Securing logistics operations in a data-first world

By Chris de Bruyn

25 Jun 2020

Have you noticed any changes in how courier packages are delivered? Electronic signature pads accompany more and more of the deliveries. Delivery employees tap away on apps on their phones, telling them where to go next. Even the simple act of finding your location is now a very digital experience thanks to GPS and electronic maps.

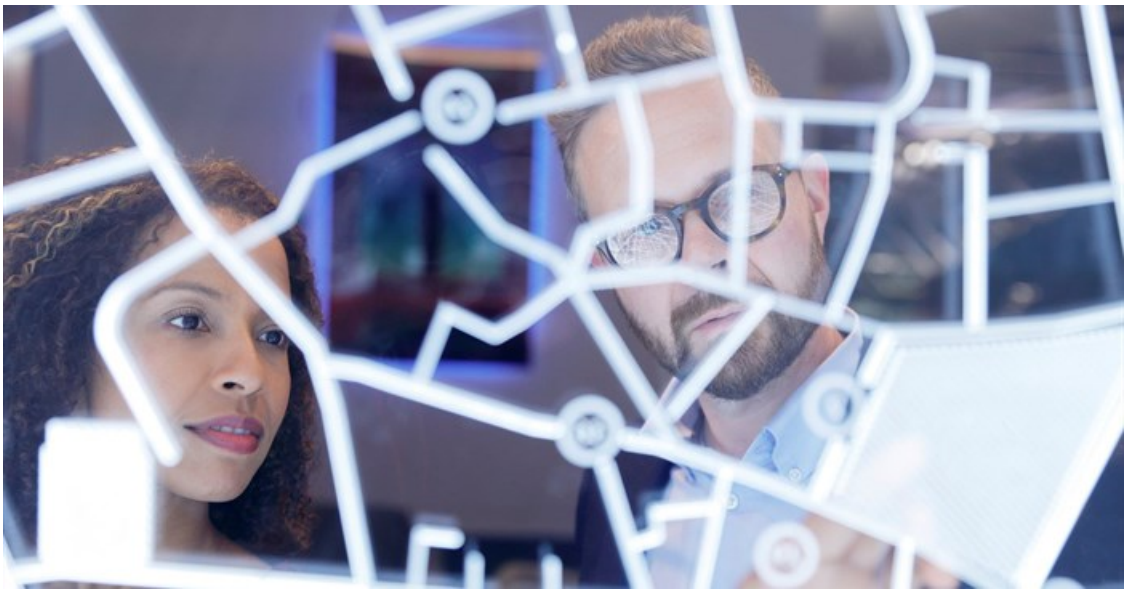

Image source: Gallo/Getty

The logistics industry has been a prime investor in data-centric technologies. Data is their lifeblood - business information has always been important in this high-volume, low-margin sector, but the means provided by digital tools have raised the bar. Everything - from driver behaviour to accurate addressing to vehicle maintenance to route and warehouse optimisation - is driven by data. It's led to greater automation of processes, enabling customers to track packages and delivery staff to follow calibrated schedules pushed to their devices.

It's also made logistics businesses very vulnerable to cyber-attacks.

For example, the Australian logistics giant, Toll, has been hit twice this year by ransomware attacks. And every time this happens, it's a question of whether to redo their entire IT environment. Toll's example is not unique, nor is how it was attacked. Ransomware is an insidiously easy and effective way to block access to data. All it takes is a well-placed infection, and the whole operation can stop. In a data-first sector such as logistics, ransomware can be devastating.

Many companies still don't appreciate how important data is, not until that flow stops and everything grinds to a halt. Data isn't just about insight. It's the fuel for digital engines, and the grease for all the automated and even manual cogs in that machine. If you lose access to your data, you might as well also turn off the power and save some money, while your business tries to drive off the impending financial impact and losses

Criminals don't need this lesson. They understand that companies rely on data. If we just look at marketing information, it's worth billions for big organisations. The criminals understand this. They know exactly what to target and who to talk to.

Logistics companies have been investing in better security, though it's a varying spectrum depending on the size of the company and what they can afford. Smaller logistics businesses are more vulnerable, and when these are brought into the fold of larger companies, they can be a security risk. Attackers can use techniques such as 'island hopping' to break into the larger systems. But larger companies are not immune - don't underestimate how motivated and knowledgeable cybercriminals are. Ransomware is powerful enough that even the dumb ones get lucky, and the smart ones have your number before you do.

Data management fights ransomware

But this can be tackled at the source, namely how you manage your data. I honestly believe that companies should focus on their core strengths. A logistics company should not be worried about security to the point where they have to do it themselves. A managed data service provider can give them the best fit and step in when things go wrong. A ransomware attack is almost inevitable. But recovering from one can be quick with the right data management culture supported by a tried and tested plan.

Data is what modern logistics companies run on, and it's that flow of data that cyberattacks aim to disrupt. A reputable managed data protection service can secure that data and, in the worst case, restore it quickly. It's not just about backup and recovery but appreciating the presence and flow of data in an organisation.

To get to that point, I recommend that logistics companies don't assume that managed data services should cost them an arm and a leg, or that all they get is a service that makes copies of their data. The provider should play a very trusting, integral role to assist in managing the data and growing the business. Small and medium enterprises should be open with the service provider and say: "This is what I'm looking for," and the service provider should be able to say "This is what I can give you."

Data is the lifeblood of modern logistics, and criminals are actively targeting it. Solving this issue can seem very daunting, expensive, complicated and removed from core business activities. It doesn't need to be. The answer lies in data management (not just backup and restore), and managed data protection service providers are the experts in that world.

ABOUT THE AUTHOR

Chris de Bruyn is Operations Director at Gabsten Technologies.