Phillip Lieberman, President and Chief Executive Officer of Lieberman Software, explains why the most basic security precautions could help save your bacon – especially when a piece of your firm's old kit surfaces on eBay...

Reports that air traffic control data has been found on network kit sold on the eBay Internet auction site comes as no surprise, says Philip Lieberman.

In fact, according to Lieberman - who heads up Lieberman Software, the privileged identity management specialist - the newswires have been peppered with reports of kits containing high-value data being sold on eBay for several years. And, he says, that hardware can contain highly sensitive details about the former owner's infrastructure thrown in for good measure. Whether it's a hard drive configured with cloned passwords or an enterprise network device with its default login still in place, they could all spell potential disaster for the incautious.

BT discovered an Alladin's cave of valuable data gleaned from over 300 pieces of hardware bought at computer auctions, computer fairs and, of course, via eBay, with BT researchers recovering a variety of sensitive information including bank account details, medical records, confidential business plans, financial company data, personal ID numbers, and job descriptions.

This problem is not just confined to the UK. According to 2009 research carried out by BT of computer equipment sourced globally including the UK, US, Australia, France and Germany, 34 per cent of the hardware examined contained '...information of either personal data that could be identified to an individual or commercial data identifying a company or organisation.'

Researchers also found that a '...surprisingly large range and quantity of information that could have a potentially commercially damaging impact or pose a threat to the identity and privacy of the individuals involved was recovered as a result of the survey.'

Lieberman said that all of these incidents prove that – regardless of the security policies in place – the urge to recycle and the current thrifty economy means that a lot of computer hardware will be sold near the end of its economic lifetime for a few pounds.

And, he explained that anyone armed with suitable data analysis software – or even the lists of default logins easily obtained from the Internet – can extract sensitive information and potentially turn it to their advantage.

Upon leaving your organization IT hardware can reveal your most sensitive secrets – including the presence of any highly-privileged passwords that have been reused or cloned (and therefore probably still in use within your datacentre); or the use of administrative logins that are cryptographically weak, unchanged from their defaults, and otherwise easily compromised. The solution, says the Lieberman Software president, is to use privileged identity management (PIM) software. PIM solutions such as Enterprise Random Password Manager (ERPM) can eliminate this risk regardless of whether your equipment is ever recycled or sold.

ERPM, he notes, can automatically discover, strengthen, monitor and recover local, domain and process account passwords in the cross-platform enterprise – preventing weak, easily-guessed, or re-used passwords from being configured in the first place.

“Put simply, the software helps IT professionals achieve full compliance with their security and operational auditor's privileged account password management and shared account password management requirements,” he said, adding that had the staff at the Air Traffic Control who sold on their network gear used this technology, there could be no chance that logins present on those systems auctioned on eBay could ever have been used to compromise the former owner's network.

It is, says Lieberman, perhaps fortunate for UK national security that the £20 Cisco Catalyst switch was bought by security consultant Michael Kemp - the co-founder at Xiphos Research Labs - who discovered that it had been used at the National Air Traffic Services (NATS) centre in Prestwick.

“Had it been bought by anyone with allegiances to a criminal or terrorist group, the security of the NATS operation centre in Prestwick could have been compromised,” he said.

“It's very easy to be over-dramatic about these types of situations, but the brutal reality is that

elementary data security mistakes can hand critical infrastructure data over to dangerous individuals. Nearly all data has a value to someone, so there is a clear risk that embedded credentials stored on discarded hardware – which can be used to attack the former owner – can cause real problems," he said.

Lieberman went on to explain that all these incidents – including the NATS data found on eBay – highlights how valuable a privileged account management solution like ERPM can be, and how it can both save your organisation's bacon and a lot of money in the process.

"In the networking hardware system incident, the seller on eBay reportedly had 12 other similar units up for sale, meaning that these items could have easily fallen into the wrong hands. This could have brought severe repercussions, both for Serco and for the UK's air traffic control systems. So while you might think that automated privileged account management is overkill for your organisation, these cautionary tales show that it's an essential precaution," he explained.