# KNP Logistics collapse reveals harsh realities of ransomware threats in UK supply chains



It began as a minor inconvenience: a computer screen freezing. An employee at KNP Logistics shrugged it off; such glitches are commonplace in the world of technology. However, within hours, this seemingly trivial event escalated into a catastrophic failure as the firm’s entire IT system crashed. With 800 employees unable to access critical software, including the Transport Management System essential for managing 350 operational trucks, the implications were dire, not just for the company but for public safety as well.

At the helm was Paul Abbott, then Group Director and shareholder of KNP Logistics. What he faced was every business leader’s nightmare. As emergency measures kicked in, the company reverted to antiquated communication methods—mobile phones, pens, and paper. The chaos intensified when IT experts discovered a chilling ransom note hidden within the system: “Hi friends, if you’re reading this, it means the internal infrastructure of your company is fully or partially dead.” This message was not merely a threat; it was the handiwork of the Akira ransomware gang, a notorious group reportedly responsible for over $42 million in profits from such attacks within just a single year.

Recent news of similar breaches affecting major retailers like Marks & Spencer and the Co-op resonated painfully with Abbott. Only days prior, M&S had confirmed a breach involving the theft of personal customer data. The gravity of such incidents lies in their potential to undermine consumer trust. Abbott recalled his own experience: "Customers can forgive operational issues, but the loss of personal data is different and far more troubling.” M&S attempted to reassure customers that sensitive payment details were likely safe, echoing sentiments Abbott had once expressed to KNP’s own client base.

KNP Logistics, a prestigious company with roots dating back to 1865, had thrived on a turnover exceeding £100 million annually. Abbott had believed they were well-prepared against cyber threats, investing heavily in advanced technology and cybersecurity training. However, amidst the hustle of adapting to a new warehouse and the complexities of logistics, the firm found itself ill-equipped for the sophisticated nature of the attack.

The reality hit home when, after hours of attempted recovery, the IT team discovered the ransom note—a crude, threatening proposal that revealed a shocking vulnerability. It detailed a process for negotiation, while also warning that failure to comply would result in data being sold on the dark web. This violation of trust left an indelible mark not only on KNP Logistics but also highlighted the growing threat of cybercrime. According to Kaspersky’s cybersecurity report, such incidents are on the rise, particularly within the logistics sector, where vulnerabilities can disrupt entire supply chains.

Abbott’s personal reflections during the ordeal reveal the emotional and psychological toll of a cyber attack. He felt a heavy burden of responsibility for his staff and the company’s legacy. In the aftermath, an investigation revealed that the breach stemmed from a trusted employee who had not employed two-factor authentication. Despite the breach not being their fault, the loss was devastating—the firm collapsed within three months, resulting in over 700 jobs lost.

As Abbott surveyed the wreckage, he made the difficult decision to abandon the ransom request. The amount demanded was exorbitant, and even should they regain access, the risk of further corruption loomed large. Instead, they opted to rebuild from scratch, a choice fraught with its own challenges. “Sadly, however, losing all our data was something we never recovered from,” Abbott recounted, underscoring the fact that even the most proactive measures could not ensure complete safety in a world rife with cyber threats.

Reflecting on his journey post-KNP, Abbott now runs a new logistics firm and dedicates significant time to consultancy, aiming to fortify other businesses against cyber attacks. “So many still don’t fully grasp the risks involved with cyber crime,” he laments. As evidenced by the recent breaches at retail giants, the threat remains pervasive, existing at the intersection of modern technology and sophisticated criminal activity. The stark lesson remains: in today’s digital landscape, no one is truly safe.

### Reference Map

1. Content adapted from the initial article detailing KNP Logistics' cyber attack experiences.
2. Insights into the broader implications of cybersecurity incidents identified in Kaspersky’s report.
3. Context on Akira ransomware and its impact drawn from Wikipedia. 4-7. Supplementary details about Marks & Spencer's cyberattack, highlighting recent trends in cyber threats.

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 details attacks on various sectors, including logistics, where UK-based KNP Logistics Group suffered a major ransomware attack attributed to the Akira ransomware gang. The attack led to the company's insolvency, resulting in the loss of 730 jobs and the sale of a subsidiary to save 170 jobs. The report highlights the severe impact of cyberattacks on industrial operations and the importance of robust cybersecurity measures.
* [https://en.wikipedia.org/wiki/Akira\_(ransomware)](https://en.wikipedia.org/wiki/Akira_%28ransomware%29) - The Wikipedia page on Akira ransomware provides comprehensive information about this malware, which emerged in March 2023. It targeted over 250 entities, including BHI Energy, Nissan Australia, Tietoevry, and Stanford University. The page details Akira's methods, such as exploiting Cisco VPN products and using double-extortion techniques. It also discusses the development of Akira v2, written in Rust, and the release of decryptors by Avast and other researchers. The page offers insights into the evolution and impact of Akira ransomware.
* <https://www.nationalworld.com/business/consumer/marks-spencer-cyberattack-update-5114900> - This article discusses the cyberattack on Marks & Spencer (M&S) that began over the Easter weekend, leading to issues with contactless payments and click-and-collect orders. M&S confirmed the incident on April 22, 2025, and temporarily suspended online orders on April 25. The attack is believed to be a ransomware attack orchestrated by the hacking group Scattered Spider, a splinter group of Lapsus$. The article highlights the operational challenges M&S faced and the broader implications of such cyber incidents on retail operations.
* <https://cybernews.com/news/marks-spencer-cyberattack-online-sales-down-phishing-customers/> - This article reports on the cyberattack that disrupted Marks & Spencer's online sales, leading to the suspension of all online and app sales. The attack, believed to be orchestrated by the hacking group Scattered Spider, resulted in significant operational challenges for M&S, including the inability to accept gift cards and process returns. The article also discusses the potential financial impact of the attack, estimating that M&S could be losing £15 million in profits each week due to the disruption.
* <https://www.northumberlandgazette.co.uk/business/ms-marks-and-spencer-scattered-spider-online-cyber-attack-uk-shopping-5110689> - This article provides an overview of the cyberattack on Marks & Spencer (M&S) attributed to the hacking group Scattered Spider. It details the operational disruptions caused by the attack, including issues with click-and-collect orders and contactless payments. The article also discusses the broader implications of such cyber incidents on retail operations and the challenges businesses face in securing their systems against sophisticated cyber threats.
* <https://www.cybersecurityintelligence.com/blog/scattered-spider-hacking-group-is-behind-the-attack-on-mands-8392.html> - This article discusses the cyberattack on Marks & Spencer (M&S) attributed to the hacking group Scattered Spider. It details the operational disruptions caused by the attack, including issues with online sales and in-store operations. The article also highlights the financial impact of the attack, noting that M&S's stock market valuation has been significantly affected. It provides insights into the methods used by Scattered Spider and the broader implications of such cyber incidents on large organizations.