Information Security:
Effectively securing your data

Achiever Software
Ashted Lock
Aston Science Park
Dartmouth Middleway
Birmingham
B7 4AZ
T: 0121 380 1010
F: 0121 380 1011

Achiever software

Contents

Introduction

As modern organisations store more and more data, they are adopting more complicated databases to cope with the increased demand. Applications are also being integrated to derive new information from the interconnected data. As the scale and complexity increase, so security and data protection become ever more important. Applying a security policy to a single application alone is not enough. Any Data Protection Manager will agree that maximising security involves people and processes as much as systems.

"Any database is only as secure as the people and processes accessing it"

This assertion comes from hard experience and encapsulates the importance of an effective data security policy.

The challenges for an organisation trying to maintain data security and comply with relevant legislation are many. However, a successfully implemented policy will give confidence to your customers and staff, protect commercially sensitive information and allow disparate databases to be drawn together to present additional information derived from those relationships. Such information can highlight patterns or trends which could prove commercially advantageous or even allow a research breakthrough.

This white paper looks at some of the challenges to data security and considers measures to address them, or at least minimize their impact.

Scope

The scope of any data security considerations is important as it helps define the boundaries of the review. You must consider which systems are to be included. A security policy that doesn't relate to the whole business risks exposing that organisation to legislative non-compliance (and its associated fines) or even to a security breach and all of the associated costs.

Implement a security policy

All organisations, whether small or large, private or public sector should have an organisation-wide data security policy. This policy should cover all data stored, both electronically and physically with processes and protocols to cover all elements of data held by the organisation.

Which data needs to be secure?

The decision about which data needs to be secured is partly an internal decision and partly dictated by legislation. All data regarding people, both external to your organisation (customers, prospects, patients, students, etc.) and internal staff, is subject to legislation (for the UK see *Data Protection Act* and *Freedom of Information Act* on page 13).

Non-identifiable or anonymous data held against individuals and general information relating to companies, sales leads, orders, research projects, for example, can be secured to a level chosen by your organisation. It can be tempting to dismiss the enforcement of security for such data but there may be consequences.

If such data isn't secured, the perception of its importance is reduced. Your data is immensely important to your organisation and the protection of this valuable resource needs to be a high priority to all employees. *All* of your data should be considered in terms of its value to either your own organisation or to a competitor and managed accordingly.

Complications when dealing with third parties

Opening up your sensitive data to third parties creates certain risks, but if properly controlled it can bring benefits to your organisation. There are often strong strategic reasons for sharing data whether it is customers accessing their account information, research collaboration with other organisations, or an external agency carrying out work on your behalf. These are all viable reasons for sharing data as long as it is managed correctly (see *Effective Security Management* on page 8).

"An organisation's data is its lifeblood and core to its successful business"

Common Security Concerns

Securing data isn't always about passwords, encryption and security levels in your databases. It encompasses the whole process of how information is passed around your organisation. The following are a few areas that often pose challenges to a Data Protection Manager.

Archiving

Physical records, such as financial information, that are no longer current but need to be stored for a number of years, will require archiving. The deciding factor for the location of archived data is often based on physical space availability or logistical considerations, with little consideration for security.

However if this storage area is not locked or is accessible to visitors or employees with unrestricted access, the data will not be secure.

If physical archiving is to be carried out, it is important to ensure that a secure location is selected.   One such consideration for an office with limited storage space could be a computer server room. Your IT Manager may disapprove but the computer server room is often considered as a short-term solution by Data Protection managers with a storage resource problem. This may also raise the issue of whether paper-based archiving is always the most appropriate method.

Fax machines

It is not unheard of for confidential paperwork to lie unattended on fax machines for long periods of time. Data received via fax should be covered by the security policy as soon as it arrives. Fax machines should not be left unattended if they regularly receive confidential information and any data received should be forwarded to the relevant person as soon as possible.

Email

The ubiquitous email message may be the wonder of modern business communication but it can also be the biggest culprit for exposing data to security risks. Data can be sent by email in seconds, but how many people give consideration to the security implications? Internal emails leave “an information trail” that is not officially controlled and can be difficult to administer.

External emails are even worse as emails are sent through public mail servers that are neither secure nor controlled by your organisation. The moment an email leaves a mail server it is exposed to the risk of interception.

