

documents might feel secure from detection if the documents are not saved to disk. However, even if the printed documents are only held in memory without being saved it may still be possible to view the printed documents by searching for the special files, which are created by Windows during the printing process. These files, which have a .spl or .shd extension, contain a wealth of information about a print job such as the name of the file printed, the owner of the file, the printer used and the data to be printed (or a list of the temporary files containing such data). In a case reported recently a suspect, under investigation for sending threatening notes, was arrested after evidence of such a note printed from his machine was located even though the document had not been saved to the hard disk

## Summary

Although computer forensics may sometimes appear like magic, able to resurrect the remains of data once thought dead and buried, in truth even the most skilled investigator can only recover data which is still physically present on a system. As we have seen, it may be possible to reconstruct a user's activities after they have attempted to cover their tracks for two main reasons: firstly, deleting data usually only means that the data area on the disk is marked as available for overwriting but until that time is still physically present on the storage medium (even though it may no longer be accessible by the user through the operating system) and secondly, operating systems may create files without a user's knowledge which can then be used at a later date to highlight their actions.

Unfortunately for the investigator, both of these issues are widely known and software is readily available which enables the less savoury computer users to cover their tracks more effectively. Nevertheless, the pace of technological change and the complexity of modern software continue to present new opportunities for evidence gathering and as a result offer forensic investigators their best chance of staying one step ahead in this fascinating field.

### About the author

Rod Morris works for Forensic Technology at KPMG in The Netherlands (<http://www.kpmg.nl/forensic-technology>) and specialises in computer and network forensic investigations. He can be contacted via email at [morris.rod@kpmg.nl](mailto:morris.rod@kpmg.nl)

# Electronic Security is a Continuous Process

*Stephen Mason*

The use of email and the Internet has added a new conduit to market for business, and some organizations have gained significant commercial advantage from using the Internet. Before computers were connected to the Internet, it was relatively easy to have effective security measures in place to protect the electronic files on individual computers or systems. However, now computers have become communication systems as well as working tools, the risks attendant upon this new breed of 'communications working platform' have increased substantially.

However, the risks attendant upon the use of the Internet are both numerous and poorly understood by end users, as pointed out by Royal & Sun Alliance in their Broker Bulletin Issue 04A/02 dated March 2002. The use and knowledge of security procedures by end users is poor and those security products that are available on the market have not been widely adopted. The potential damage to the loss of data that a corrupting virus, for example, can cause, is so significant that the response by the same insurer is to

remove all cover for damage relating to such losses for business-related policies with effect from April 2002. This means that organizations will, when they renew their insurance policies, find they must reconsider the security arrangements in far more detail than they may have considered in the past.

In addition, boards of directors in private companies and senior management in public bodies have yet to fully understand the need to:

- Map out the risks.

- Reduce exposure to the risks.
- Implement suitable policies and training to all members of staff.

## The Information Security Breaches Survey

The Information Security Policy Group at the Department of Trade and Industry produce a bi-annual report relating to breaches of security, "Information Security Breaches Survey". The first Survey was published in April 2000, the second in 2002. These surveys reveal some pertinent findings:

In the 2000 Survey, 60% admitted they had suffered some form of security breach in the previous two years (the range of breaches included accidents, errors committed by users, acts of god such as flooding and natural disasters, and intentional acts that demonstrated malicious intent or some form of premeditation, such as unauthorized access and use of a system, fraud, theft and the introduction of a virus).

In the 2002 Survey, 44% of businesses suffered a security breach in the past year, although 78% of large businesses acknowledged they suffered a breach.

It used to be considered that the main security threat is from people working inside the business. However, the 2002 Survey indicates that 34% of businesses reported that an employee caused their worst security breach, whilst others caused 66%. These figures are in line with the CBI Cybercrime Survey 2001 and 2001 CSI/FBI Computer Crime and Security Survey.

