Shred of evidence

Vulnerability of the information asset is crucial for all blue chip organisations. Many companies are well versed in protecting their PC-based sensitive information, but how many security managers out there are really getting to grips with safeguarding vital paper-based documentation? John Julian proffers a beginners' guide for in-house professionals.

Information security is a constant and growing concern not only for government and businesses but also for individuals. To date safeguarding information has primarily been IT driven with the emphasis on protecting electronically generated or stored information.
This is somewhat understandable in the light of the level of publicity that worm and virus attacks receive, particularly when they manage to paralyse whole sectors and even, at times, countries.
The whole topic of information security is also emphasised by current legislation and Codes of Practice whereby, for example, EN 17779 (BS 7779) dictates an information management requirement that focuses entirely on data security.

Whatever happened, though, to the threats posed to information security that existed before we all turned on our computers? Have all of the old commercial spies retired? Has bin searching – otherwise known as 'dumpster diving' to some –ceased to occur?
Have we finally reached the stage of the paper-less business environment, at least as far as sensitive information is concerned?
Nowadays, we hear of rare cases where a bundle of files is found on a tip, or where allegations are made that Court case-related documents were found in a skip, but generally speaking the 'gurus' seem to be silent on risks posed to hard copy information – be it in the form of paper, microfilm, or photograph, etc.
Of course we still live and work in a paper-intensive environment, with computer printouts adding to the many other documents that are still produced. Unfortunately, while the majority of businesses and organisations are now alert to the consequences of hacking, their attitude – or rather the employees' attitudes towards basic information (document) security hasn't improved.
So are documents still a target for industrial espionage? Can their compromise bring harm to the company? The answers are fairly obvious but, to bring the need for document security into focus, there are several factors to consider.

PRIOR KNOWLEDGE IS POWER

Early information on activities that affect share prices allows opportunities for profitable share trading, or 'dumping' before values drop. That early information could include snippets of news on planned acquisitions, major contract news, company results (either quarterly or year end, for example), new product launches, changes in marketing strategy and moves by key individuals.

Prior knowledge of contract budget information or leakage of other tender values could give an advantage to those bidding for the contract. Similarly, advance knowledge of poor company performance or planned redundancies could lead to crippling action being taken against a company by it's employees or shareholders. Equally information that shows the company in a bad light can be used to damage image, reputation or credibility. This will allow a competitor to gain market advantage or an individual to exact revenge against real or perceived grievances.
In the latter case the information may equally be used to target an individual rather than an organisation, although the two often happen together.

Thus far the Data Protection Act 1998 has proven to be the best 'tool' that has appeared in the fight for the protection of information in that, at last, there are penalties that can be applied against persons who fail to protect information. Although this is only applicable to 'personal information' it has started to make managers and information custodians take notice and apply some protective steps. Alas it will probably require a high profile Court case and a stiff sentence before it becomes universally applied.
At the present time, many of the staff we encounter 'have heard of the Act' but do not really believe it applies to them and whilst they protect their data (in the network) paper is handled no differently to the past.
Many organisations and businesses have, of course, enforced the Act with the seriousness it merits, and have implemented sound personal information policies and practices to the degree where both data and hard copy information is both protected and safely handled.
In a small percentage of these organisations the policy and handling requirements are also extended to sensitive information that is not 'personal', i.e. company sensitive information, but from our direct experience these are in a minority.
One should condition that statement; there are many managers and individuals in these organisation/businesses that are really trying to get sensitive information policy and procedures to work, but with mixed levels of success. (One of course excludes, in this area, the government and defence organisations where classified document handling has been established and regulated for many, many years)
Regrettably many organisations and businesses continue to face enormous vulnerability with the potential for serious compromise and the subsequent consequences. Is this caused by lack of awareness of the threat, apathy, a false sense of security, or a resistance to change? It's driven by a combination of all these possibilities.

THE COMPROMISE OF INFORMATION

In many cases, Boards of Directors consider that they have security in place in that their buildings are controlled against unauthorised entry, staff are vetted, separate bins are provided for sensitive material and they have contracts in place with 'confidential waste disposal organisations'. Do the security team members in such an organisation really need to do any more? Does this level of security afford sufficient protection to information?

