



Cryoserver Business Drivers in Law

January 2008

Contents

INTRODUCTION	3
THE COST OF FINDING EMAIL.....	4
THE RETENTION DILEMMA.....	6
EMPLOYMENT LAW	7
BEST PRACTICE.....	8
CRYOSERVER.....	9
DEPARTMENTAL BENEFITS.....	11
HR DEPARTMENT	11
IT DEPARTMENT	11
COMPLIANCE OFFICER	12
DATA PROTECTION	13
LEGAL.....	13
FINANCE AND ACCOUNTS DEPARTMENT.....	14
CLIENT SERVICE BENEFITS.....	14
EMPLOYEES	14
CONCLUSION	16
APPENDIX A. QUESTIONS TO ASK	17
APPENDIX B. CLIENT TESTIMONIALS	19

Introduction

Issues surrounding email in the work place are complex, and growing ever more complicated as the regulation and legal requirements for record keeping proliferate. No matter what the size of your firm, forensic compliance of email is already an issue you need to address. It will have greater resonance as the use of email as a viable business communications tool grows. The potential for email misuse in the workplace is increasing, exposing firms to the liabilities inherent in this medium.

Post September 11th and the *Enron*, *Andersen* and *WorldCom* scandals, businesses are scrambling to put in place information retrieval systems that will enable them to efficiently and securely produce information "on demand". Growing regulation is also increasing the potential demand on firms to produce documents with sufficient evidential weight quickly and easily. More cases than ever before are being taken to court or tribunal, and email is now fully accepted as legitimate evidence to be presented in court.

It is also increasingly recognised that a firm is held responsible for the behaviour (and misbehaviour) of its employees and to that end a firm needs to prove the authenticity of email sent to, from and around its network.

In today's world, email holds much of a firm's critical business knowledge. Cases and matters are discussed and contracts agreed, amended and exchanged via email. Clients make complaints. Firms make promises. These are all recorded in email. Law firms receive instructions by email, and give advice by email. In the past, email was printed out and put on the file. However, by doing this, the firm loses the associated metadata, which is the crucial evidence that gives the email evidential weight.

A recent survey by *Bailey Teswaine* (as reported in *Legal IT, March 2005*), found that lawyers rely more heavily on e-mail than other professionals, and that 14% regarded email as the best way to communicate controversial information. The survey also found that lawyers rely more on email in their personal lives than other professionals. Another 25% stated that they avoided on line communication because of perceived IT department monitoring.

The increase in regulatory compliance has created a focus on records retention, especially with regard to email. In the US, laws such as the *Sarbanes-Oxley Act* and emerging requirements from both the *Securities and Exchange Commission* (SEC) means that law firms will need to be able to demonstrate appropriate retention and compliance policies to clients or prospective clients who are subject to such laws.

The Cost of Finding Email

Increasingly, email provides the main method of contact between firms and their clients, and this dependence brings with it inherent problems. Lost access to an email system, or to specific messages involving a customer, can have a dramatic effect on the business. If messages are archived in the wrong place, or are hard to identify, it may prove impossible to respond to a client within an acceptable period of time.

Suddenly email ceases to be a business enabler, and becomes an inhibitor instead. The task of finding a 'needle in a haystack' – an erroneously filed or deleted message residing somewhere in the firm, imposes huge and often unnecessary support costs on the firm.

An IT administrator can spend on average 5 to 6 hours a week recovering old messages, and it can take an estimated 11 hours to locate and retrieve a message from a traditional back-up system. This is clearly not an efficient use of the time of expensive technical staff, and the costs involved can mount up rapidly.

A way of calculating the cost of restoring email

Formula:

$$\alpha \times \beta = \gamma$$

$$\gamma \times \mu = \text{Total Costs of the requests}$$

Where:

α = Hourly Rate of Technical person to recall email (£40/hr)

β = Amount of time to retrieve email from back-up tape (5hrs)

γ = Cost per retrieval

μ = How many requests per week / year (44 requests per year or 1 request per week)

Example:

$$£40.00 \times 5 = £200.00$$

$$£200.00 \times 44 = £8800$$

Email housekeeping activities can cost up to £6 per employee per day. For a firm of 100 people, this would add up to around £135,000 per year. Have you carried out an analysis of your costs of retrieving email?

