Security and the Digital Domain

James Currall

Introduction – what is security about?

Security does not sound a very exciting topic for this book, which is showing you new and challenging ways to view your business and how you conduct it. Security means many different things in different contexts. Most of the time, what it is about is protection of people or objects. In our context, security is about protection of information. Two questions arise from the notion of protection of information:

- Why is protection necessary?

and

- What are we protecting it from?

The first question concerns the fact that information has value. If it did not, there would be little point in keeping it. That value is not always value in a strictly financial sense, although the cost of recovering or recreating information may be a significant issue. Archivists have traditionally defined four main types of record value, namely: administrative/informational, legal/evidential, compliance/regulatory and historical. Security is about protecting these as much as anything else. Additionally, a great deal of information is about people, and in many cultures and circumstances people have a right to expect that at least some of the information about them is treated as confidential. Confidentiality implies protection.

The second question concerns the fact that there are threats to information, an aspect that we will return to at intervals in this chapter. If one is to protect something, one has to identify what the threats are, so as to take appropriate steps to mitigate them. This chapter is essentially about what the threats are and the steps that can be taken in relation to them. If you have been an archivist or records manager for some time, you will probably have a fairly shrewd idea as to how to deal with many of these issues in a world of physical manifestations of information (books, manuscripts, ledgers, minute books, maps, plans and such like). You may be rather less clear how to deal with these matters in a world of digital manifestations (bits, bytes, computer files, databases and networks). One of the tasks of this chapter is to make the connections between the two worlds, so that you can use and build upon what you already know as the balance of your work moves from physical towards digital, as it probably will.

Security – the what and the who

It is convenient to split the varied aspects of information security into two groups: those concerned with ensuring that the information itself remains undamaged and genuine and those concerned with ensuring that those who can access the information have a right to do so. In concept, these matters are no different in the world of digital representation from what they are in the world of physical representation. The differences are differences of degree, how they manifest themselves and how those responsible for managing information assets can minimise the threats to their security.

What – ensuring that it is the Right Stuff

There are three areas of information management in which security plays a role, ensuring that the actual information that you manage is safe and secure: authenticity, integrity and availability. Digital assets are not directly perceived by human senses; they can only be viewed and manipulated rather indirectly through complex processes that cannot be fully understood by the end user. A great deal is taken on trust in our interactions with computers, and the possibility of fraud and duplicity is always with us. In addition, the concept of an original is problematic in the digital world, where copies can be identical to each other in all respects and the process of simply viewing a digital object may make several copies along the way.

In the digital world, it is every bit as important as in the paper world that we know that the information we manage is authentic, that its integrity is guaranteed and that people can gain access to it when they need to. This presents considerable challenges to the archivist and records manager who will have to learn new skills and cultivate new partnerships to deal with them.

Who – ensuring that it is the Right Person

There are two elements to information access control or ensuring that the right people have access to the right thing. The first is identifying who the person wishing to access information is and the second is whether or not they should have access to the information resource. The first is termed authentication and the second authorisation. In digital information security this distinction is very important.

IT personnel have long realised that access to computers, rooms and information should be based on individuals, but what has taken rather longer to acknowledge is that we have access to information as a result of roles that we occupy rather than directly as a result of who we are as individuals.

- Lecturer or Teacher, Student or Pupil, Employee, Parent, Member of Parliament, etc.
- Resident of X, Member of Club Y or Society Z.

A single individual may have many intersecting roles and what information they have access to is the sum of what each role entitles them to. A separation of authentication from authorisation makes it much easier to model and manage the linkages between people and information resources.

Some aspects of ensuring that only the right people have access to information are common to both paper and digital worlds. Physical security falls into this category. Information may be made available to selected people by keeping doors, filing cabinets and drawers locked and not leaving information lying around where anyone passing by can see it.

In some situations security is assumed in the digital world because of mistaken beliefs or understanding of the situation. An example is that many people assume e-mail to be secure because they send it off and it usually reaches the person they sent it to and they are unaware of anyone else seeing it. In fact, e-mail is sent across the Internet as ‘plain text’, that is as a sequence of characters that could be read by anyone along the way. Information on the Internet is put into the system and bounces its way from place to place until it arrives at its destination. If I set up a suitable monitoring program, I can watch very large amounts of information go past that are not destined for me. E-mail is thus similar in many ways to putting a postcard in the mail; it can be read by many people as it makes its way from you to me. There are techniques that can be used to put e-mail into the digital equivalent of ‘sealed envelopes’, but this strong encryption is rarely used and confidential reports and references fly around the Internet unprotected. People have started to understand that a floppy disc or CD, whilst needing a computer to reveal its secrets, will yield them to anyone who gets hold of it.

