# How a single security lapse brought down KNP Logistics in a devastating ransomware attack



It began with an inconspicuous glitch. An employee at KNP Logistics reported a frozen screen, a minor inconvenience that caused little concern at first. However, within hours, this seemingly trivial issue spiralled into a full-blown crisis, leaving all 800 employees unable to access vital systems, including the Transport Management System, essential for coordinating the company’s fleet of 350 trucks.

Paul Abbott, then Group Director and shareholder at KNP Logistics, recounted the harrowing day in June 2023 when the company was struck by a ransomware attack attributed to the infamous Akira gang. This group, based primarily in Russia, has gained notoriety for its ruthless methods and financial success, claiming over $42 million from around 250 attacks in the preceding year. The sense of urgency escalated as operations transitioned to old-fashioned methods of communication and logistics management, with employees resorting to using pens and paper to keep the wheels of business turning.

Abbott's attempts to maintain morale amid mounting stress and confusion were commendable but ultimately overshadowed by the looming threat posed by the hackers. The arrival of an ominous ransom note, with its chilling greeting of “Hi friends,” was a stark wake-up call. Featuring poor grammar and spelling, the message outlined the hackers' demands and hinted at dire consequences should the company refuse to engage.

The ramifications of the attack were catastrophic. Although KNP Logistics had invested significantly in cybersecurity measures—spending £40,000 on insurance and employing up-to-date firewalls—these precautions proved inadequate against the specialised tactics of Akira. According to a report by Kaspersky ICS CERT, many organisations are currently ill-equipped to combat advanced ransomware threats, particularly in sectors critical to infrastructure like logistics.

While KNP Logistics struggled to recover, the attack highlighted the vulnerabilities within the logistics sector. The Federal Bureau of Investigation (FBI) notes an alarming upwards trend in such incidents, impacting hundreds of organizations worldwide. Abbott expressed particular concern over the recent attacks on well-established retailers like Marks & Spencer and Harrods, whose operational disruptions echo the devastating effects his own company endured.

Three months post-attack, KNP Logistics succumbed to insolvency, leading to the agonizing loss of around 730 jobs. This not only marked the end of a company with a history dating back to 1865 but also the tangible impact of cyber crime on individuals' livelihoods. The situation was dire enough that some portions of the business were sold off to save around 170 jobs, showcasing the cascade of devastation that cyber incidents can trigger.

One of the most troubling aspects was the revelation that the breach stemmed from a simple lapse in security practices: a trusted employee had failed to use two-factor authentication. It raised unsettling questions about internal security and trust, elements essential for the operation of any successful company. Abbott’s introspection on these themes resonates strongly in an age where cyber threats are becoming increasingly sophisticated and hard-hitting.

Despite the overwhelming challenges, Abbott resolved not to succumb to despair. After a period of reflection, he founded a new venture, Yarrow Group Ltd, alongside his wife. Furthermore, he has embarked on a mission to consult with other logistics and transport businesses about the critical need for robust cybersecurity measures. It is a lesson in resilience, as he advocates for both awareness and preparedness in the face of an ever-evolving cyber threat landscape.

The tragedy of KNP Logistics serves as a cautionary tale, one that highlights the increasing prevalence of ransomware attacks threatening businesses of all sizes. As the nature of work continues to change, organisations must remain vigilant, proactive, and educated about the pivotal role cybersecurity plays in their operational health. With incidents like those affecting major retailers and KNP Logistics, the reality is stark: no company is immune from the insidious reach of cyber criminals.

As Abbott aptly summarised, the chilling prospect still haunts many businesses: they can now operate from anywhere in the world with little more than a laptop and an internet connection, making proactive measures not just advisable but essential for survival.