While there are email encryption products available that allow emails to be encrypted and only opened by the intended recipient, they are rarely used due to the inconvenience of setting them up and concerns about compatibility with the email application. Almost all email clients (including Microsoft Outlook, Outlook Express, Novel GroupWise, and IBM Lotus Notes) support secure email, but many organisations think it too much trouble to configure. Third party software allows security to be added to your existing email client - see www.pgp.com, www.essentialsecurity.com, www.globalsign.com among others available online. At the very least, email attachments should be encrypted before attaching them.

CDs, DVDs and flash memory sticks

If email is the biggest culprit for data security risk, then “pocketable” data devices come a close second. All modern PCs are fitted with CD or DVD writers where data can be easily copied onto a disk, making it difficult to manage from a security point of view. Such disks are often produced for a single-use data transfer – often from one computer to another within the organisation where network access isn’t convenient. After the data has been transferred however, the disk usually lies around on a desk or, even worse, is thrown in a waste bin without being destroyed.

Commercial waste is now an easy source for thieves looking for commercially sensitive data. CDs and DVDs that are no longer required should be destroyed before being disposed of. Many office shredders have the ability to destroy unwanted disks and credit cards. Your security policy should include a process for such unwanted media.

A similar risk, but not usually through the disposal process lies with the common flash memory sticks that are now very popular. They are one of the easiest ways of transferring data and with increasing price reductions and increased capacity almost everyone carries one. However, their small, convenient size also means that they are easily lost and therein lies the security risk.

Laptops

Mobile computing and home working is becoming more commonplace, which again causes security problems as sensitive data can be stored locally. A number of recent high-profile cases have appeared in the national news regarding data losses by Government personnel. While some laptops have fingerprint readers, and all have passwords, these are mere inconveniences to a data thief. Opening a laptop and removing the hard drive takes only a few minutes, your data can then be accessed or loaded onto another machine very easily.

Some laptops are configured to encrypt the contents of their hard disk drives and this feature can be a useful protection in case of laptop loss or theft. Windows itself (Windows XP Professional and Vista) can be configured to automatically encrypt folders or complete drives (see screenshot 1, below). These steps are no substitute for a well implemented security policy but can be very useful tools to help implement security for an organisation.

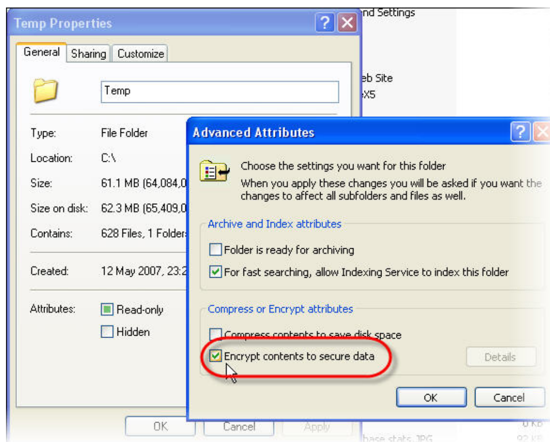

Figure 1 - Configuring data encryption in Windows XP professional

A more effective method for reducing risk from laptop users is to provide secure remote access to your office network and only allow access to a single secure copy of the data. This ensures there is no remote copy to lose or be stolen as the laptop is only used to give remote access to the central data store.

The use of virtual private networks adds security to such remote connections by encrypting all data that flows between the office network and the client laptop. A robust password policy should be implemented and an awareness of security considerations by laptop users should dissuade them from using unsecured wireless networks without forethought.

Discarded hard disk drives

Another risk can arise from old discarded hard disk drives that have been replaced by higher capacity units. As data volumes steadily increase and are matched by the seeming limitless capacity of newer drives, many older drives are being squeezed into obsolescence. There is a risk that such drives are either installed in less demanding machines or thrown away with commercial waste.

Often old drives are simply formatted before discarding or placing in another machine. However, this is not effective as a standard drive format leaves all data intact removing only the file indexes. These indexes can be easily restored allowing full access to your sensitive data.

To truly erase data, it needs to be overwritten. There are many free and inexpensive wipe programs (also known as shredders) that cover the data with zeroes or random patterns, making it unreadable by data-restoration software. Whether you use a freeware shredder or take a hammer to your old drive (a shredder is far more effective), an appropriate process should be considered for your organisation and included in the security policy.