Although obvious if you think about it, paper manifestations of information are only available to people who are present in the same place at the same time. This is not true of digital manifestations on

computers that are attached to networks. Computers and networks make information potentially available to everyone, everywhere, all the time. This opens up the number of people who might gain access to your information (whether or not you want them to). Much of computer security is about trying to make sure that people around the globe do not obtain unauthorised access. In recent years this has become increasingly difficult. If you really do not want unauthorised people to access your information, do not connect the computers containing it to a network. Instead, transfer information to and from them using removable media such as tapes, floppy discs, memory sticks and CDs.

The Nature of Threat

Traditionally, records managers and archivists know a lot about the threats to physical manifestations of information. In many ways the types of threat are the same in the digital and physical worlds and any of the following can happen to both physical and digital manifestations. The main differences are: how likely each of them is, where the threat comes from and how it may be reduced.

Getting into the Wrong Hands – confidentiality When information gets into the hands of people who have no right to have it, this can have serious consequences, with the possibility of your organisation being sued or facing charges under privacy or data protection legislation and, even if the consequences are less serious, embarrassment or loss of commercial advantage may result.

Being Damaged – integrity Damage, whether accidental or deliberate, is potentially serious. It may be costly to put right, may be undetected until it is too late and may lead to further security problems.

Becoming Out-of-date – integrity/relevance Information that is out-of-date may be misleading, resulting in extra work or other unnecessary cost, and may be damaging to the organisation, its workforce, customers or reputation. After all, who can have confidence in an organisation that does not manage its information resources?

Being Unavailable or Irretrievably Lost – availability The unavailability of information will almost certainly reduce efficiency of operation and affect the quality of decision-making. More importantly, it may result in damage or lead to a loss of reputation.

Not being what it says it is – authenticity Clearly, if information is to be useful, those making use of it must be able to have confidence that it is what it purports to be.

Information Security Management is concerned with the preservation of confidentiality, integrity, availability, relevance and authenticity. The objectives are to ensure that: information is accessible only to those authorised to have access to it; the accuracy and completeness of information and processing methods are safeguarded; authorised users have access to information and associated assets when required; people are seeing the correct version; and the information object is what it appears to be.

Information is particularly vulnerable during:

- Creation – poor practice in naming, capture of appropriate metadata and ‘filing’.
- Storage – failure to ensure that information is not overwritten, is adequately backed up, etc. and protection from on-site and off-site attackers.
- Access – ensuring that the appropriate people have access to the information to view and to alter it.
- Transport – information is particularly vulnerable when it is beyond the confines of the organisation.

Additional risk arises through keeping information for too long. There need to be suitable processes for proper destruction. In the digital world getting rid of information can be a very difficult thing to do.

Technical Threats

Information security is not all about technical threats. In fact, security is not a technical issue, but use of technology can represent a threat to information security and technologies are often required to implement security solutions. In this section we are going to put the technical threats under the microscope because it is an area with which many archives and records management professionals are uncomfortable. It has probably not been included as part of their training and the landscape changes with each passing day.

The Information Architecture

The information architecture of most organisations has a number of elements.

First, there is the 'personal' machine on your desk that provides your primary instrument of access to digital information. This machine is at least partly managed by you – you have responsibility for many aspects of how it operates, although in many organisations other aspects are managed by technical support staff. Unlike a standard office telephone, which operates in a set way as it was manufactured to do, your computer will operate as the programs that are loaded on to it tell it to. This means that, if a program is loaded on to your machine (in addition to those that are normally there) that instructs it to send copies of every keystroke that you type to my computer in Glasgow, that is exactly what it will do. For this reason you need to take the management of your computer very seriously. Remember that, if you are authorised to access and manage certain information, then to all intents and purposes so is your computer (whether or not you told it to and whether or not you are actually present). Poor use of individual computers has the potential to compromise the whole of your digital record-keeping or archiving systems.

