructure, including the distribution network, and meters, and ensuring reliable supply to customers. Additionally, standing charges contribute to covering administrative costs associated with billing and customer service.

How can small businesses reduce their energy costs?

Small businesses can reduce gas and electricity bills by implementing various strategies such as conducting energy audits to identify areas of inefficiency, investing in energy-efficient appliances and equipment, utilising programmable thermostats and smart lighting systems to control usage, implementing insulation measures to minimise heat loss, encouraging employee awareness and participation in energy-saving practices, negotiating competitive energy tariffs with suppliers, and considering renewable energy sources like solar panels where feasible. A number of local authorities also offer grants to help subsidise capital investment aimed at reducing energy consumption.

Additionally, regular maintenance of equipment and facilities can help optimise energy performance and reduce overall consumption, ultimately leading to cost savings for the business.

Get in touch

Our experts

We act for a large number of clients in this sector across our three offices, ranging from hauliers to international couriers, and understand the challenges this dynamic sector faces.

Nearly every other commercial sector is reliant on the services transport and logistic businesses provide and, in many ways, this specialist sector is the linchpin for our country's economy.

With our experience in the transport and logistics sector we are able to develop a close understanding of your business and, through active year round involvement, we can help you anticipate and deal with challenges quickly and effectively.

Scott Sanderson
Partner
0114 266 7141
ss@hawsons.co.uk

Sheffield Office
Pegasus House
463A Glossop Road
Sheffield, S10 2QD

David Owens
Partner
01604 645600
davidowens@hawsons.co.uk

Northampton Office
Jubilee House
32 Duncan Close, Moulton Park
Northampton, NN3 6WL

Paul Wormald
Partner
01302 367 262
pw@hawsons.co.uk

Doncaster Office
5 Sidings Court
White Rose Way
Doncaster, DN4 5NU

Hawsons