

## 2

# The Need to Raise Awareness

The previous chapter suggested that security can be successful only when it is based upon firm foundations. However, it certainly does not stop there. Things can easily go astray if we do not understand what we are doing on a day-to-day basis, and if vulnerabilities are present, then they will eventually cause problems. We readily use new technologies without giving proper thought to their security implications, and we frequently show a lack of regard for security within existing systems that we have used for some time. In some cases, security is overlooked because people are unaware of the relevant information, whereas in other cases it would be more accurate to say that the issue is simply ignored. In either case, the result is that we may not appreciate that a problem is waiting to happen until it is too late. This chapter presents a number of examples to illustrate this point. Although each section focuses around a different aspect of the problem, they ultimately share the common characteristic that those involved were unaware of the threat to which they were exposed.

### Ignorance or Negligence?

Chapter 1 has already established that if you have not taken the time to properly assess your risks, then you are very unlikely to be protected against them. However, if people are honest, their most common countermeasure is often ‘blind faith’. Such faith may take the form of believing that an incident will not happen to them (on the basis that it has not done so to date), or that even if a threat does manifest itself, they will be protected by the standard measures incorporated into their operating system and application software. In fact, when looking at things from an organisational level, one could be forgiven for thinking that many companies are blissfully unaware that there is an issue to address at all. Evidence to support this assertion is, unfortunately, rather easy to find:

A survey of 1000 IT executives, conducted by U.S.-based Computer Sciences Corporation (CSC) in 2001, found that 46% of organisations did not have a formal information security policy in place, and 68% of them did not conduct any form of regular risk analysis or tracking of their security status<sup>23</sup>. These statistics are, of course, indicative of similar problems to those from the UK surveys discussed in Chapter 1. In this case, however, the responses were gathered from respondents all around the world (34% from North America, 29% from Europe, 24% from Asia, and 13% from Australia), suggesting an international problem of organisations that do not seem to be taking their security very seriously.

The Information Security Breaches Survey 2004 (ISBS 2004), from the UK Department of Trade & Industry, asked respondents to consider the importance of information in their business. Each was asked to indicate whether their business held anything that was highly confidential or that would cause significant business disruption if it was to be corrupted or rendered unavailable. The overall responses suggested that 58% had something highly confidential, while 52% and 44%, respectively, believed that corruption and unavailability would be significant problems<sup>24</sup>. Thus roughly half of the respondents in each case considered that their information was not very important—a view that is, to say the least, extremely unlikely to be true. What about customer details, staff records, and financial data? These are fairly baseline categories of information held by most businesses, and the majority would find the disclosure or loss of such data to be a significant cause for concern. It is likely that the respondents were swayed more by their own personal interpretations of what constituted ‘highly confidential’ information (e.g., many peoples’ interpretation of this is restricted to obvious candidates like medical details) and then overlooked the fact that even quite mundane types of data could actually be critical to the operation of their business.

The 1998 Information Security Survey from KPMG illustrates that even where security requirements have been identified, organisations can undermine their own good intentions. Results from 1,000 respondents showed that, although most had formulated recovery plans for use in the event of a security incident, in many cases these had never been tested to see if they actually worked (71% had not tested their business recovery plan, 38% had not tested their network plan, and 25% had not tested their computer system recovery plan)<sup>25</sup>.

Another 1998 survey, this time from the Audit Commission, posed questions about how respondents had identified security breaches in their organisations. The results revealed that an astonishing 50% were only discovered by accident, which did not say very much for the likelihood of there being effective security monitoring practices in those cases<sup>26</sup>.

The 2004 Global Information Security Survey from Ernst & Young found that less than half of the respondent organisations provided ongoing security training for their staff<sup>27</sup>. Given the lack of training, it is perhaps not surprising to find that end users fail to appreciate their role in keeping systems secure. Indeed, an example of this problem is provided by findings from Novell, who surveyed 1,000 users and discovered that 90% of them believed they had no responsibility in preventing the spread of viruses (variously considering it to be the role of their IT department, Microsoft, or the government)<sup>28</sup>. The reality is, of course, that end users can have a significant part to play—a fact illustrated by an example later in this chapter.

Although some of these figures may be alarming, many readers will doubtless have encountered similar problems in their own organisations. But why is it happening? As the title of this section suggests, there are essentially two possible

explanations. The first is that those involved are not sufficiently aware of security to realise that there are issues to be addressed. The alternative is that recognised problems are simply being left unresolved. Although neither situation is particularly desirable, the problem of ignorance is easier to tackle—it may be that a suitable wake-up call is all that is required to get security onto the agenda (issues relating to security culture and awareness are considered in Chapter 3). The cases in which known risks are being left unresolved are more difficult to deal with, and, unfortunately, no definitive solution can be offered. In some cases, further awareness and training could again be a solution. For example, although a risk is recognised, those concerned may not have a clear idea of how it might really affect them if a breach was to occur. Evidence of the undesirable impacts arising from the same incidents' occurring elsewhere could potentially encourage a change of heart. In some cases, however, no amount of third-party evidence will be enough, and an organisation might be convinced to act only if a damaging incident is actually experienced at first hand. For example, loss of data can be a good incentive to start making backups, whereas a spate of hacking incidents may encourage a more comprehensive approach to authentication and access controls.

There are also scenarios in which problems of ignorance and negligence may intersect. For example, in some cases people will have enough awareness to realise that there is a risk, but do not attempt to understand the details of why, or what they ought to do about it—and so leave it unresolved. A practical illustration of this is provided by the use of wireless networking technologies, which are examined in more detail in the next section. The security of wireless networks has received so much publicity in the technology media that the vast majority of system administrators (and indeed the more IT-aware home users) must realise there is a potential risk with using them. At the same time, however, many deployments remain chronically insecure—suggesting that the owners have not taken the risk seriously when considering their own situation.

Of course, it would be rather unfair to suggest that all cases of known risks' remaining unresolved are completely attributable to negligence. In some cases, financial constraints, lack of technical expertise, and other practical limitations will represent legitimate reasons that prevent risks from being addressed. Indeed, some of these issues are picked up as part of the discussion in the next chapter. For now, however, the remainder of this chapter provides some examples of how ignorance or disregard for security considerations can ultimately cause problems for those concerned.

## **Walking in a Wireless Wonderland?**

A frequent benefit of new technology is that it enables us to do things more quickly, cheaply, flexibly, or efficiently than we have done before. Unfortunately, however, these benefits sometimes come at a price, and in computing circles this is often paid in terms of the security or reliability of the technology concerned. Nonetheless, so great are the perceived advantages that the technology has to offer, that people rush to embrace them, without giving much, if any, consideration to the associated

security risks. A very good example of this can be seen with the deployment of wireless networks, which have become very popular in recent years, particularly in a corporate networking context.