The second element is the array of servers that provide you with a variety of services: printing, web interfaces, filestore, electronic document and/or records system (EDMS/EDRMS), backups and so on. These machines are generally managed by specialists who know what they are doing, but cannot be guaranteed to know what you think they are doing or want them to do. These people will ensure that these machines are well managed to minimise the threats that they know about and wish to control. You cannot assume that this includes all the threats that are important to you. An example might serve to illustrate the difference in perspective. Most servers have some arrangements in place for backup. Suppose you accidentally delete a digital object on the file server that you use. You might naturally assume that those running the server can simply go to the backup and retrieve the object for you. This may not be the case. Those managing the server are making backups to deal with one major eventuality – disc failure. If a disc fails, what they want to do is to get a new one and recreate the filestore exactly as it was before. It is often easier for backup systems that have this objective to store material in such a way that the only restoration possible is to recreate a new disc by overwriting everything, rather than by finding and restoring every object individually. The result would be that they would be unable to satisfy you requirement without buying an additional disc, restoring the whole backup on to it and then looking for your object to copy to your storage space on the old disc. They are unlikely to wish to do this unless someone's life depends on it. Some threats are related to how these servers are managed.

The third element is the network that connects the computers in your organisation. Again this is likely to be managed by professionals, but remember that its purpose is to make it as easy as possible for information to get from one machine to another (although there will be some controls). The network frequently cannot distinguish between information that should be travelling from machine to machine

and that which should not. A rogue program that gets on to your machine might easily be able to travel to everyone else's. Some of the threats to information security lie on machines (and with people using them) attached to your organisation's network.

The fourth element is the connection of your organisation's network to the global network or Internet. In many ways this is the Wild West, where the Law of the Jungle applies (to mix metaphors). It is likely that there will be some sort of gateway between the two, but, in order to allow useful information in, the controls are unlikely to be draconian. The rest of the computing world is attached to the Internet and that is where many of the threats that we are discussing lie or originate.

Threats to confidentiality

From a technical perspective, the key to confidentiality is access control mechanisms. In a sense this is no different from the paper world where you lock confidential papers away in filing cabinets and drawers and behind locked office and building doors. You allow people past these controls using keys and, increasingly, swipe cards and other tokens. The major threats to digital information result from having inadequate access control mechanisms and through people being able to bypass the access control mechanisms as a consequence of security compromise elsewhere in the system. You need to be concerned with the design of access control at a logical level, cooperating with systems designers and support staff. You need also to be concerned with access control at an operational level, cooperating with the systems support staff to ensure that they manage system security appropriately.

Technical measures that are required to counter these threats to confidentiality are: secure systems, secure authentication methods, and an authorisation process and system that matches your needs.

Failure to destroy completely information that is no longer required or relevant is another important threat to confidentiality. Typically information resides in: local copies on individuals' machines or on shared file servers, backup copies of individual and shared filestore, copies in the filestore of other people (both within and outside the organisation) to whom the information has been distributed, and finally in the backup systems of these other people. Little wonder that it is very difficult to actually destroy *all copies* of a digital object. To make matters worse, when you delete a digital object on your computer, it is not actually removed. What happens is that the directory entry for the item is removed. One of the functions of this entry is to point to where it can be found on the disc. There are easily obtainable tools that can restore deleted digital objects. The main determinant of success is how much disc activity has taken place between deletion and the attempt at restoration.

The measures needed to deal with this threat to confidentiality are really organisational rather than technical: clear distribution policies, clear destruction policies, single sources rather than copies that have to be updated individually, shared originals on file servers rather than individual copies in personal space, carefully worked-out destruction processes and a shared understanding between archivist, records managers and technologists about types of backup and the needs of record keeping and destruction

Threats to integrity

The threats under this heading are those that affect computer systems generally, causing widespread disruption rather than being targeted at a specific piece of information. As computer applications have become more sophisticated and the users have become more demanding in relation to seamless integration of one type of activity with another, so it has become easier to embed instructions within e-mail messages, documents, spreadsheets, etc. This class of threat seeks to execute code using mechanisms that under normal circumstances are intended to support this ease of use. In general, the objective is to allow unauthorised activity or access to computer systems rather than to specific digital objects. A general heading for the software that constitutes this type of threat is Malware. Malware can be classified on the basis of how it is executed, how the code is distributed, and/or what it does:

Viruses Self-replicating programs that spread by inserting copies of themselves into other programs or documents, they are frequently distributed via e-mail or other standard person-to-person communication mechanisms. The infection routine of the virus arranges that, when the host program is run or the document opened, the viral code is run as well. Normally, the host program or document operates as normal after infection by the virus. Some viruses overwrite other programs with copies of themselves, which destroys them altogether.