Effective Security Management

To ensure that your organisation's information is managed effectively, it is important to formalise security guidelines and procedures in a policy. This should include the details of those responsible for managing and enforcing the guidelines. The following section outlines some areas that you may want to consider when implementing a security policy.

Appoint a Data Protection Manager

To set up and administer a security policy, a Data Protection Manager should be appointed. For small organisations this does not need to be a full-time post, but there should be someone responsible for data security that has the authority to recommend policy changes and to implement and enforce good practice.

Most organisations have many systems which should all be covered by the data security policy, taking into consideration different security requirements for each individual system.

The Data Protection Manager's remit should include compliance with relevant legislation including, in the UK, the Data Protection Act and the Freedom of Information Act. There are also other considerations such as compliance with the Telephone Preference service and regulations associated with other direct communications (see *Legislative considerations* on page 13).

User buy-in and data ownership

For many users, the security of their company's data is seen as someone else's responsibility and they would not consider security unless data becomes unavailable. Therefore it is important for a Data Protection Manager to educate staff on security issues. This will be easier in some departments than others as areas such as HR, Accounting and Marketing have a greater appreciation of data security than others due to the nature of the data they manage.

"This battle for security is as much a battle for hearts and minds as for technical solutions"

Implement Employee Contracts with staff

One method of enforcing compliance from employees is to include a data security element in employee contracts. A clear statement of data policy in a contract or the employee handbook can help raise awareness to individuals of the issues and their responsibilities. It may also be useful to include a section on non-disclosure of data and the associated penalties if contravened, where relevant.

Budget

Acquiring sufficient budget to carry out all the necessary security preventions can pose a challenge for a Data Protection Manager.

The most effective way to justify any spend on data security is to assess the impact and associated costs that would be incurred if critical data were lost. The following are questions which could be used to help organisations understand the impact of lost data.

- How much would it cost the business if all current sales leads fell into the hands of the major competitor?
- What would be the impact on the relationship with a major client if they found that their details were being sent using unsecured emails and exposed to interception?
- What would be the financial penalties if the organisation could not be shown to be compliant with the Data Protection Act or if a customer requested their details in accordance with the Freedom of Information Act and were given the wrong details?

When faced with a limited budget, categorise risks accordingly and ensure that any spend is concentrated on areas at most risk.

Sharing information with external agencies

Many corporate information systems allow some sort of access for customers, partners, and external agencies. This can range from allowing customers to check their account details and place an order online to partner portals on a corporate website. Whatever the level of functionality there is always a limited amount of data made visible to allow such work. Such access needs to be carefully considered as your organisation is responsible for the security of this data even when it is being processed by an external source.

As well as the technical considerations of making the access method secure, (i.e. by using an HTTPS secure web connection or IP-restricted access) any external agencies should be required to sign a comprehensive non-disclosure agreement (NDA). This should be a legally binding agreement that ensures that the external agency will apply your security policy with the same level of rigour as your company.

Ideally, whether it is a customer, a partner, consultant, or marketing agency, the data being shared should exist within your organisation only. Where possible, do not send copies of your data to third parties “to facilitate local processing” because the management of its security becomes much more difficult. Applying your security policy to data held off-site is very difficult indeed and should be avoided if at all possible.

Customers

Customers are typically given access to their data through a web-based interface. Customer web portals are now quite mature and customers rightly expect their data to be secure. Therefore ensure that any such systems use HTTPS rather than HTTP as this significantly increases security between the customer and your web server. HTTPS authenticates each user by more robust criteria. It is also imperative that the software application ensures that each customer can only see their own data.

Partners

Similarly, partners are also commonly given access via a web portal. There are, however, still some applications that require proprietary links to be in place involving databases at both sites synchronising data between them. Such links require heavy IT involvement and usually involve a high level of IT administration.

It is important to consider which areas of your system you allow partners to access. While they may be able to view information regarding leads, clients and orders that relate to them, there may be other data, such as competitor information, that is not considered sensitive to your company, but which could prove invaluable to partners.

Therefore, ensure that no shared or general information is available to partners. One example might be the advanced publication of a product launch campaign where one geographical area has been set up and made visible before the rest of the campaign has been set up.