Before launching into a discussion of the security issues, it is relevant to spend a few moments explaining what wireless networking is all about. At the most basic level, what we are talking about is networking our devices together without the need to run cables between them—which has some fairly immediate benefits in terms of cost and flexibility. There are actually several forms of wireless networking, from satellite-based services (with large-scale geographic coverage), down to short-range radio technologies such as Bluetooth (which can now be found in a variety of mobile devices, allowing them to talk to each other provided that they are in close enough proximity). However, the technology that has given rise to the majority of discussion about security sits in between these two extremes—the Wireless Local Area Network (also known as wireless LAN, or WLAN). Indeed, despite having inherent security provision, WLAN managed to acquire a reputation as one of the least secure technologies around.

As the ‘local area’ part of the name suggests, WLANs provide network coverage within relatively small areas such as offices and homes. Commercial WLAN products have been on the market since mid-1999, and recent years have seen the technology become very popular—largely because it is seen to be a convenient method of providing access that does not impose the investment demands of traditional wired networking. Indeed, such has been the popularity that wireless coverage is now routinely being deployed in public areas such as airports, hotels, and coffee shops. When WLANs are used in this context, people will naturally expect (and probably intend) that a wireless access point will be detected by a multitude of wireless devices in the vicinity. However, when a wireless network is deployed in a private environment (e.g., at home or in an office), then the intention will almost certainly be that access to it is reserved for the specific users for which it was installed. It is here that the security issues start to appear. In general terms, not only do WLANs face all of the security issues that may trouble their cabled counterparts, they are also more vulnerable to other threats as a specific result of the wireless medium. The first issue is that, although the owner of the wireless network may like to think that only the intended users can see it, the radio waves could be propagating significantly beyond the range actually required. For example, a typical operating range quoted for a consumer-level wireless access point is 450 metres, assuming line of sight and no interference. The presence of physical obstacles such as walls will certainly reduce the signal strength, but the network may still reach people in neighbouring buildings, or parked in the street outside—in fact, under the right conditions the radio signals could be picked up several buildings away. So, what are the implications of this? At a fairly benign level, you could find that other people are piggybacking on your access point and using up some of your network capacity without paying for it. Although this is certainly a bit cheeky, it does not significantly affect the security—unless of course the freeloaders place such a drain upon network resources that it impacts the availability for legitimate users. A more direct threat to security could arise from the potential for eavesdropping on data.

Transmission over the air means that data is far more vulnerable to illicit interception than when it is sent through wires. In a wired context, an eavesdropper would need to tap into a physical line, but now the data can literally be plucked from the air by just being in the vicinity of the access point. Encryption techniques can be used to preserve confidentiality, but as later discussion will establish, many wireless networks have failed to do this. Additionally, the threats do not stop at eavesdropping. An unprotected wireless link could also be exploited to allow unauthorised access to legitimate users' devices, including any software and data that they hold.

Of course, because of such recognised problems, the instinctive expectation would be that anyone considering the use of wireless LAN would take appropriate steps to protect themselves. Unfortunately, however, most survey evidence suggests that, although deployment is increasing dramatically, very little attention is being paid to security. Indeed, as far back as 2002, the issue of insecure wireless networks was already such a recognised problem that the U.S. president's special advisor for cyberspace security was citing them amongst his top five security offenders, warning that

Companies throughout the country have networks that are wide open because of wireless LANs.<sup>29</sup>

Further illustrating the level of concern in official circles, the Office of the Secretary of Defense in the United States subsequently restricted the use of many wireless technologies, with a memorandum promoting the release of the Pentagon Area Common Information Technology Wireless Security Policy in September 2002<sup>30</sup>. This policy prohibited the connection of wireless communication devices to classified computers or networks. In addition to wireless LANs, the restriction also encompassed other devices with wireless communication capability, such as cell phones and Personal Digital Assistants. Indeed, it required any "network-capable, wireless computing devices" within the environment to utilise appropriate mechanisms for user authentication, as well as facilities to allow their wireless transmission capabilities (whether they are radio frequency- or infrared-based) to be disabled.

Of course, users in other environments may consider their systems to be at somewhat less risk, and assume that while the Pentagon has to protect itself against targeted attacks, other wireless networks would stand little chance of even being discovered. However, the latter excuse can be quickly shot away—not least because some people have actually started searching for wireless LANs as a hobby, and openly publicise the results of their activities. In fact, the hunt for wireless networks has given rise to a couple of new terms in the networking community. The first is WarDriving, which basically means driving around searching for insecure wireless networks, and the other is WarChalking, which refers to the practice of marking symbols on pavements and walls to indicate nearby wireless access facilities<sup>31</sup>. So, not only could people potentially stumble across the existence of your network, they might also literally signpost it for the attention of others.

Although WarDriving and WarChalking are not exactly mainstream activities, both have made enough headlines to prove that wireless LANs are not hard to find, and unsecured networks cannot simply rely upon being hidden from view.

Getting the equipment to become a WarDriver is not particularly difficult—a typical kit involves a laptop or handheld computer, equipped with an omnidirectional antenna, and suitable network-sensing software, such as NetStumbler (see [www.netstumbler.com](http://www.netstumbler.com)). In fact, such is the popularity of WarDriving that the activity has even given rise to annual event—the WorldWide WarDrive (WWWD). At this point it is worth noting that WarDriving does not involve hacking the networks that are discovered, and thus the activities are not illegal. The participants in the WWWD, for example, do not actually connect to the networks that they find, and the event’s website provides links to guidelines on other aspects of good conduct in an attempt to ensure that the WarDrivers stay within the law (e.g., advising them to obey traffic laws, and to take notice of property signs to prevent them from trespassing in their quest to chase a signal)<sup>32</sup>. Nonetheless, the WarDrivers’ results have provided a good indication of the poor state of WLAN protection. The various participants in the fourth WWWD event (which was held from June 12 to 19, 2004) found a total of 228,537 access points. Of these, around 62% did not have encryption enabled, and 31% were still found to be using a default network identifier (almost 28% exhibited both problems)<sup>33</sup>. The lack of encryption would have left the traffic on the network vulnerable to eavesdroppers and would also have removed one barrier to unauthorised users’ sending their own data into the network. Meanwhile, using a default network identifier (or to give its proper name, the Service Set Identifier or SSID) would have removed another barrier. The SSID can provide a basic form of authentication for devices wishing to connect to the network—acting like a shared password, with a wireless device needing to have the same SSID as the network it is trying to use. However, each WLAN access point comes with a default name specified by its manufacturers (e.g., the default SSID for Intel equipment is ‘intel’), and so if this has not been changed, then attackers will not need to work to discover the information.