The number of breaches that were the result of premeditated or malicious intent increased from 24% in 2000 to 44% in the 2002 Survey.

Infection by viruses remains the predominant cause of a security incident, with incidents increasing from 16% in 2000 to 41% in the 2002 Survey.

## The cost

The costs of attacks will vary, depending on the size and nature of the organization. The cost of an attack to an individual may be small in monetary value, but crippling if their computer cannot be used and data is lost for any length of time. Whilst most costs related to breaches of electronic security are minor (two-thirds of the most serious security incidents cost £10 000 or less to resolve), 4% of businesses reported costs of more than £500 000 following a single incident. (An investment bank commented about the problems caused by their security breaches. Whilst they did not suffer direct financial loss, they experienced the loss of data, wasted staff time, opportunity cost, remedial action and downtime, and, after major virus problems, giving IT staff time off work to recover from the stress they suffered.)

## Applying appropriate security standards

Of the organizations interviewed for the 2000 Survey, only 25% were aware of the existence of the British Standard (BS 7799) on Information Security Management (now adopted as an international standard as ISO 17799). In addition, awareness of c:cure, the accredited

certification scheme for BS 7799 was very low. In the 2002 Survey, the focus was on whether organizations were aware of the content of BS 7799, rather than the awareness of the standard (as was asked in 2000). Only 15% of those interviewed were aware of the content of BS 7799, although this percentage rose to 42% in large organizations.

## Data protection

The reader will be aware of the existence of the UK Data Protection Act 1998. A number of risks accompany connection of the computer and system to the Internet. Protection of personal data is ubiquitous, but this includes, by way of example only: the security of emails sent and received through the system, and the provisions in place to offer protection where the system is connected to the website, causing the organization to have an interface between the operation of the website and the data held in the system. For example, in 2000, PowerGen had to advise 7 000 online customers to change their bank card numbers when it was discovered that people visiting the website could obtain access to their name, address and bank card details. PowerGen also paid each customer £50 each in compensation for the inconvenience.

Failure to protect personal data could demonstrate negligence, as well as a breach of the Data Protection Act.

## External threats

The range of external threats must be considered carefully. The degree of risk must be considered against the cost of implementing a solution. The types of threat include:

- The activities of hackers, who seek to obtain access to systems and networks.
- Attacks on websites, including the use of clone or mirror websites to trawl for intelligence, appropriating content from the website, and attacks on the image or brand by defacing the website.
- Denial-of-service attacks, where a Web server is flooded with useless information

to prevent legitimate traffic getting to its destination, the types of attack include bandwidth consumption and resource starvation.

- Virus attacks where a virus runs on the system without permission, including terminate and stay resident file viruses, parasitic viruses, overriding viruses, stealth viruses and polymorphic viruses (this list is not exhaustive).
- The use of worms that can systematically eat through and destroy stored files before moving on by sending a copy of itself to other machines to replicate the process.
- The introduction of malware such as a Trojan horse, that permits a remote user to take control of it over the Internet to download files, change system configurations to permit easier access when entering on later occasions, see what is on a user's screen, reboot the computer and capture passwords.
- The monitoring of the network, called a sniffing attack, that involves deploying a piece of code on the network that monitors all traffic, looking for passwords and other information.

## What should be done?

The extent of time and energy set aside to assess the organization's exposure will depend on a number of factors, including size, any in-house expertise, and what security policies and procedures, if any, that already may be in place. The following discussion is meant to guide the reader through some of the issues that should be considered.

## Identify the assets to be protected

Assess where the computer or system is vulnerable and establish the range of threats that may attack or exploit these vulnerabilities. It may be necessary to seek specialist advice for this part of the exercise. Determine the degree of risk and set out what liabilities may be incurred in failing to protect the organization's assets. In carrying out this assessment, it is

appropriate to establish how the computer or system is used; how many people are connected to the system; the types of facility individuals are entitled to use when on the system (for instance, some people are only granted email facilities, whilst others will be able to obtain access to the Internet); what connections exist to the Internet and what, if any, products there are in place to protect the system from both internal and external threats.

