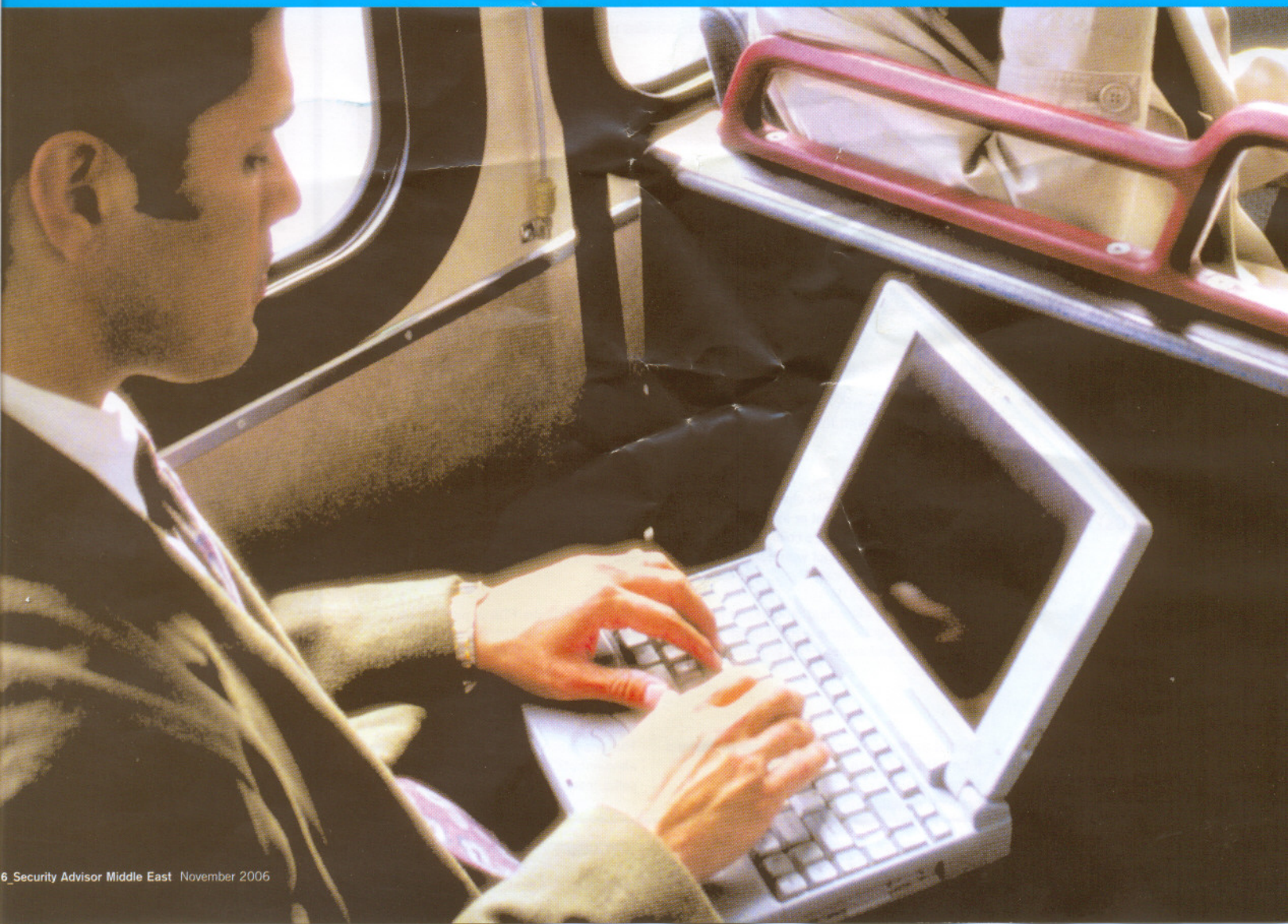


front view

Security on the move

Laptops and Smartphones are increasingly vulnerable to malicious attacks. The threat of having them stolen or lost is also not inconsequential by any extent of imagination. Much more than the hardware that is lost, it is the threat of losing invaluable corporate data that underlines the need for religiously securing your portable devices. The article walks you through some of the key tips on how to do so.