Aside from discovering that almost two thirds of networks were not properly protected, another notable finding was that the 2004 results were not dramatically different from those of previous WWWD events. All four events up to this point had found that somewhere between 62% and 72% of wireless networks lacked encryption. The main difference was that successive WWWD events found substantially greater numbers of networks upon which to base their percentages (rising from tens of thousands in the first few events to well over 200,000 in 2004). There are, of course, many reasons to explain the larger samples (e.g., having more participants and covering new regions), but whatever way you look at it, ignorance of security issues was continuing to triumph. Either new networks were being deployed without security enabled, or existing networks (that had not previously been discovered) were continuing to operate insecurely. This provides a good illustration of just how difficult it can be to address security if it is not present from the outset.

All this leads to the rather obvious question of what people ought to be doing to protect their networks—and having established how important it is to secure wireless network environments, it may now seem a little disappointing to find that it is not quite that simple. The Pentagon policy mentioned the need for technologies such as authentication, intrusion detection, and virus protection, but these are



actually things that ought to be used in a network anyway—whether it is wireless or not. When considering the wireless networking context more specifically, there are some additional points to address. As a starting point, many breaches could be avoided by employing some fairly basic security measures in relation to wireless access points:

- ensuring that access points are located away from the outside walls of buildings (thus reducing opportunities for outsiders to pick up signals);
- enabling the use of the device's encryption capabilities;
- changing the network identifier value from the default;
- changing the administration password for the access point from its default setting (defaults are documented in manuals, so anyone can find them out).

Although these steps would dramatically reduce some of the high vulnerability statistics reported by WarDrivers, readers who are already familiar with WLAN may also be aware that the security features in early versions of the technology were not very good anyway. The encryption method used by first-generation WLAN devices, the Wired Equivalent Privacy (WEP), could be broken, and network identifiers could still be determined even if you changed them from the default names. As such, determined attackers could still find a way in. However, it would be unrealistic to believe that this was the main reason that security was not being used, and even the flawed methods were still of some value as safeguards against attackers of a more opportunistic nature. Meanwhile, newer WLAN technologies have come to include more capable security features, based upon more robust mechanisms, and so users of more recent kits cannot claim that the protection is too weak to bother with.

Overall, the discussion of wireless networks has given us an example of a technology that *can* be secured to some extent, but where many deployments have nonetheless occurred without protection at all. Faced with a technology that cannot be fully secured, there are some cases in which it is necessary to take a hard-line view (like the Pentagon did) and simply not use it. In other cases, the solution does not have to be that severe. For example, as long as people are made aware that protection is lacking, then, in some cases, they can make their own decision about whether to use the service or not. The real problem with wireless LANs has been that too few of the people using and deploying them had thought to ask the question.

## **Users Go Mobile . . . but Security Stays at Home**

Another context in which security is most definitely required, but many people have not got to grips with it yet, is with mobile technologies. In the past we might at least have been able to rely upon our systems staying in one place, but since the advent of laptop computers, they have frequently moved around with us, placing them at increased risk of loss or theft. Over time, the range of mobile devices has broadened to include pocket computers and mobile phones, and all of them have the capability to store and communicate sensitive data while we are on the move. Security issues

can consequently be identified in all of these contexts, and there is plenty of evidence to suggest that related incidents are occurring.

In considering these devices, the discussion will focus upon aspects that the user can control, with the aim again being to show that a lack of attention or awareness can lead to vulnerabilities that would otherwise be avoidable. This is not to suggest that the points identified are the only ones that apply to the devices. For example, a clear security issue in the context of mobile phones is the prevention of eavesdropping, which can be addressed by encrypting the transmission. To date, however, this aspect has been under the control of the network operator, and so the user has no decision to make. However, as some of the following examples will show, even when users do have the opportunity to protect their devices, they often fail to use it properly.

### ***Protecting Pocket Devices***

By far, the most common mobile device is, of course, the telephone, which has rapidly become one of the most popular forms of technology in everyday life. Nonetheless, these offer significant potential for security incidents—with a fundamental reason being that they have proven to be attractive targets for thieves. For example, a study from the UK Home Office, published in December 2001, suggested that over 700,000 phones had been snatched from users in England and Wales during the previous year<sup>34</sup> (a rise of 190% since 1995). With this threat in mind, it is interesting to consider how seriously mobile users take the security of their devices. Relevant evidence here can be cited from a survey that was conducted by my research group, which aimed to examine the attitudes of mobile phone users and assess the degree to which they used available security features to protect their device in case it was to be lost, stolen, or left unattended<sup>35</sup>. Questionnaires were distributed to a broad range of mobile phone users, yielding over 160 responses.

To date, the main user-configurable feature has been a personal identification number (PIN), which the user must enable before any protection is actually provided. With this in mind, the most significant survey finding was that, although 89% of respondents knew about the facility, only 56% actually used it (of those who did not, 65% blamed inconvenience). It was also discovered that 26% had told their PIN to someone else, and 17% had forgotten it, meaning that they could not use the facility if they wanted to. In spite of these relatively poor results, it could be argued that the level of security delivered by the PIN was sufficient for the type of device being used. The potential consequences arising from theft or impostor access to a basic mobile phone could be broadly categorised as financial loss (due to the possible loss of the handset and any subsequent calls placed using it) and breach of personal privacy (due to the impostor's gaining access to contact details and text messages held on the device). In the case of a stolen phone, the thief's ability to run up a bill at the owner's expense could also be limited, in some cases, by reporting the theft to the network operator, who could block subsequent use. In terms of data loss, meanwhile, there would often be little to tell. Typical handsets would reveal telephone numbers and possibly a number of text messages, and although there would be the



potential for these to be classed as sensitive information in some contexts, it can be reasonably assumed that the impacts of disclosure in most cases would be minor or nonexistent. However, more recent devices (so-called smartphones) are increasingly geared towards a far more advanced profile of data services, many of which are linked to the concept of mobile commerce (mCommerce), including

- digital wallets
- event ticketing
- mobile shopping
- electronic banking
- payment-based entertainment services (music, video, games, etc.)

In the survey, we discovered that 88% of respondents were interested in being able to access such additional services, and as a consequence their phone could hold a variety of more sensitive information. All of this would naturally increase the potential for misuse if a device permitted access without authenticating the user.