Ian Johnson Associates Limited - Linden place - Seale - Farnham - Surrey - GU10 1HS.
T: (+44) (0)1252 782664 **F:** (+44) (0)1252 782818. **E:** info@ija.co.uk **W:** www.ija.co.uk

Continued from page 1

The compromise of information, even theft or deliberate espionage, is more likely to be by someone who is legitimately inside the premises so where access control helps keep out the external or 'freelance' spy, any internal lack of control by a document 'owner' still leaves vulnerabilities.
n this day and age many organisations have outsourced some or all of the non-core functions and thus the selection and vetting of staff is now beyond their control.
Whilst the service providers ('partners') may present pledges or even written statements of selection/vetting, their standards may be well below those that that your own organisation would apply. This is of particular concern in the services that suffer from high staff turnover. Combine this with staff attitudes where they view most long-term contract or agency staff in the same way as other employees (once they have been on site for a few weeks or more), the potential vulnerability increases.

Often such individuals are in the type of employment where we abandon our premises to them on a daily basis, leaving contract cleaning, maintenance and catering personnel under the watchful eyes of our contracted security force; with not a company employee in sight! Think of the penetration of one of the major telephone companies by a reporter using the agency staff route; reporters airside after joining cleaning companies or security firms; the potential for planned penetration becomes only too apparent.
Add to this possible financial motivation that may attract low paid staff, and the possibility of specifically targeted espionage assumes an even higher significance.

CAN WE LEARN FROM CASE HISTORIES?

Unfortunately there is a dearth of 'public knowledge' case histories that would allow us to demonstrate this vulnerability to senior management. In most instances the knowledge of such an incident will be kept 'in-house' to reduce its impact. The internal 'spy' can be defeated by good internal document security controls but these require the management and employees of the company to 'buy in' to the programme. If the 'spy' cannot access the document than no compromise can occur.
To achieve such a condition a number of measures need to be in place. Firstly it needs to be appreciated by all that protecting sensitive information is a positive action that requires effort and resources. It would be nice to be able to class all information as 'sensitive' and apply all of the protective measures to all of it, but the reality is that too much time would be required, even in just tracking each document through its life-cycle. Ultimately, there's a definite need to define what is truly sensitive to the organisation, restricting this to a manageable minimum. It's suggested that the criteria for sensitivity should be against the degree of damage that any compromise or inadvertent disclosure would cause.

Ultimately, it's likely that only three categories of sensitivity would emerge:
Company Secret: where compromise would seriously affect the ability of the business to continue operating (whether through financial impact or loss of reputation);

Company Confidential: where compromise would cause serious financial losses (in the context of the business, this figure would vary depending upon the value and / or assets of the business as a whole);

Personal in Confidence: all information that relates to personnel and is subject to the Data Protection Act.

Obviously information protected by existing legislation, e.g. patent, copyright, etc would have some protection (or at least deterrent against compromise) but other documents would then fall under the protection afforded to 'proprietary' information. Much would be considered to require no protection beyond being retained in the building or to be adequately disposed of.
Once the grading has been accepted, on the basis of content, then effective controls of sensitive information become less time consuming and have a chance of actually being applied. Such information needs to be marked with its sensitivity grading throughout its life-cycle from first draft to final copy and then be subject to recorded and auditable (tracked) distribution to only those with the business 'Need to Know'.
The right of access to information by rank needs to be controlled. If certain members of staff aren't involved, they don't need to know.

'NEED TO HOLD' AS A PRINCIPLE

A 'Need to Hold' principle has to be applied both to keep volumes to manageable levels and to ensure that such information is only held where it can be protected; if a person only needs sight then they do not get their own copy, they view and sign-off on a central copy.
When a document is no longer needed it is destroyed; destruction by an approved security method and recorded so that 'lost' documents can be highlighted. For effective control, documents should be returned to the originator for destruction.
The method of destruction also needs to be addressed. We often find high profile organisations relying on shredders that that cut documents into full-length 0.5cm strips; presenting a not too difficult task of re-assembly.
The principle of shredding sensitive material within a secure handling area is sound but shredding should be cross cut and of no more than 0.2cm in width. Even then, the shredded material should be treated as sensitive until it's totally destroyed for good.

The latter is, and can safely be, contracted out to specialist companies but these should never be taken at face value. Even where such a company is BSIA listed as an ID (information destruction) company, their facilities and operation should be subject to full assessment. It is only in this way that you will gain assurance that the certificate of destruction they give you is a real record of what happened to your information.
The audit, both pre-contract and periodically during thereafter, should include the logging and tracking of your waste bags/containers, transport, unloading, storage, sorting, final destruction. It is essential that your material is stored and handled under secure conditions at all times until destroyed and that a full audit trail of every bag is maintained. We still come across cases where 'classified waste' is recorded as a bulk collection from sites and not even the number of bags is recorded.
Whilst all of the ID companies are considered to be adequate under the DPA requirements, it is strongly recommended that 'raw' company secret or confidential material is rendered unreadable before leaving your premises. In most cases the recommendation is that you employ a cross-cut shredder.