Worms Similar to viruses but they are stand-alone programs and thus do not require host documents to spread themselves. They usually modify the operating system of their host machine, so that they are started as part of the startup process. To spread, worms either exploit some vulnerability of the host operating system or use some kind of bogus incentive to trick users into running them.

Trojans Named after the classical Wooden Horse of Troy, these programs present themselves as an appealing prospect such as a screen saver, greetings card or useful free program. Whilst they may do what they claim, they also carry out other tasks, which may result in third parties being able to take control of your computer at will (including having access to all your digital objects), or use your filestore for the distribution of copyright or illegal material. Trojan horses cannot replicate themselves, in contrast to viruses or worms. To complicate matters, some trojan horses can spread or activate other types of Malware, such as viruses.

Viruses and Worms often act as carriers for other types of Malware, such as:

Spyware Collects and sends information about your browsing behaviour to other parties without your knowledge.

Keyloggers Copy the sequence of keystrokes that you make when using your computer into a computer file. This file may then be inspected directly by a hacker or e-mailed to another party without your knowledge. Keyloggers are primarily used to collect credit card details and passwords, which are then used by unauthorised people.

Backdoors Are pieces of software that allow access to your computer system, bypassing the normal authentication procedures.

Innocent documents from people that you know may contain malicious code put there by any of the mechanisms. If your record system contains documents ‘infected’ in this way, opening them could destroy the record system or at the very least spread the ‘infection’ or other malady to the computers of anyone accessing it.

Technical measures are needed to deal with these threats: effective, up-to-date virus detection software (new viruses appear on a daily basis), up-to-date operating system and applications software patches to deal with security loopholes that are discovered from time to time and may be exploited by the above mechanisms, and regular checking of the integrity of computers, software and user files.

This is the area where individual users need to recognise that they have a role. The mechanisms used to distribute malicious code often make use of ‘social engineering’ – spurious incentives to download or open a digital object – and also make use of the fact that people are either lazy or ignorant in relation to managing and maintaining their computers properly. Some of this maintenance can be, and in many organisations is, automated, but it cannot all be. Resisting ‘scams’ that introduce malicious code is entirely down to individual responsibility.

Threats to availability

Information availability is often not seen as a security issue, but if information is kept securely it should be available when it is required. From a technical perspective, there are four types of problem that affect availability of information.

Perhaps the most obvious problem is system malfunction. We have all experienced unavailability as a result of our computers, networks or file servers breaking down. Often the loss of access is temporary and thus simply inconvenient but, if the right precautions have not been taken, the unavailability may be permanent and very large-scale.

The second problem is human error. One might not regard this as a technical matter, but human error frequently occurs as a result of unfamiliarity with systems, poor understanding of what systems are really doing, poor system design or high levels of system complexity. It may be very easy to delete important information without realising fully what the result of a particular action is.

The third problem is caused by the fact that digital information is only 'available' via the use of computer programs and not directly via the senses. Possessing the digital object containing the information is not enough, as you also need a program that can access the information and render it in such a way that you can understand it. In a world of rapid technological change, those designing and selling software are constantly changing the formats in which they store information and the way that their programs operate.

The final problem is related to the nature of the medium on which digital representations of information are stored. There are several aspects to this problem. With paper-based representations of information, a visual inspection will reveal that degradation is taking place. In the digital realm it is often not possible to detect problems visually and it is only when one comes to 'read' the medium via computer software that one discovers that there is a problem. If a paper document starts to degrade, it may happen relatively slowly and most of the information is still readable; the loss of 'availability' is very gradual and can be arrested at any time. In the digital domain, the corruption of a single byte of a large digital object might make it completely unreadable. Most digital media types (tapes, floppy discs, hard discs, CDs, DVDs, etc.) have a relatively short usable life by comparison with paper. These aspects, taken together, mean that information stored in a digital form can be very vulnerable to loss, unless managed very carefully.