With the arrival of smartphones, the overall functionality has converged with that of another pocket device—the Personal Digital Assistant (PDA). These have already been with us for some years as standalone devices, with major standards having emerged in the form of PalmOS and Microsoft's Pocket PC, but the user community has been much more focused towards the professional market. However, when considered from an organisation's perspective, PDAs have a number of characteristics that serve to increase their risk when compared to other devices that employees may use. One of the most obvious issues is still the size and inherent portability of the devices, which increases their susceptibility to accidental loss, while the increasing functionality increases their desirability to thieves. Another increasingly important factor is their potential connectivity, with current PDAs supporting personal, local, and wide area networking capabilities. If used or configured incorrectly, this means there are several ways in which a device could inadvertently leak data, or leave itself open to unauthorised access. Indeed, results reported from a study by Gartner Inc. in 2004 suggested that around 90% of mobile devices lacked protection to prevent hackers from gaining access<sup>36</sup>. A third issue is the actual ownership of the devices. Whereas the desktop and laptop computers used within the workplace are typically purchased by the organisation—which consequently has the ability to securely configure them and the right to restrict the software and services deployed on them—most mobile devices are owned by the employees themselves and are therefore outside the organisation's administrative control. Nonetheless, employees may use their devices in the workplace, synchronise them with office PCs, and use them to carry potentially sensitive company data—all of which introduces a level of risk. For example, in May 2002, UK-based *Computer Weekly* magazine revealed the results of a survey that it had commissioned to assess the security awareness of PDA users. A total of 332 IT professionals were surveyed, revealing a number of notable trends in terms of their use of the devices:

- 89% used it as a business diary;
- more than a third of devices carried corporate information;

- 46% held passwords or PINs relating to other services;
- a “substantial” number held customer information, credit card numbers, and social security details.

From this, it is clear that valuable and potentially sensitive information is routinely held on PDAs, and as such, the potential consequences of the devices’ falling into unauthorised hands could be severe. Such issues provide another reason for having a clear and well-promoted security policy and ensuring that users are made clearly aware of what is permitted. Unfortunately, the *Computer Weekly* findings were not very encouraging in this respect:

- only 35% of respondents indicated that their companies had a specific policy to regulate the use of PDAs (e.g., to indicate what data could legitimately be transferred to the device and carried around; what level of protection needed to be enforced when devices were on the move, etc.);
- 41% claimed never to change their passwords, and a further 26% only did so infrequently (the reported results did not address the other forms of misbehaviour that were previously observed in relation to mobile phone PINs, but it would not be surprising to find similar problems occurring).

When considering the fact that they are often using their own personal devices, the potentially lax practices of users represent a tricky problem for the organisation, as it cannot easily mandate the appropriate use of a resource that it did not provide. As such, many environments are electing to ban the devices from the workplace altogether. This at least aims to reduce the risk posed by the devices from the business perspective. Nonetheless, as more people are provided with comparable functionality in their standard phone, the more it will be utilised by nonbusiness users as well. As such, without a change in attitudes towards the protection of such devices, there will be increased amounts of personal and private data up for grabs.

### ***Laptop Laxity***

If the security of pocket devices is a problem, then a possible explanation is that they are still relatively new technologies, which users may not think of protecting in the same way as their desktop systems. However, this excuse clearly cannot apply to laptop computers, which have been around for much longer and are clearly comparable to desktop PCs in terms of the operating systems, applications, and data that they handle. In this sense, a laptop ought to have at least the same level of protection that we would give to a comparable desktop system, as well as additional consideration to account for the fact that it will be used outside the (theoretically) safe confines of a home or business environment. Unfortunately, however, the evidence suggests that despite the obvious risk resulting from their mobility, the security of laptops is approached in a fairly cavalier fashion. For example, surveys have shown that they frequently slip through the net in organisational scenarios and are not subject to the same restrictions that might be applied to PCs permanently situated in the environment. As a consequence, it is not unusual to find laptops lacking

password protection and properly updated antivirus software, as well as being out of the loop when it comes to things like backups. A good statistic for the later came from a 2003 survey commissioned by disaster recovery firm Veritas, which questioned 850 IT managers in the United States, Europe, and the Middle East, and found that although 90% of them had backup regimes for their desktop systems, laptop computers were far less protected (with a fifth of respondents making no backup provision at all, and 32% leaving it up to end users<sup>37</sup>). Even more surprising, however, is the apparent lack of attention when laptops are on the move. Consider, for example, the UK Ministry of Defence (MoD), which, according to figures that emerged in early 2002, had lost almost 600 laptop computers in the previous five years (with the devices having been either stolen or mislaid). In contrast to average members of the general public, the MoD would, by its very nature, be expected to take more care than most in safeguarding such assets—which, of course, served to make the published statistic all the more surprising. A spokesman at the time sought to downplay the significance, pointing out that “not all laptops contain classified information”<sup>38</sup>. The statement was, of course, quite revealing in what it did not say—it implicitly made the point that some laptops *did* contain classified information, and it did not deny that such data was lost. Indeed, one might instinctively assume that, unless the parent organisation has policies and controls in place to prevent it, laptops are quite likely to contain significant information—by virtue of the persons they are allocated to. The justification for this assumption is that, in general, laptops are not routinely given to all employees and are therefore more likely to be the preserve of higher-ranking personnel. These individuals are, in turn, likely to have access to more significant information—which they will carry around on their laptops in order to keep it available to them. The validity of these assumptions is illustrated to some degree by example cases that are presented ahead.

The MoD is by no means the only UK government agency to have fallen victim to the problem. The figures published in January 2002 revealed that the total number of government laptops lost (i.e., stolen or mislaid) since 1996 was 1,354. The distribution of these and the departments concerned are shown in Table 2. Meanwhile, outside the UK, organisations such as the U.S. State Department and the FBI have also suffered the theft of laptops containing sensitive information, illustrating that as with other aspects of security, this problem is international in nature.

TABLE 2. UK Government Laptops Lost from 1996–2001<sup>39</sup>

Department	Laptops lost
Ministry of Defence	594
Work and Pensions	419
International Development	115
Department of Trade & Industry	79
Lord Chancellor's Department	77
Cabinet Office	43
Treasury	14
Northern Ireland Office	3

With so many government laptops having been lost, it is not surprising that some of the incidents have hit the headlines in their own right. Indeed, these help to shed light upon why the losses occurred, and it is clear that, in many cases, security policy was not being very carefully adhered to:

---

March 2000	An MI6 officer left his computer in a taxi after an evening out drinking in a tapas bar. The computer, which contained training information relating to the intelligence agency, was recovered by the police two weeks later <sup>40</sup> .
March 2000	An MI5 officer's laptop was snatched when he put it down at Paddington Underground station (either to buy a ticket or to help a passer-by—reports vary on this issue). The laptop contained classified information about the situation in Northern Ireland, but the cause was believed to be an opportunist theft rather than a planned attack <sup>41</sup> .
March 2000	A laptop was stolen by an intruder who broke into the home of John Spellar, the armed forces minister at the time <sup>42</sup> .
May 2000	A naval intelligence officer lost his laptop, and other personal luggage, after boarding a train at Paddington station. The computer allegedly contained the specifications of a next-generation fighter aircraft, and was returned to the MoD after a dealer (who had bought it from the thief) tried to sell the story to a UK tabloid newspaper for £15,000 <sup>43</sup> .
April 2001	A laptop belonging to a Ministry of Defence consultant was left in a taxi after a journey from London's Waterloo station <sup>44</sup> .
July 2003	A man was charged with stealing a laptop from the Cabinet Office of the UK government. The theft prompted a government admission that a total of three laptops had actually been stolen from the Cabinet Office in the preceding weeks, as well as three more from other government buildings <sup>45</sup> .