### Reference Map

1. Lead article
2. Summary (2)
3. Summary (3)
4. Summary (4)
5. Summary (5)
6. Summary (6)
7. Summary (7)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

* <https://www.dailymail.co.uk/news/article-14712981/It-began-single-screen-freezing-ended-100m-year-firm-going-bust-really-feels-like-targeted-Russian-hackers.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - Please view link - unable to able to access data
* <https://ics-cert.kaspersky.com/publications/reports/2024/04/11/h2-2023-a-brief-overview-of-main-incidents-in-industrial-cybersecurity/> - This report by Kaspersky ICS CERT provides an overview of significant industrial cybersecurity incidents in the second half of 2023. It highlights the impact of ransomware attacks on various sectors, including logistics and transportation. Notably, it discusses the case of KNP Logistics, a UK-based company that declared insolvency after a major ransomware attack in June 2023. The attack, attributed to the Akira ransomware gang, affected key systems and financial information, leading to the loss of 730 jobs and the sale of a subsidiary to save 170 jobs. The report emphasizes the growing threat of ransomware to critical infrastructure and the need for enhanced cybersecurity measures.
* <https://therecord.media/knp-logistics-ransomware-insolvency-uk> - This article from The Record discusses the insolvency of KNP Logistics, one of the UK's largest privately owned logistics groups, following a ransomware attack in June 2023. The attack, attributed to the Akira ransomware gang, led to the encryption of critical systems and financial data, adversely affecting the company's financial position and its ability to secure additional investment. Approximately 730 employees were made redundant as a result of the administration process, although one of the group's key entities was sold, saving about 170 jobs. The article highlights the severe impact of ransomware attacks on businesses and the broader economy.
* <https://www.livemint.com/companies/news/ransomware-gangs-merciless-attacks-bleed-small-companies-dry-11733463633513.html> - This article from LiveMint examines the increasing threat of ransomware attacks on small and medium-sized businesses, focusing on the Akira ransomware gang. It details the case of KNP Logistics, a UK-based company that suffered a significant attack in June 2023, leading to the encryption of critical systems and financial data. The attack resulted in the loss of 730 jobs and the eventual insolvency of the company. The article underscores the financial and operational challenges posed by ransomware attacks and the need for businesses to implement robust cybersecurity measures.
* <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a> - This advisory from the Cybersecurity and Infrastructure Security Agency (CISA) provides detailed information on the Akira ransomware, including its tactics, techniques, and procedures (TTPs). It reports that since March 2023, Akira has impacted over 250 organizations, claiming approximately $42 million in ransom proceeds. The advisory describes how Akira threat actors use a double-extortion model, encrypting systems after exfiltrating data, and provides recommendations for organizations to mitigate the risk of such attacks. It also details the encryption methods used by Akira and the characteristics of their ransom notes.
* [https://en.wikipedia.org/wiki/Akira\_(ransomware)](https://en.wikipedia.org/wiki/Akira_%28ransomware%29) - This Wikipedia page provides an overview of Akira ransomware, a malware that emerged in March 2023. It details the group's activities, including targeting over 250 entities such as BHI Energy, Nissan Australia, Tietoevry, and Stanford University. The page notes that Akira is offered as ransomware-as-a-service and has been estimated to have earned up to $42 million from its inception until April 2024. It also lists notable incidents attributed to Akira, including attacks on Nissan Australia and Tietoevry, and mentions the group's claim of responsibility for a ransomware attack on the Toronto Zoo.
* <https://www.bnnbloomberg.ca/business/company-news/2024/12/06/ransomware-gangs-merciless-attacks-bleed-small-companies-dry/> - This article from BNN Bloomberg discusses the impact of ransomware attacks on small and medium-sized businesses, focusing on the Akira ransomware gang. It details the case of KNP Logistics, a UK-based company that suffered a significant attack in June 2023, leading to the encryption of critical systems and financial data. The attack resulted in the loss of 730 jobs and the eventual insolvency of the company. The article highlights the financial and operational challenges posed by ransomware attacks and the need for businesses to implement robust cybersecurity measures.