Any of the problems outlined have the potential to destroy individual objects or whole systems. Careful management of digital information assets and programs to access them is the key to countering the threat to availability. A crucial component of this is to have a well thought out backup strategy, which ensures that there is an adequate number of copies stored securely in more than one location, that backup copies are taken at suitable intervals, that this is driven by the needs of records and/or archival management and permits full destruction where needed. A second component is to put in place processes to detect problems with digital objects and carry out appropriate remedial action. It is no use waiting until you need to use a particular digital object and discovering that it is unreadable. By that time, the unreadable object may well have been faithfully backed up, replacing the uncorrupted version on all media. Technologies that may be appropriate as *part of* such processes include digital signatures, checksums and hashes,[1] all of which can be used to detect whether objects have suffered any change or degradation. A third component is to ensure that you know what programs produced your digital assets and the formats they are stored in. The National Archives in the UK have established a resource called PRONOM, which contains technical information about the structure of digital object formats and the software products that support them, and is available on the Internet.[2] It is often helpful to select a more robust format that can be read by many different programs rather than a proprietary one that can only be read by current software from one supplier.

Threats to relevance

In the digital world it is now fairly frequent for colleagues to have been working with the different versions of a document and as a result have wasted effort or been seriously misled. This problem is not confined to the world of digital representation, but the speed and ease with which information can be changed in the digital realm does increase the likelihood of working with an out-of-date copy or out-of-date information. In spite of this, many documents have no version information that would allow someone to distinguish the current version from any previous or future one.

As with many of the threats that we have considered in this section, there is no substitute for good management practices, but there are technical measures that can help. The problem can be reduced by ensuring that systems are designed such that they share information and all participants draw a particular piece from the same source rather than each keeping a separate copy. There are technologies and techniques for achieving this across many types of system but a fuller discussion of these is beyond the scope of this chapter. At a practical level, storing documents or other digital objects in shared file space on servers rather than sending copies around by e-mail can go a long way to reducing proliferation.

In addition, there are technologies, often in the form of EDM or EDRM systems, that handle revision and allow individuals to 'check out' a document for editing and check it back in once they have finished. This approach keeps track of changes and allows the recovery of any previous version and details of what particular changes were made, when and by whom. Surprisingly, the overhead in terms of file space required to achieve this is very modest. I have a dozen versions of a recent document available at a cost of less than twice the file space required by the final version alone.

Threats to authenticity

Under this heading, we are concerned primarily with the substitution of one version of a digital object for another in order to falsify the record. We will not concern ourselves with issues concerning whether or not what was accepted by the archivist or records manager was the genuine article in the first place. The approach to dealing with that aspect is no different from the one you might take with paper accessions.

The ease with which digital objects may be modified means that, without appropriate processes in place, they may leave no readily discernable trace. This is a major issue in terms of being able to establish the authenticity of digital objects.[3] As in the paper world, there is no substitute for good custodianship. In terms of the technical measures that may be employed to aid archivists and records managers in the maintenance of authenticity, there is one area that deserves mention – digital signatures.[4]

The traditional concept of a signature is:

> *any mark made with the intention of authenticating the marked document (American Bar Association)*

A digital signature is designed to serve similar purposes to a traditional hand-written signature:

- authentication (establishing the identity of the author);
- integrity (that the signed document, or other object, is unchanged); and
- non-repudiation (the author cannot deny the transaction).

Digital signatures are produced from a combination of something unique to the person signing (a person's 'private key') and something unique to the document being signed (a digital digest of its contents). Each signature is therefore unique to the document to which it relates. Moreover, a person may have as many 'keys' (see section on 'How are digital signatures created') as are required to

generate different signatures for different purposes. Traditional hand-written signatures are impossible to steal but easy to forge. Unlike traditional signatures, digital signatures are almost impossible to forge but the keys used in signing may, if not properly looked after, be stolen or misused. A useful analogy is with seals that were used widely until the late nineteenth century to authenticate documents (Moss and Currall, 2000). There were personal seals and seals associated with offices (or roles) held by individuals and with institutions. In the case of seals they were also difficult to forge but could be stolen or misused.

