Malware hits Fedex systems

FedEx has confirmed that some of its IT systems have been hit by the 'Wannacry' malware attack that has disrupted companies and organisations around the world, including the National Health Service in the UK.

In most cases, the malware has targeted companies with older Microsoft operating systems such as Windows XP that have not been 'patched' to prevent such attacks.

The express carrier has issued a statement saying: "Like many other companies, FedEx is experiencing interference with some of our Windows-based systems caused by malware. We are implementing remediation steps as quickly as possible. We regret any inconvenience to our customers."

A DHL spokesman said that the express and logistics company "has not recorded any incidents involving the malware on our network, but our IT team is closely monitoring the situation and implementing a range of security measures to further strengthen our defences against any potential attack."

There is widespread speculation that hackers are poised to make further attacks.

A UPS statement said: "UPS is aware of the reported cyber attack impacting some European hospital systems and other companies. Up to now, we have not experienced any impacts. We continue to actively monitor the situation."

HM Revenue & Customs added that none of its services had been affected.

However, Claire Russell, strategic development director at insurance broker and risk management advisor, Perry Appleton Risk Services, said that there had long been concern in the freight and logistics industry over malware and similar attacks on IT systems, and that this had intensified following the recent publicity problems at the NHS.

Over the years, many companies in the sector had suffered attacks, and she stressed that it was important that companies had robust back-up systems, disaster recovery plans and of course suitable insurance cover in place to ensure that they are able to recover from an attack.

Association of Freight Software Suppliers Gordon Tutt said that he had not had any reports from members of any confirmed software problems.

Tim Morris, director of marketing at IT security firm Crises Control said that while Wannacry had gained a lot of attention recently, cyber security was a major if not the major concern of most company chief executives, and had been for some time.

Fortunately, though, there were measures that companies could take to protect themselves, said Morris. "For example, Crises Control's parent company, Transputec, offers cyber security as a service." This can provide a level of expertise, 24 hours, which would be very expensive for a company to provide in-house. It can also take steps to limit the damage and keep people informed.

As well as external threats, there are internal ones, deliberate or accidental. The former would include disgruntled employees, and there are behavioural monitoring systems which build up a picture of normal network activity and which are then able to spot someone, for example, downloading data that they shouldn't, or repeated password attempts.