This assessment may take five minutes for some, but will take longer for those with big systems that interconnect across time and space. It is important to establish the full technical construction of a system, because the architecture could be such that additional products, such as a firewall, may, as the result of the way it is configured, cause the system to be vulnerable to outside attack.

## Put protective measures in place

Select and implement appropriate security controls to reduce the risk of exposure. Security controls should cover such discrete areas as the people using the system, the need for physical security and the security of the system or computer. In seeking to demonstrate the organization carried out its duty of care, it is recommended that consideration be given to complying with relevant codes of practice and security standards such as BS 7799 or ISO 17799.

## Policies and procedures

Develop and implement suitable policies and procedures. A core component is the education of all members of staff, because everybody using the system should be aware of the security issues in just the same way that they know that leaving their car unlocked invites the possibility of the contents being stolen. Also, people in senior positions must be seen to adhere to the security policy in the same way as any other member of staff.

A common problem relates to the use of passwords. Cracking a password can be easy when common examples include

'password', 'secret', and even the names of football teams. In addition, writing the password down tends to defeat the reason for having a password. Hackers also have software tools that try every alphanumeric combination of user name and password at high speed, which highlights the need to ensure passwords are changed regularly and comprise a random combination of numbers and letters. Finally, monitor, review and update the effectiveness of the policy regularly.

## Technical solutions

Consider what technical solutions there are on the market to protect the system. There is a balance to be struck between the cost of reducing the risk against the consequences that follow if the organization fails to implement appropriate measures to protect the system. Weigh up the use of encryption to protect sensitive data, but beware of the practical issues, such as the problems that may occur in complying with a s49 notice under the Regulation of Investigatory Powers Act 2000, the storing of key numbers, the inappropriate use of private keys by employees, the improper use of encryption by employees where inappropriate content is hidden in files that are encrypted, and how to determine where on the system viruses should be checked, both inbound and outbound. It is not advisable to use encryption in isolation. Failure to close the electronic doors to hackers will render ineffective whatever expensive encryption solution is purchased.

Most IT directors will probably have reconfigured the system at some time. The aim is to change the configuration set by the manufacturer. To further provide for the maintenance of the system's security, the latest fixes should always be patched, a regular review of computer and network security configuration should be conducted, and appropriate restrictions on access to data and network resources by employees should be in place. The existing software should be properly maintained. If more software is added or changes are made, the organization opens itself up to creating more

security loopholes. As a result, additions and changes to the software should be controlled and documented to reduce the risk of introducing new bugs that open backdoors to the network.

Other products that are available on the market that help to reduce exposure and increase the security of the computer or system include access, authentication and authorization software, firewalls and intrusion detection systems. If these products are used, it is crucial to ensure they work, are secure and are configured into the system correctly, otherwise the organization may be creating another opening for an enterprising hacker at some stage in the future.

## Security in context

Many of us understand security in the physical sense, such as the provision of locks and physical barriers such as safes, or preventative measures such as security guards and burglar alarms that are designed to alert the owner of a property to an attack in progress. Whilst physical threats exist in the electronic world (computers are prone to being stolen and can be damaged when the power supply is suddenly interrupted), the most dangerous threats are those that are intangible and cannot be seen by most end users.

Static security measures do not work after we have connected our computer or system to the Internet. We all now need to think of security as a continuous process. The budget must include a figure for electronic security each year. Practices and procedures must be continually updated. Keeping members of staff educated is a crucial component to the successful implementation of the security ethos.

To defend an action in negligence, the organization will need to show it made itself aware of the issues and that suitable precautions were taken to fulfil the duty of care. It is not a question of whether electronic files will ever be compromised, but the effectiveness of the security in place when they are compromised.

*stephenmason@  
pariocommunications.co.uk*