LOCATION, LOCATION, LOCATION

All of the locations where sensitive information is handled need to be provided with adequate privacy and security; as we are required by the DPA to prevent oversight of personal information on screen we also need to prevent access to sensitive information.

Page 2

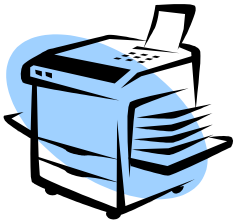
Continued from Page 2

Thus we need to ensure that persons receiving and holding sensitive documents are afforded privacy and also have the physical storage away from prying eyes when the holder is not present.

For example, contractors repairing PCs might have sight of neighbouring office workers PC. How do you avoid them having sight of a personal document whilst it's being worked on? What about when all of the staff go for lunch or a team meeting, does everybody ensure that all data is secured beforehand and that access to that area will be controlled in their absence? Sometimes the security policies you would like to implement might not be so practical.

If a document is left exposed it is less likely to be taken as this would be noticed and allow mitigating action; it will be read or, more likely, be copied. The ability to copy documents must therefore be brought under control. Photocopiers pose particular risks and even if PIN operated will not stop an authorised user making copies.

Many networked copiers/printers also retain the last document or documents produced, allowing a print to be made after the official copies have been printed. Some organisations with more rigid procedures have implemented a policy whereby a clear screen is 'printed' after the run, thus over writing the last document. For most companies, this would be too costly and impractical a policy, and it would depend on the cache facilities of the printers in question as to how beneficial it would actually be.



In house security managers must also remember that fax machines can both transmit a copy offsite (not too much of an issue if they print transmission information on the originals) but also can be used as photocopiers. If these are located anywhere near sensitive information handling areas they need to be secure with power and, preferably, PIN controls.

STAFF COMPLIANCE IS VITAL

Unfortunately, even where management support results in mandatory sensitive document procedures, the nature of staff is such that there will always be those who do not comply. Your security system therefore needs to include the means to detect violations and educate transgressors.

This really means physically checking that material is not left exposed or vulnerable and highlighting transgressors for management action.

You'll find that the inspection process can be greatly eased by operating a clear desk policy but this has different meanings to different firms.

In some it means that, literally, all desks are fully cleared when the 'owner' is out of office (including during meetings, lunch and breaks as well as outside normal working hours). This is perhaps the ideal situation as a glance is sufficient to confirm that nothing sensitive has been left exposed. Each person will, of course, need to be provided with sufficient lockable, secure storage to hold all of his or her material.

In more cases we find that 'clear desk' means that staff are required to only lock away sensitive material and thus work areas tend to include desks bearing massive piles of 'unclassified' documents, magazines/journals, computer print outs and so on. It is then no easy task to determine that there's no sensitive information either buried in the piles or, as is also common, sitting in/on a desk but bearing no sensitivity marking. Ever heard the cry 'everybody knows that everything I write is secret'?

INFORMATION VULNERABILITY AUDITS

We conduct Information Vulnerability Audits for a number of clients as part of their overall programmes of information and communications security and whilst some programmes are effective and well supported other audits continually discover highly sensitive documents left in full view.

The 'successful' clear desks programmes are almost invariably those that contain some form of censure/penalty for transgression – again an area requiring serious board level support. Thus it is not just a question of writing a policy it is also a question of enforcement. Enforcement means that you need to have a management support process of checking/auditing together with a 'penalty' system.

Various organisations use different methods. A few have included compliance with security requirements in the terms and conditions of their employment contracts, and reflect staff performance in their appraisals. Others use the embarrassment factor of 'naming and shaming' individuals or departments.

In some cases, where sufficient resources are available, the items have been confiscated and have to be collected from security staff or other centralised point. Care is needed with a confiscation programme as if there is no report or penalty and no management involvement, many employees will start to use the system as an effortless desk clearing service. If you do confiscate, then make sure you have the offender's manager waste precious time in collecting the items.

Whichever method is deployed – you should make good use of the embarrassment factor to promote the policy, as publishing the finds and penalties 'encourages' other employees not to transgress. Personal embarrassment should be avoided at all costs and I have found that publishing violations by cases per department is normally sufficient.

If you are worried about any of the issues discussed in this paper or would like further advice on introducing information security controls into your working environment and would like to speak to an advisor, call our consultants on 01252 782664 or alternatively email: info@ija.co.uk

This article appeared in the November 2003 edition of Security Management Today.

Ian Johnson Associates Limited - Linden place - Seale - Farnham - Surrey - GU10 1HS.
T: (+44) (0)1252 782664 **F:** (+44) (0)1252 782818. **E:** info@ija.co.uk **W:** www.ija.co.uk