Partners should always have signed an NDA and agreed in writing to the relevant parts of your security policy before being given access.

Other External Agencies

Consultants, data cleansing organisations and marketing agencies are all examples of organisations that you may choose to share your data with.

These organisations should be well aware of data security issues and should also have an NDA that commits them to keeping your data secure. Do read these agreements as they will be drafted with any advantage favouring the external agency. It is preferable to provide your own NDA for them to sign. This is common practice and should present no obstacle to the business. It is also worth getting confirmation in writing from the external agency to ensure that they are in compliance with the relevant legislation. You should also get written confirmation that any copies of your data have been completely destroyed on completion of the work.

Marketing Agencies

It is worth getting confirmation in writing from any marketing agencies that they are in compliance with the relevant legislation and also adhering to guidelines regarding the Mailing Preference Service or appropriate equivalent.

You should also get written confirmation that any copies of your data have been completely destroyed on completion of the work.

Data Cleansing Organisations

Data quality is very important for the effective application of a security policy and it is important that your organisation maintains accurate and timely data. Poor data quality not only impacts the business but can also be in breach of security legislation (see Impact of data quality on security below).

External data cleansing specialists are often used by organisations to maintain clean data. Such organisations should be fully aware of the security implications of their work.

The impact of data quality on security

Having poor data quality can impact an organisation's ability to control security and to comply with legislation.

Many organisations periodically schedule formal data cleansing operations. These might be annual or bi-annual and are aimed at reinforcing the on-going maintenance of quality data. These exercises reinforce the message that data quality is important to the organisation. Involving end-users can help to ensure they are more diligent when entering and maintaining data records in the first place.

Duplicate records

One of the most serious problems among corporate databases is data duplication. Records that are entered into a database more than once cause havoc with data quality, user confidence and security. There are several reasons for duplication such as user error, lack of validation when integrating with a second application/database or poor data cleansing prior to data import process, among others.

When trying to identify and resolve duplicate contact records in a database it is very useful to be able to use address data to confirm or discount suspected duplicate pairs. If two seemingly identical contact records each have different geographic locations then they are probably not representing the same person. However, any level of automation of this process needs address data to be consistently formatted and to be as complete as possible.

Cleansing address data

One area of data that can be very effectively cleaned is address data. Addresses that have no postcode can have their postcode generated, those that have a postcode but not a complete address can have their full address generated and address components can be moved to the correct fields within the address, such as ensuring that a town name actually appears in the *town* field rather than address line 2. Once address data is clean then it can be used to support contact authentication. There are several products that can help in this task including QuickAddress (www.QAS.co.uk/Quick_Address) and Postcode Anywhere (www.postcodeanywhere.co.uk).

Inaccurate records

While duplicate records are a significant problem when applying security rules so too are inaccurate records. Field values need to be present when processing decisions are to be based on them and they need to be consistently spelt and formatted to allow reliable processing. A person cannot be processed correctly as a customer if their record status is still set to “Prospect” or if it is omitted altogether.

The general defences against poor or incomplete data can be bolstered by the use of third party tools. Such tools can integrate with an application or work alongside. Such tools include PAF systems that automatically correct and format address data at the point of entry. Other automated duplicate record search tools can alert system administrators to possible duplicates before the situation causes complications for information disclosure.

Professional advice on this subject can be very valuable in the long term.

Integrating other applications

The integration of applications introduces another level of complication to data quality issues. The most obvious difference is that records shared between applications, for example a CRM and an accounts application or a patient management system and a medical test scheduling system, are used for different reasons in the two systems.

Data ownership between applications

Where a record is accessible by two separate applications, only one of them should be the owner. The owner should have priority for updating the record and the shared application may have read access only, or may only be able to update this field at a certain stage.

An example of ownership might be organisation records which, when first identified by a company, are inserted into the CRM application, usually as sales prospects. It is normally not appropriate to enter such organisations into a financial accounting application until a sale has taken place and the organisation has therefore formally become a customer. The CRM owns the organisation record and has full update responsibility until the organisation becomes a customer. Once it becomes a customer, ownership might be passed to the financial accounts application and updates to the record might be controlled primarily by accounts.