---

There is, of course, more at stake here than simply the embarrassment of having the incidents reported in the media. For instance, the Gartner Group estimated that the loss or theft of a laptop may ultimately cost an affected organisation over £6,000 per incident—some three to four times the cost of the device itself<sup>46</sup>. Furthermore, this figure does not take into account the potentially most significant aspect of all—the value of the data that the system might have contained, and the implications of it falling into the wrong hands. In all of the examples listed above, the laptops could conceivably have contained confidential information, the disclosure of which may even have threatened national security.

### Dangerous Disposal

Even in cases of loss or theft of equipment, the incidents are often excusable (or at least explainable) to some extent on the grounds of human error, or the fact that attempts to protect the assets may simply have failed. In other cases, however, the organisations concerned can simply be seen to have been manifestly careless in their regard for IT equipment security. A classic case is the disposal of equipment where, in contrast to accidental loss or theft, the systems concerned are known to be leaving the organisation, and yet appropriate measures are not taken to ensure that sensitive or confidential material is removed beforehand.

It is not uncommon for PCs or internal components that have reached the end of their useful life to be resold, donated to other organisations, or simply junked altogether. However, any system that has been in use will doubtless have software installed, and more importantly will have accumulated data during its past life. As such, one would expect any confidentiality-conscious owner to remove such material before allowing the hardware to leave. In practice, however, the issue is often overlooked, leading to the risk of the associated data's ending up in entirely the wrong hands. To illustrate the problem, here are some fairly typical cases that have been reported in the media over the years:

Back in December 1993, three computer hard disks that had been disposed of by the UK Department of Health were purchased by a dealer at a second-hand computer equipment sale. It was not until about a year later, when he examined their contents, that the dealer discovered the disks to be holding more than 4,000 files, containing internal Department of Health materials such as confidential reports and memos<sup>47</sup>. Amongst these documents were the diary of the then health minister, personal information about the department's staff, and a variety of sensitive reports, such as confidential assessments of companies as potential health service suppliers, and the first draft of a policy relating to care for mental health patients.

In early 1998, a freelance computer consultant purchased a laptop computer from a high-street electronics outlet. The machine was advertised in the shop as being "ex-demonstration", but upon taking it home, the purchaser soon discovered that it contained a variety of details belonging to a previous owner. The owner in question was a psychiatrist, and the details stored on the hard disk included personal correspondence, patients' letters, appointment information, and name and address details—all of which could be regarded as confidential and sensitive information, showing that the individuals concerned were receiving psychiatric care. In the wrong hands, this could have led to the patients' being contacted and subjected to blackmail, but the issue was ultimately brought to the attention of data protection officials instead. It transpired that the computer had been returned to the high-street store after it had developed a fault while still under warranty. The psychiatrist claimed that the store had promised to wipe his data from the system, whereas the store subsequently claimed that they had not been told the system contained sensitive information<sup>48</sup>.

In September 2001, UK police were called in to investigate how a computer that had been used in a university research project about child abuse cases had been sold to another party while still containing data that included the names of alleged paedophiles and their victims. The computer had been used as part of a Home Office project conducted at Bristol University, and after the study had ended, the PC was passed to a postgraduate student, who later sold it at the students' union. It was only when a computer company was later asked to perform a virus check on the machine that the sensitive data was found lurking on

its hard disk. The files, containing information such as testimonies and transcripts of police interviews, had originally been provided by the police and the Crown Prosecution Service and should have been deleted as soon as the research was completed. Indeed, this was the stated policy of the university, and the incident was a catalyst for an urgent review of its procedures. Meanwhile, the abuse victims and their families, who had not even been told that their details had been released to the university, were understandably concerned that the information should find its way into public hands. As the mother of one of the victims told reporters, “It’s disgusting really. It’s supposed to be private and confidential. It’s not supposed to leak out. . . . You put your trust in the professionals who deal with these things and it seems they trivialise it”<sup>49</sup>.

It would, of course, be fairly easy to dismiss these as isolated incidents and assume that organisations in general are more careful. In January 2003, however, the results from a study conducted by two graduate students at Massachusetts Institute of Technology (MIT) gave an indication of the true scale of the problem. In this particular case, the researchers set out with the specific intention of obtaining second-hand hard drives just to see what data they could find; they spent around \$1,000 purchasing 158 such devices from sources such as eBay. When they came to analyze their hoard, the researchers discovered that 44% of the drives still contained recoverable files (in fact, in 18% of cases, no attempt had been made to delete the information in the first place). The most significant finding, however, was that 31% of the drives contained some form of sensitive personal information. The nature of the information, to quote an MIT press release, included

more than 5,000 credit card numbers, detailed personal and corporate financial records, numerous medical records, gigabytes of personal email and pornography<sup>50</sup>.

The published version of their study, which appeared in *IEEE Security & Privacy*, also cited figures from Dataquest indicating that some 150 million disk drives were retired from service in 2002<sup>51</sup>. If the findings from MIT are scaled up to estimate the likely proportion of these that still contained sensitive data, this suggests that a massive amount of material is up for grabs—with a 30% chance of you finding some if you buy a second-hand drive.

In all of the preceding cases, the problems and bad publicity would have been avoided if the data had been erased from the disks prior to disposal. Having said this, however, successfully erasing data so that no trace can be recovered is not as easy as it might sound. It is not, as many people might suppose, simply a question of using the standard ‘delete’ operation that is provided in PC operating systems such as Windows. Contrary to what the command suggests, it does not actually delete the file from the disk (even if you empty the recycle bin or trashcan)—it simply removes the name of the file from the look-up table that the computer uses to find its position on the disk. The file itself remains intact until the portion of disk space it is occupying is later overwritten with new data (and even then old files may



be only partially overwritten—which effectively means that they are also still partially recoverable). Even formatting the disk does not wipe it clean—in the MIT study, for example, the 5,000 credit card numbers mentioned above were recovered from a reformatted disk. Of course, this apparent deficiency is not really a problem while a machine remains in the possession of the same user, and it still serves the purpose of freeing up disk space for other uses. If, however, a computer (or, of course, just its hard drive) that has contained sensitive data is to be sold, passed on to another user, or simply thrown away, then a more secure method must be considered in order to sanitise it and prevent the data from being recovered by someone else. Several options are available, the selection of which will depend upon what is to happen to the computer (or hard drive) and the sensitivity of the information that it held:

### **Overwriting**

This involves a low-level reformatting of the disk to wipe the original data, followed by multiple iterations of overwriting the whole disk with random data. This serves to make the original information difficult to recover. A number of suitable secure delete applications are available, such as *Cyber Scrub* and *Data Gone*, and anyone disposing of a PC that has held sensitive information would be well advised to use one.

