Grow trust. Secure the supply chain.

Logistics is under attack. Secure data now or risk serious reputational damage, and losing customer and staff confidence.

Logistics businesses need more than the consistent robust connectivity a powerful, reliable network brings to deploy the latest IoT and AI technology, capture key data and turn it into actionable insight. The network must also be as secure as possible to safeguard the growing amounts of business-critical data and avoid what happened recently at Hellman Worldwide Logistics.

On 9 December 2021, the Germany-based business disabled servers at its central data centre after a security breach was detected. Hellmann, which provides air and sea freight, and rail and road transportation across 173 countries, was targeted by RansomEXX ransomware, putting its business and customer data at serious risk, according to Security Week.

Such attacks are increasingly common. In addition to data compromise and ransom demands, they can also severely disrupt operations if systems are disabled and data is lost. Arguably more damaging is the reputational impact and loss of customer trust, especially important in logistics. Hellmann reported that its customers were experiencing an increasing number of fraudulent calls and emails following the incident, as the hackers quickly began monetising stolen information.

Cyberattacks remain a continual threat in the transport and logistics industry. In addition to knocking customer confidence, they can seriously

UK cybercrime incidents increase

The National Cyber Security Centre said it had helped deal with a 7.5% increase in cases in the year to August 2021, fuelled by a surge in ransomware attacks with criminal hackers seizing control of corporate data and demanding payment in cryptocurrency for its return.

National Cyber Security Centre

Ransomware attacks on the rise

The Supply Chain Disruptions and Cybersecurity in Logistics report, published in April 2021 in the US, reveals a sector at risk:

3x

From 2019 to 2020, **ransomware attacks on shipping and logistics firms tripled**.

#1

Ransomware is the #1 cyber threat to logistics companies today, suggesting a situation of imminent and extreme risk.

100%

of the companies surveyed showed some evidence of threat targeting against their network.

damage workforce morale. Two notable recent incidents include the forced IT systems shut down at Japan Post-owned freight forwarder Toll Group in February 2020, and the NotPetya malware cyberattack on Damco, the freight forwarding and logistics arm of Danish container shipping giant Maersk. The latter resulted in a US$8m loss in turnover in the first half of 2017.

Cybercrime experts Intel 471 recommend that logistics companies constantly monitor their systems to identify malicious behaviour, and scale up tools to prevent attacks. Despite warnings, a report in April 2021, assessing 20 of the top global shipping companies, found that 90% of the organisations studied had insufficient cybersecurity.

As well as providing a secure network with maximum resilience to deter cyberattacks, a technology partner should be able to offer expert advice and guidance on securing the tools and applications necessary to capture and analyse the data logistics teams need. Ideally, they should also be able to provide access to an expert cybersecurity team. During selection, it's important to ask any potential partners about the availability of 5G-powered mobile private networks, upcoming technology that will not only deliver the fastest and most reliable connectivity to optimise IoT, AI and automation, but also provide a secure environment.

We hope you enjoyed this excerpt from our report on how hybrid working strategies that harmonise humans and digital innovation optimise the performance and value of your data and technology.

BT: the power to protect

At BT, we're trusted to protect nation-states and royalty. We have 3,000 personnel dedicated to cybersecurity, including ethical hackers, a specialist innovation consultancy practice, and we invest £40m a year in cybersecurity.