Legislative considerations

All UK organisations are controlled by one or both of the two pieces of data legislation, the Data Protection Act and the Freedom of Information Act (FOI). The former is aimed at ensuring that only appropriate information is held about individuals, that it is only held for as long as it is of direct use and that communications can be opted out by the people to whom they relate. The FOI Act is aimed at making available to a person all information held on them by a public-owned organisation. These pieces of legislation relate to all contact data held by these organisations.

The main implications of each of these are as follows.

Data Protection Act

All contact records must have opt-out preferences allowing the recording of personal communication preferences. Further, all mailings and communications generated from the system need to honour these preferences. Failure to comply can result in financial penalties to the organisation and can harm any relationship that currently exists with the prospect or customer.

Data about a person should only be stored for as long as it is directly useful. It is not acceptable to leave information stored against a contact for possible future use.

Freedom of Information Act

Any person has the right in law to request within “a reasonable period” (generally accepted to be about 48 hours) a copy of all information held about them by a public-owned organisation. An administration fee (generally between £10-15) can be charged, however, the work and costs involved in collating such information can be very extensive if the organisation employs multiple databases.

Having a single primary database containing all contacts in one single application makes this task much easier and if users avoid keeping local copies of data (even temporarily) then gathering such information is at least possible.

If requested to provide data according to the Freedom of Information Act, it is as important to ensure that the correct data is sent to the person making the request. For example, where there may be several records relating to John Smith on the database, it is imperative that only the correct record is issued to the John Smith requesting his information.

Mailing Preference Service

Any organisation that carries out direct mailing should cross-reference its target contacts list against a central opt-out contact list administered by the MPS called the *MPS Consumer File*. Avoiding sending unwanted mailings to people on this file makes good business sense as it contains contact names representing the least effective target list.

Honouring such preferences shows professionalism and a respect for the customer. It also reduces spend on natural resources and postage and can give a boost to a company's "green credentials".

See the Information Commissioner's Office website (www.ico.gov.uk) for information on the UK regulations relating to unsolicited communications via mail, telephone, fax, email, SMS and other electronic messages.

Summary

Ensuring data security for your organisation is not just about minimising the risks of data-related disaster but can lead to positive benefits such as cost savings and improved business relationships.

Streamlining archiving and data sharing processes can reduce costs and free up time for productive work. Updating authentication processes can give users faster access to a more focused view of information.

Cleaning data and reducing duplicate records can improve compliance with legislation and give a clearer view to users who might previously have complained about poor targeting and unfocussed, inefficient campaigns.

Raising and maintaining data quality and security awareness can take considerable effort but the benefits are felt throughout the organisation from board-level to office workers and partner organisations.

Maintaining an ethos of data quality and security and ensuring that staff have appropriate tools and training should ensure that your data will continue to be one of your organisation's biggest assets.

Appendices

Further information

1. **Maintaining data quality and integrity** white paper available from Achiever Software at www.achiever.co.uk
2. Data Protection Act - www.opsi.gov.uk/ACTS/acts1998/19980029.htm
3. Freedom of Information Act - www.opsi.gov.uk/ACTS/acts2000/20000036.htm
4. Mailing Preference Service - www.mpsonline.org.uk/mpsr/
5. Encryption - en.wikipedia.org/wiki/Encryption

About the authors

Founded in 1992, Achiever Software is a UK-based Customer Relationship Management (CRM) solutions developer that has extensive experience of implementing Corporate Information Management solutions in the Private and Public sectors.

Achiever Software's innovative partnership approach to the delivery and implementation of the Achiever Anyware application facilitates the creation of a solution that suits the unique business process and data requirements of each customer. Achiever's flexible relational data structure allows solutions to be designed to suit diverse business requirements across multiple departments and industry sectors including Public Sector, Education, Contact Centres, Medical Information Systems and Financial Services.

Achiever is aimed at organisations requiring a Corporate Information Management solution capable of managing sophisticated and complex business requirements whilst allowing them to maintain system ownership.

Achiever's strong integration capabilities allow it to maximise the benefits of a customer's existing business systems to create a complete solution providing benefits such as improved visibility of information, increased productivity, and reduced administration work.

Data security is paramount. Achiever is designed to ensure that only authorised users have access to sensitive and confidential information whether on screen or in reports.