### **Degaussing**

Hard disks are magnetic media, and a degaussing operation attempts to wipe the disk by demagnetising it using alternating electric currents.

### **Destruction**

To be sure of totally removing the opportunity for data to be recovered, the disk should be completely destroyed. It should be noted that even cutting or breaking a disk into pieces will not prevent data recovery by a determined attacker. A method such as incineration can be considered far more effective, and specialist companies can be found that offer such a service if it cannot be performed in house. It should also be noted that destruction is the only option when disposing of storage media such as CDs, as these cannot be overwritten or degaussed to remove sensitive data.

Ultimately, if the system is to be disposed of, then the method chosen should be one that would make the task of recovery (in terms of cost and effort) exceed the value of the data concerned. If the information is of such sensitivity that a value of this nature cannot be placed upon it, then there is no option but to destroy the media concerned (so, if the computer itself is to be reallocated or sold, then this must only be allowed to happen once its hard drive has been removed). Organisations dealing with this level of sensitive data on a routine basis, such as the U.S. Department of Defense, typically have policies and guidelines in place to address the issue<sup>52</sup>. Unfortunately, the fact that other organisations do not routinely handle such obviously sensitive data does not exempt them from this consideration, and the examples above illustrate that, without appropriate attention, serious oversights may occur.

## Your PC Can Tell a Story

All of the discussion about losing computers or disposing of them with data still intact certainly draws attention to the need to protect information from accidental disclosure. However, it also leads to the interesting question of whether we know what to protect. In short, do you know what is stored on your computer? My guess is that most people would say yes, especially when talking about a machine on which they are the only user. In many cases, however, they would probably be surprised. This is not because they have been careless in organising their files, or have just forgotten things that they saved or installed a long time ago, but because the computer stores things that many people are unaware of. A very good example of this is the information that gets stored on your PC by a web browser. As many readers will have found, some web pages can take a long time to download, particularly if you are using a slow link or the page contains a lot of images. The developers of web browsers are aware of this, too, and have included facilities within the software to help alleviate some of the problems. Chief amongst these is the fact that the browser maintains a local copy (or cache) of the various elements that make up a downloaded web page (e.g., text, images, and other embedded content), so that if you visit the same page again the main content can be retrieved from the local version rather than having to be downloaded again. This has the advantage of making things much faster, as well as offering the facility for pages to be browsed offline if you have already cached all of their content. In a typical PC environment running Windows, the cache is physically stored in the 'Temporary Internet Files' directory. From the average user's perspective, this directory is effectively buried away, out of sight, in a Windows subdirectory, possibly several levels deep (e.g., on a Windows XP system, the path to the browser cache would be 'Documents and Settings\user-account\Local Settings\Temp\Temporary Internet Files', where *user-account* is the login name of the associated user and all of the 'Local Settings' content is in a hidden folder)—where most people generally do not go looking unless they already have a very specific purpose in mind.

All this is fine, you may say, but why should I be worried about it if my family and I are the only ones that use the computer anyway? What does it matter if this 'hidden' information is lurking around? Well, there may be some scenarios in which at least knowing that it is there would help to enable an informed decision about whether it should stay there. What if the PC was to leave your possession—e.g., to be sent away for repair? This was exactly the scenario that occurred for the vintage British rock star Gary Glitter, who got somewhat more than he bargained for when he took his faulty Toshiba laptop back to a PC World computer store for repair in November 1997. With a celebrity's machine in their possession, the PC World repair staff seemed to get a little curious, and despite a request from Glitter not to look at the files, they began to browse the contents of the laptop's hard disk. If their aim was to unearth some of Glitter's secrets then they certainly succeeded—their inspection of the disk revealed a large stash of indecent images, including pornographic pictures of children being sexually abused and tortured. At this point, having Gary Glitter's PC in the repair shop became more than a matter of in-house gossip, and

the story found its way to the police and the media. Any protests on Glitter's part that PC World staff had no right to be nosing around on his computer in the first place were, unsurprisingly, drowned out by cries of outrage and disgust from all other quarters at the discovery that he possessed such material. The story led to Glitter's arrest and, ultimately, a jail sentence of four months (along with his name being entered onto the UK register of sex offenders for seven years), after he admitted to 54 charges of possessing child pornography downloaded from the Internet<sup>53</sup>.

It could, of course, be argued that the Glitter case is not a particularly good one to illustrate the point that people ought to have more knowledge about what can be found on their PCs. In this case, Glitter clearly got what he deserved. However, in the first instance, he had protested his innocence in the matter, and at one point his defence had claimed that the images had been cached when he inadvertently visited web sites hosting such content by mistake. This claim is not quite as ridiculous as it might first seem. It is sometimes possible to enter a web address or navigate to a site with the expectation that it will be about one thing, only to arrive and find something totally different. For example, anyone looking for information about the rock band Queen might reasonably make a guess that *www.queen.com* would be a good place to look. However, going to that site (at the time of writing at least) would not lead to pictures of Freddie Mercury et al., but to pictures and other material of an adult nature. Such material could then end up being stored in the Temporary Internet Files directory of the user's PC, providing implicit evidence to suggest an interest in looking at pornographic pictures, even though this was not their intention at all. In Glitter's case, there were a total of some 4,000 incriminating images on the hard disk, leading to the suggestion that he may well have used the PC almost exclusively for such pursuits<sup>54</sup>, and certainly undermining the possibility of a defence that he had happened upon them all by accident.

The Glitter case related to the discovery of material that was illegal, and so there was not much scope for disagreement about what should have been done with it. However, the issue will not always be as clear-cut as this—what if the material discovered is simply private or sensitive? In this context, the desirability of maintaining proper security is easier to see. To give a suitable illustration of this, let us consider the true story of Alice and Bob, an estranged couple in the process of a divorce. Their parting had not been amicable, and it was not until several months later that Bob managed to get some of his belongings back. Notable amongst these was a PC, and upon using the machine, Bob quickly discovered that Alice had taken steps to remove her personal information from it, deleting the directory in which she had stored all of her documents, and deleting some of his as well for good measure. However, she had by no means removed everything. Although Alice did not realise it, the browser cache was still there, and it had maintained many details of her previous six months or so of web browsing sessions (with the system configuration setting aside around 190MB of disk space for the storage of temporary Internet files). It was very unlikely that Alice even knew that the cache directory even existed, but Bob did—and so, in the absence of very much else being left on the computer to look at, he set about examining what it had to say. It did not take long for him to make a few revealing discoveries, that gave him more than a little insight into what

Alice had been up to in the months since his departure. Particularly revealing information was provided by pages that had been cached from the Yahoo! web-based email service that Alice seemed to favour. From the content and dates of the cached pages, Bob was able to establish the following chain of events:

- On the day he had left, Alice had enrolled with an online dating agency (apparently wishing to waste no time in finding a replacement!).
- She had received contact from, and subsequently corresponded with, a number of different parties through the agency.
- She began a more focused dialogue with one person in particular, leading to some quite intimate and explicit messages, which were ultimately occurring alongside telephone conversations and face-to-face meetings.
- Other email correspondence revealed job applications and property enquiries that Alice had emailed to agencies in the region where her new friend lived.
- Alice's friends were clearly supportive of her new relationship, and some of them had even begun to correspond with her new boyfriend themselves.
- Ultimately, however, Alice had decided not to pursue things—because she had also begun a concurrent email relationship with someone more local.