A digital signature does not look like a traditional signature and is in fact a small incomprehensible digital object. An example is given below:

```
-----BEGIN PGP SIGNATURE-----
Version: PGPfreeware 6.0.2i

iQA/AwUAOVMeDypYUiSnnmBwEQLh6QCePfQXRriaPoHaZifxYqSAn+0QwjIAn3lh
TxSvy2tQZSlvEPkFi/5dl6bq=u9gB

-----END PGP SIGNATURE-----
```

In the world of paper, documents are viewed directly by the human observer. In the digital world all ‘objects’ are streams of bytes that have meaning only when interpreted by a ‘program’. Similarly you do not require any tools to make traditional signatures (except a pen). To verify a traditional signature, you need to have some sort of knowledge about what the signature ought to be/look like. It is relatively easy to detect alterations to paper documents, so long as you are looking at originals and not photocopies. You do, however, require tools to create and verify digital signatures and to detect alterations to those digital documents, in addition to contextual knowledge such as who the document should be signed by and what their signature is like.

Finally, it is important to emphasise that digital signatures are distinct from computer graphic images produced by scanning hand-written signatures. These graphic images may easily be copied from document to document, so they are not useful or valid in terms of asserting identity or integrity. Digital signatures on the other hand provide for increased confidence in digital information exchange in the areas of identity and integrity. The most common use of digitally signed objects is the set of signed certificates installed in your web browser that permit secure connections to be established between your browser and the web servers of e-retailers such as Amazon.com or the online sales sites of airlines.

Like any other device, digital signatures are only as useful as the process that surrounds their issue, distribution, use and revocation. With appropriate processes (including traditional processes such as registration in an associated volume, multiple witnesses and the participation of the most senior executives), digital signatures can carry the same sort of authority that seals do. Without such processes, they have little value.

Risk

Earlier discussion has focused on a wide range of possible threats to digital information. It is now time to try to put these into some sort of perspective. There are three elements to this: first, the principles of most of the things that have been discussed are no different in kind from those that you deal with in respect of physical information manifestations; secondly, you can make life much easier by ensuring that, as archivists and records managers, you establish good understanding and working relationships with those that provide technical support for your operations and, finally, it is necessary to undertake a risk analysis before rushing to action.

What is risk?

So what is risk and how is it analysed? The list of threats above is **not** a list of risks. Writing them down in the form of '100 reasons why you should not be able to sleep for worrying' is not a risk analysis. A risk has three elements: a contingency, a consequence or impact (with some measure of how big) **and** a likelihood of occurrence. As I sit here writing, a possible risk occurs to me. A large passenger jet could come crashing into my house. This is a contingency. The impact of that would be disastrous for me and my family. So why am I not worried and trying to do something about it? Clearly, the answer is that the likelihood is so low that this contingency becomes relatively unimportant to me. People are often rather perplexed when they say 'we must do something about X because we might get sued' or 'we must do something about Y because it is a legal requirement'[5] and I say 'so what?' I am interested in taking action only if there is a real risk. The e-mail server has failed three times in the last six months and the supplier says he can no longer get parts to fix it, so next time it fails it fails for good – this gives a manager all three elements and they can take appropriate action as a result.

There are a number of difficulties with risk in general and in the digital domain in particular. An example is that people do not take risks seriously until the contingency actually occurs. They then overreact and rush around doing things. Gradually the memory fades away, leading to an unwillingness to act. Think about what happens after a rail or air crash. Many of the consequences are rather remote unless you have actually experienced the outcome concerned and therefore it is difficult to understand the impact. The assessment of likelihood can also be difficult, particularly in relation to new legislation for which there is no case law and when it is difficult to know how many people will exercise new rights. Likelihood is also notoriously difficult to assess for 'rare' events (such as multiple failure of nuclear reactor safety systems). In computer security, many security problems do not happen often enough to get a good estimate of likelihood, and for the most part our systems are too good for our rhetoric. This leads to people relying on them, leaving things until the last minute and having no plans for the eventuality of failure.

Security is about reducing risk:

- risk to the individual
  - loss of a day's/week's/month's work
  - impersonation
- risk to the organisation
  - reputation
  - litigation
  - the work of members
  - financial loss
  - fraud.

Security is also about controlling risk. We cannot control risk if we have not identified the risks and evaluated them in terms of impact and likelihood. In other areas of risk management, the establishment of a formal risk register, together with processes to ensure that it is reviewed and revised at regular intervals, is undertaken. This is rapidly becoming the norm in information management and is a part of the developing standards discussed in the next section. The threats discussed earlier need to be assessed in your situation and approaches to tackling them identified and prioritised. There are essentially four ways to deal with risks:

- Treat – control the risk by taking appropriate steps to make it less likely or lessen the impact
- Take – accept the risk and its consequences (especially if there is nothing feasible and/or affordable that can be done about the risk)
- Terminate – avoid the risk by not doing the activity any more
- Transfer – make the risk someone else's problem (e.g. by insurance, outsourcing, etc.).