THE THREAT TO DATA CANNOT BE UNDERSTATED

in the world we live. Loss of valuable data can lead to huge financial and credibility loss for businesses. While executives keep flying in and out of different cities that their business takes them, there is always the likelihood that their devices get stolen or lost under some unfortunate circumstances. The threat of losing their portable laptops or smartphones is quite a real one for these globetrotting executives.

Whichever way we look at it, mobile computing has opened up some of the biggest threat areas for I.T. & Security Managers worldwide. Following the classical approach, threats to mobility computing include Industrial spying, Intellectual Property theft and Identity thefts. It has not helped that in recent years it has become increasingly difficult to 'enforce' boundaries on networks and ensure that the network itself is protected; we live in a converged TCP/IP world, where network boundaries are increasingly blurred.

Justin Doo, MD, Trend Micro says, "if you add into this mix mobile workers or 'road warriors' we have personnel carrying, potentially, large amounts of sensitive company data outside of our 'controlled' environment; these mobile workers use Internet access points on un-secured wireless networks, hotel Internet access, home Internet and other corporate Internet provisions – all the time operating outside of the 'protection' of corporate networks. We typically provide these workers with secured access via VPN tunnel etc back inside the corporate infrastructure – thus inviting any malware or antisocial application straight into the heart of our operations – typically unchecked."

Securing these portable devices that hold sensitive and valuable business information is a huge challenge. If a portable device that has company's customer data is misplaced, a following data breach by a mischief-maker can potentially compromise the welfare of thousands of customers and along with that, the company's reputation would also be at stake. However, awareness on this front is only beginning to grow as biometric features and encryption software become more popular with users of mobility devices.

Asem Galal, GM, McAfee, Middle East says, "Just by virtue of being mobile, laptops, notebooks, PDAs and smart-phones face more danger than desktop computers or desk phones. In 2003 an estimated 600,000 notebooks were stolen in the USA only (safeware insurance). Stolen PDA & Smart-phone numbers are much higher. To secure such devices from

theft and to secure information in the case theft or damage happens is now a major focus in the industry."

Proliferation of threats

In addition to this obvious danger, mobility presents a challenge to secure the surrounding environment from attacks and malicious code. Eavesdropping on information transmitted over wireless connection is a main concern with mobile computing. New waves of attacks and viruses specially targeted at PDAs and smart-phones are on the rising. Even SMS spam is becoming more and more of a daily annoyance.

Guillaume Lovetp, Fortinet's Antivirus Team leader, says, "As for smart phones, whenever we run tests with our various customers operating in the field of mobile communications, our statistics show that 3 to 5% of all MMS messages were infected with one of the numerous variants of the Commwarrior worm. In practical terms, this means that up to 1 out of 20 MMS is infected. The threat is therefore absolutely real, in terms of prevalence."

He adds that fortunately, the Commwarrior worm is still in a "proof of concept" stage. That is to say, the goal behind it is not financial yet, and people who get infected are "only" confronted with the bill resulting from the messages sent by the worm to all the contacts on the phone. But this could get worse. Mobile worms could be programmed to send MMS and issue calls to premium rate numbers, hence generating significant loss of money for the infected users (and conversely, tremendous gain for his author, owning the premium rate service being silently contacted).

Sooner or later, only smart phones will be available on the mobile phone market, and the number of smart phones in the world will surpass the number of desktop PCs. It is highly probable that smart phones will become the main target of online gangs, which are now operating on desktop PCs.

Within corporate networks, the usage of portable USB drives or mp3 players also poses serious threat. It's a huge issue because portable devices offer huge storage, upto 60Gb or so on an iPod or an mp3 player. Without overstating the threat, it would be pertinent to add that there is a risk that some one could even steal out a small database on them.

Doo adds, "There is also a growing number of security breaches and incidents being launched 'from within' the corporate network, not deliberately but through the increased portability of applications and environments."



Guillaume Lovetp, Fortinet's Antivirus Team leader.



Asem Galal, GM, McAfee, Middle East



Justin Doo, MD, Trend Micro