Having uncovered this information, Bob could potentially have used it to help improve his position in the ensuing divorce, but in the end he contented himself with mild amusement at the discovery. Nonetheless, if Alice had been aware of what was on the machine when she returned it, she would surely have deleted those files as well rather than risk the chance of Bob's finding them. The fact that she did not simply illustrates an aspect of security that is likely to affect all PC users, and which most will be similarly unaware of.

## When Admin Got It Backwards

The last two sections have presented examples in which those concerned did not realise they were letting go of systems with sensitive data onboard. As such, the ignorance aspect was in not recognising that protection was required. However, even when the need for security has been identified, there is still the potential for problems to occur if misassumptions are made, or the capability of the selected countermeasure is not properly understood.

Back in September 2001, I received an illustration of why you should take care not to become complacent when it comes to security countermeasures. One of my colleagues and I were on a way to a meeting, when we heard from one of our university system administrators that a new worm called Nimda had been released the previous evening and had hit the machines on the main university campus quite hard. We were not unduly concerned, however, because we ran auto-updating antivirus software on our machines, and we knew that a patch to detect and eradicate the worm had been released at midnight. Our machines performed their check for new updates at 4 a.m. every morning, so they would have got the patch already and be actively protecting our other group members from any problems. So far, so smug. It was not

until about an hour or so later, after our meeting had ended, that we realised that things had not gone as smoothly as we might have hoped. In spite of our antivirus regime, some of our key machines had become infected by the worm. How had this happened? Well, in simple terms, the Nimda infection elsewhere on the university campus had affected our machines' ability to protect themselves.

Once it infected a machine, the Nimda worm was highly active in its attempts to seek other targets and spread itself onto them as well. It did this by scanning other machines on the network, looking for exploitable vulnerabilities. The result of this was an explosion in the level of network traffic, as each newly infected machine began to scan other systems. In a short time, virtually all of the network traffic was Nimda-related, with the side effect that any legitimate network traffic was likely to get blocked. It was as a result of this network congestion that our research group's machines had failed to protect themselves—they had simply not been able to successfully connect to the antivirus site and obtain their updates when they tried at 4 a.m. Consequently, a number of them had become the victims of Nimda infection.

So, what did this mean for us, and what was the impact? One of the infected machines was the web server, hosting our research group's own site, the site for another group, a site advertising a forthcoming conference, and a number of staff member's personal sites where students were routinely directed to download course materials. As such, this was a system that was accessed on a continuous basis for one reason or another. To give an idea of the extent of the problem that the worm posed, the server in this instance was host to approximately 13,500 files, of which 1,398 had become infected. This was most definitely not good, especially as anyone who might have attempted to connect to any of the websites from another unpatched machine would instantly become infected by Nimda themselves.

The fact that our web server had become infected brought to light another unforeseen security failing. Disregarding the failure to obtain the antivirus update, this system should not have been vulnerable to Nimda in the first place, because the vulnerabilities that the worm exploited in order to infect a system should have already been addressed by our security administration activities. In order to protect against Nimda, administrators needed to apply a succession of security patches to the standard installation of Microsoft's Internet Information Server. These had been released individually over a period of weeks earlier in the year. However, to make life easier for administrators as the number of patches grew, Microsoft released a cumulative patch that claimed to apply all of the other fixes in one go. This was the version that we had applied to our web server. As it transpired, however, the full set of patches had not been applied as we expected (i.e., the effect of the cumulative patch was not the same as applying each of the individual patches separately). It can be observed at this point that punishing those administrators who had not taken steps to patch their systems properly was probably the rationale of the Nimda worm—astute readers may have already noticed that Nimda is the word 'admin' spelt backwards.

The result of the Nimda infection was significant. Our university was not able to fully restore network access until 14.00 the following day—representing almost 30 hours without network access for the majority of the campus. In terms of

disruption alone this was a significant impact. For instance, no one was able to send email or access the web during this period—two activities that have become routine and often essential elements of day-to-day operation, even in academia. Moreover, many systems had lost data as a result of Nimda's corruptive activities (luckily we did not have to count ourselves amongst these, as the antivirus software was ultimately able to clean up many aspects of the infections, and our daily backups provided the fallback for anything that was not recoverable at this stage). Indeed, some sources estimated the worldwide cost resulting from Nimda-related cleanup and lost productivity to be around \$635 million<sup>55</sup>.

So what does this incident illustrate? Well, the basic message is that you can never be 100% sure that you are secure. The research group was aware of the risks posed by malware and had installed auto-updating antivirus software to minimise our exposure. We were also aware of the problems posed by unpatched security vulnerabilities, and we had installed the vendor updates that were provided to close some of the gaps. Nonetheless, our systems were breached by a worm that exploited known vulnerabilities. Our situation was by no means unique. For example, of the organisations responding to the 2004 CSI/FBI Computer Crime and Security Survey, 99% claimed to have antivirus software on their systems. Nonetheless, as Chapter 1 has already highlighted, 78% of the respondents still claimed to have detected viruses on their systems in the previous 12 months, and virus-related losses totalled over \$55 million<sup>56</sup>. As Paul McNabb, the deputy director of the Center for Advanced Research in Information Security, put it:

It is nice to have antivirus software to prevent being a victim of the virus aftershocks, but neither antiviral software nor firewalls can completely protect a system. . . . There simply is no fail-safe protection.<sup>57</sup>