This section has introduced only the bare bones of risk and hinted at how to go about tackling it. What you now need is solid guidance and fortunately you do not have to make all this up from scratch; there are templates, standards and guidelines to help you and we will deal with these in the next section.[6]

Information Security and Organisations

As archivists and records managers, what are the real risks that you are trying to guard against? Both in relation to your work and to that of the organisation that you serve, the fundamental high-level risks are of being unable to get on with your business and spending a lot of time sorting out compromised information. As professionals, you are also trying to guard your organisations from compliance failure, litigation and corporate amnesia while also enabling the organisations to assert their legal and other rights.

Organisations require policies and practices recognising that information security is not just about computers and networks; it needs to cover most areas of work practice. This will become clearer in the discussion of the standards in this area. Organisational policy frameworks need to recognise the need for a good understanding of the issues surrounding security and serious commitment at all levels. There needs to be a risk-based approach to managing the security. Security measures need to be easy to use and to provide access to information according to multiple cross-classified roles in the organisation. It is clear that whatever you do will provide more inconvenience to the legitimate users of information than to those who might seek to disrupt your information environment. It is just the same with the security measures in your house or car which make life much more difficult for you than for potential thieves.

One size does not fit all. You need different levels of security for different purposes. Think for a moment about a bank. The security measures to restrict access at the front door (during banking hours) are very limited. It is much more difficult to get behind the counter and there are security systems to ensure that only employees do that. To get into the vaults, where the things of real value lie, there are further layers of security involving multiple keys, time locks and so on. We need to ensure that the measures deployed are proportionate, bearing in mind that it is sometimes cheaper and more effective to accept risk rather than eliminate it. If we take a suitably balanced approach, people will find it easier to accept higher levels of security for the really important matters.

What we are seeking to do is to strike a balance:

- Ease of Use with Protection of Information
- Cost of Protection with Risks posed by Inadequate Protection
- Privacy of Information Access with Monitoring for Aberrant Behaviour
- Automatic Protection with User Understanding and Behavioural Change

Standards for Information Security

Information security is an important matter for all organisations and the subject of international standards. The current standard started off as a British Standard (BS7799) but has now become an International Standard (ISO/IEC 17799:2005 and ISO/IEC 27001:2005).[7] The standard is in two parts:

ISO/IEC 17799:2005 – 'Information Technology – Security Techniques – Code of practice for information security management', which can be viewed as a comprehensive list of best practice in security matters. It consists of 132 specific security controls under eleven major headings or Control Areas:

- Security Policy

- Organisational Security
- Asset Management
- Human Resource Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance.

In assessing and applying the controls, it needs to be borne in mind that they do not all apply to all organisations, but identifying that some of them are not relevant is part of the task. What you can see from the list is that ISO/IEC 17799:2000 is very wide-ranging and is not focused purely on 'techie' matters.

ISO/IEC 27001:2005 – 'Information technology – Security techniques – Information security management systems – Requirements' is a specification for Information Security Management Systems (ISMS), a framework within which an organisation can monitor and manage all aspects of information security to control risk. It is against this that certification to the Standard can take place for organisations that require certification. The steps in the process are:

1) Define an information security policy
2) Define scope of the Information Security Management System (ISMS)
3) Perform a security risk assessment
4) Manage the identified risk
5) Select controls to be implemented and applied
6) Prepare a 'Statement of Applicability' (SoA).

The implementation and operation of an ISMS is based around a PDCA (Plan, Do, Check, Act) cycle.

Plan understand security requirements, establish policies, carry out risk analysis

Do deal with risks and implement and operate controls

Check monitor and review performance and the ISMS itself

Act identify and implement improvements, deal with new issues and apply lessons learnt

Many organisations, and perhaps more importantly their insurers, are now demanding that their business partners have certification against standards such as ISO/IEC 27001 and its predecessor BS 7799-2, as a condition of doing business with them, in order to defend themselves against poor information management practices in others that might impact on their own business.