Returning to the specific case of the Nimda worm, there is an interesting footnote to the tale, which highlights a vulnerability of a different kind. Whereas the infection in my research group had resulted from a reliance on protection measures that did not work as we had expected, this incident was caused by a more blatant security oversight. At the centre of the incident was Microsoft—a name that has a tendency to crop up quite often in the context of security, and not always for the right reasons. This case certainly fell into the latter category, because about nine months after the original outbreak of Nimda, a news report revealed that Microsoft had unwittingly dispatched a copy of the worm within the Korean version of its Visual Studio .NET development software<sup>58</sup>. As a result, customers were installing a package on their systems that had a worm hidden within it. Luckily, the worm was buried within one of the help files, and so simply installing and running Visual Studio would not have caused machines to be instantly infected. In fact, because of the very specific circumstances that would have had to occur in order for the worm to be activated, Microsoft was correct in its assessment that risk of infection was “extremely low”<sup>59</sup>, and it acted quickly to contain the problem (customers were notified and an appropriate fix was issued). Nonetheless, the fact that it happened at all was still a fairly significant case of egg on the face for Microsoft, raising questions of how infected software could possibly find its way into a distributed release without being



trapped by internal antivirus checks. The source of the problem was apparently a third-party company that had performed the translation of the help files into Korean. However, the software would still have gone back to Microsoft before being shipped, and thus one would have expected that all files in the distribution would have been scanned for malware (indeed, good practice would also suggest that Microsoft should have checked the files before this stage and scanned them when they came back from the translation company). So yet again, the lesson is that if you trust something to be correct, but do not actually check to make sure, then there is a good chance of getting caught out when you least expect it.

## What Are the Users Up To?

Staying with the theme of trust and unchecked assumptions, let us look at a completely different example. In a company setting, it may be tempting to assume that the same views about security will permeate the whole organisation. For example, if a security policy has been established, the implicit expectation at management level will undoubtedly be that employees are abiding by it. In practice, however, there is often a significant disparity between the views of the organisation and the actions of its staff, and if they do not think about security, users can start to cause quite a few problems. This point can be illustrated by another example relating to malware.

The Nimda discussion has already shown that relying upon antivirus software can sometimes provide a false sense of security. However, you do not need a state-of-the-art worm to muck up your protection—errant staff can also do that quite effectively! The following incident, from another university environment, illustrates the point. The environment in question housed a mixture of individual and shared PCs, and one particular shared machine that had a variety of hardware resources that were not provided on staff stations (e.g., scanner, CD writer, etc.). Because the facilities on the machine were open to equal use by all users, the normal situation was for the system to be logged in under a generic account rather than requiring each person to log in and out individually between uses (and yes, this is already a classic example of convenience triumphing over security, with a scenario that removes any kind of individual accountability—don't worry, though, because they paid for the mistake later). The result was that 10 or so users were all accessing the system, and all using it at one time or another to scan documents, edit images, burn CDs, and so on. These activities involved opening and closing myriad applications, downloading data, and exchanging removable media—all of which continued quite merrily and flawlessly . . . until someone decided to close down the antivirus program!

Of course, nobody could tell who had closed it (the consequences of the dubious group access decision coming home to roost!), and in view of what happened next, nobody was about to own up to being the culprit. What could be determined, when the antivirus (AV) software was restarted, was that something nasty had found its way into the system in the interim. With the AV scanner off, and Internet downloads and media exchange continuing, it was perhaps not too surprising that a virus had

been introduced—maybe what was surprising was that it was *only* one! The virus in question was a program called Elkern, which had the rather troublesome habit of overwriting the contents of files with zeroes. This could cause major problems if essential system files were overwritten and could potentially prevent a machine from being able to restart the operating system once it had been infected. Luckily for the affected system, the results were not quite that drastic, but there were still over 450 infected files on the machine, which were continuing to infect other executable files on the hard drive. In addition, the Elkern virus was network-aware and was trying to spread to other machines on the local network. In these cases, however, it was thwarted by local copies of the AV software, which the users had thankfully not disabled (clearly, the protection of their own machines was given a somewhat higher priority than the shared resource!).

The point of all this is that, if the users had fully bought into the concept of security, then none of them would have contemplated shutting down the AV software in the first place. What the example illustrates is that there can often be a significant difference between what the management or IT administrators believe is happening with security, and what the users at ground level actually do (and understand) about the issue on a daily basis. And the issue is by no means restricted to the misuse of antivirus software—a point illustrated by some results from a small survey of corporate end users and system administrators, which aimed to assess their differing perspectives on security issues<sup>60</sup>. One of the most revealing questions asked the users whether they had signed up to a security policy to govern their use of the IT systems. Although 68% were able to recall this correctly, the remaining third were less impressive—20% did not remember that they had signed one, whereas 12% claimed to have signed up when their company did not have a policy in the first place! Another discrepancy was revealed in relation to viruses. Here, the responses from the system administrators had established that all of the users had antivirus software on their systems. However, this fact was clearly lost on some of the users, because 12% were unaware of it. Of course, such disparities are not helpful, especially when users remain unaware of security issues, or do not know what they ought to be doing about them. The likely consequences are that ignorance and misunderstanding will then prevent security from being realised to the extent the organisation desires. Some approaches for tackling these problems are considered in the next chapter, as part of the discussion of how an organisation can foster a security culture amongst its staff.

## Summary

This chapter has illustrated a number of ways in which security problems can come along and bite us if we are not fully aware of the technologies we are using, or the assets we should be protecting. Wireless LANs and mobile devices are both examples of technologies that have been embraced without consideration of security. They are by no means the only technologies that present risks, but they provide good illustrations of how ignorance can lead to our systems and data being exposed

unintentionally. However, the issue does not end with the incorporation of new technologies. Providing effective security also assumes that we know what we need to protect in the first place. The examples relating to disposal of systems have highlighted that people are often ignorant of what their computers actually contain, which can lead to them inadvertently allowing devices to leave their possession with unprotected sensitive data still intact. The final sections have shown that if security is used already, then we need to ensure it is doing what we expect of it. The example of Nimda infection, despite the presence of antivirus software, shows that if we do not appreciate the limitations of our security technologies, then we will not realise when we are still vulnerable. In addition, it is important to make sure that everyone who comes into contact with security appreciates its importance. Although the system administrator may appreciate the threats that are faced, and the consequent need for safeguards, this will often come to nothing if the end users have missed the message. If users do not know what they should be concerned about, they themselves become security risks and can undermine the security measures that are put in place (e.g., by shutting down antivirus software).

Although they are far from the only possibilities, the different scenarios serve to demonstrate the scope and variety of the problem that ignorance can pose. Unfortunately, there is no definitive list of the situations that we need to look out for, and therefore the only way to safeguard a system is to ensure that we know enough about it to understand where security issues are present (a means of achieving this would, of course, be to conduct a proper risk assessment, as already highlighted in Chapter 1). However, recognising and responding to our security requirements is not the end of the story. Even when needs have been identified, and measures have been put in place, there is still plenty of scope for them to be undermined. Some of the ways this can happen are the focus of the next chapter.



<http://www.springer.com/978-1-85233-943-2>

Computer Insecurity

Risking the System

Furnell, S.M.

2005, XIII, 240 p. 30 illus., Softcover

ISBN: 978-1-85233-943-2