Conclusions

The principles of information security in the digital world are essentially the same as in the physical world. This means that, as a practising archivist or records manager, you are already well versed in

them. The practice however is rather different. There is really only one feasible approach to dealing with the new situation and that is to form a close partnership with professionals in the IT domain, such that they understand what you are trying to do and you understand what is practically possible. You should be aiming for innovation as a result of partnership, rather than a simple supplier–consumer relationship.

From your side, you need to understand the threats, where they come from, what they mean and the effects that they can have. In addition, you need to understand both the role that technology can play in providing solutions and also the problems that technology brings with it.

A systematic approach must start with a thorough analysis of threats facing your holdings and the risks both of taking steps and of not taking steps to counter them.

From the IT side, it is essential that you operate on relatively secure machines, both individual workstations and the server and network infrastructure that supports them. You should not underestimate the role that every person who uses a computer has in ensuring that their machine does not fall prey to a range of types of Malware. Your IT professionals should be able to take care of the server and network infrastructure, but their job will be made difficult if individuals indulge in practices that open up security vulnerabilities.

As is the case in the world of physical information manifestations, in the digital world much of security is about good management and processes, and there is a clear need to establish good practices that are proportionate to the risks involved. People will circumvent procedures that are unnecessarily cumbersome and the net result of over burdensome procedures may be poorer rather than greater security.

Things will go wrong. So you need to plan on that basis and have appropriate tools to monitor the situation and to recover from problems. Every aspect of security discussed in this chapter needs the support of good record keeping, so that you know what has been done, how, when, by whom and to what

---

[1]Digital Signatures are discussed in the section on 'Threats to Authenticity'.

A checksum is a simple way to check the integrity of information by detecting errors. It works by adding up the basic components of a message, typically the bytes, and storing the resulting value. Later, the same operation can be performed on the information and the result compared with the original checksum, and (assuming that the sums match) conclude that the message was probably not corrupted. The simplest form of checksum, which simply adds up the bytes in the data, cannot detect a number of types of errors. In particular, such a checksum is not changed by reordering or multiple errors that cancel each other out.

A hash function takes a sequence of characters of any length as input and produces a short fixed length sequence of characters as output, sometimes termed a message digest or a digital fingerprint. If the same hash function is used, the same result will be produced for a particular input sequence, but a radically different result if the input sequence has changed in any way. Hash functions are less vulnerable to the problems indicated for checksums. Common hash functions are MD5 and SHA-1.

[2] The first version of PRONOM was developed by The National Archives digital preservation department in March 2002. Its genesis lies in the need to have ready access to reliable technical information about the nature of the electronic records now being stored in Digital Archives. Digital information is encoded into a form that can only be processed and rendered comprehensible by very specific combinations of hardware and software. The accessibility of that information is therefore highly vulnerable in today's rapidly evolving technological environment. PRONOM holds the technical information about the structure of the formats, and the software products that support them. It was developed to provide this function, initially as an internal resource for National Archives staff, but is now on the Internet at: http://www.nationalarchives.gov.uk/pronom/.

[3] The InterPares project has been doing some interesting work applying diplomatic to the digital world (http://www.interpares.org/).

[4] A good, non-technical account of digital signatures and the context of their potential use can be found in Clifford Lynch's article 'Authenticity in a Digital Environment: An Exploratory Analysis of the Central Role of Trust' (Washington, 2000) (available at http://www.clir.org/pubs/reports/pub92/lynch.html, accessed February 2006).

[5] There is usually a good reason for the legal requirement and the risk may be better specified in terms of that more direct consequence than in terms of breaking the law.

[6] The ERPANET Risk Assessment Tool (http://www.erpanet.org/guidance/docs/ERPANETRiskTool.pdf) is one useful resource, as is the DIRKS guidance on risk assessment in Appendix 11 of the DIRKS documentation (http://www.naa.gov.au/recordkeeping/dirks/dirksman/dirks_A11_risk.html).

[7] Documents relating to the standard can be purchased from the BSI (http://www.bsi-global.com/) or ISO (http://www.iso.org/) or Standards Direct (http://www.standarddirect.org/), and many consultancies have websites via which ISO/IEC 17799:2000 and BS 7799-2:2002 or ISO/IEC 27001:2005 advice, guidance, information and service can be obtained (e.g. http://www.gammassl.co.uk/bs7799/, http://wwwinduction.to/iso17799/).