Some email packages have built-in facilities (such as PST files in Microsoft Exchange) for helping users to restore accidentally deleted messages. Such facilities are fine for informal email use, but they can become unstable and unreliable when dealing with very large volumes of mail. They can even become part of the problem: end users are often unsure how to use PST files and, without careful management, they can become as difficult to control as the messages they are protecting; let alone the ability to rapidly search these files firm wide.

Spam is an email problem that law firms are addressing, on the whole successfully using a combination of filtering software and services. So assuming that destructive and illegal email is successfully filtered out, firms still need to make sure they are retaining all

messages alongside the business-focused ones. Keeping everything puts a firm into the fortunate position of being able to prove a negative, for example, proving that an email was not received.

Unwarranted deletion and necessary retention of email are only two of a whole range of problems facing firms as they wrestle with their messaging applications, and all of these issues need to be managed as cost-effectively as possible. Cryoserver is cost effective as it manages and removes these issues.

Email is:

- Inherently insecure, yet they now convey large amounts of highly sensitive data.
- Easily corrupted or changed, leading to 'multiple versions of the truth', where theoretically identical copies have different content.
- Hard to organise and difficult to search for key information. This is having a negative effect on productivity throughout the business world Enterprises that rely heavily on email need far more robust management tools and they need management procedures to match.

The Retention Dilemma

Post-*Enron*, almost every month there is another new piece of UK or European legislation mandating lengthy retention periods for records (many of which will be in email format). And there are potentially severe penalties for not retaining those records. On the other hand, there is also more and more privacy and confidentiality legislation that requires firms to get rid of personal data a lot quicker than in the past. These two conflicting requirements of retention/deletion are becoming more and more difficult to reconcile unless careful attention is paid to the practice of records management within the firm. Too often email management is seen as an IT issue rather than a records management issue - this must be changed for the firm to have any hope of complying. There are at least one hundred different pieces of legislation and retention periods covering the information sent around via email. Commonly firms leave the retention decisions one mails to users, and this can lead to mistakes when email is accidentally deleted or misfiled.

Currently, Law firms typically do not manage their business email through any process defined by the firm, but rather by whatever means and individual chooses. This could be:

- None
- Personal folders
- Public folders
- A combination of personal and public Folders
- Archive folders used in combination with any/all of the above.

Increasingly, law firms are starting to define an electronic filing policy that will store mails in Client- and Matter-related electronic folders. These folder structures may exist with the firm's email system, but will increasingly be held within the firm's document management or case management system. The benefit of a Client/Matter folder structure is that a lawyer can quickly go to information relating to that matter and see a chronological history of document and email exchanges. Problems arise, however, when an email has been accidentally deleted, incorrectly filed, or perhaps relates to more than one matter, necessitating filing in more than one folder.

There are also issues around the filing of email that contains a mixture of business and personal content, which may lead to an email being altered prior to its being filed. Firms are therefore realising they cannot rely solely on human intervention for filing of email. They need a solution that provides a fail-safe mechanism to capture and record all email in its original form, maximising the authenticity of the record being sent or received, and preserving the integrity of the document. This, in conjunction with more traditional filing mechanisms, provides a complete solution for law firms' email problems. Today, the law recognises electronic documents as a legally viable format - this includes email being used in a court of law. Therefore, firms need to ensure that its electronic document retention and disposal policy reflects how its employees create, alter, and manipulate email documents.

Email created on the firm's domain is corporate property, making the organisation responsible for the content and use of corporate email. Allowing personal use of corporate email without proper email policies in place can expose a firm to enormous risks, known as vicarious liabilities. There have already been some well-known cases where email has been the deciding piece of evidence against a firm and/or employee in a court room.

Employment Law

Records relating to various aspects of employment need to be held 'on file' for a given length of time to comply with a variety of employment legislation. For example training records should be retained for 6 years after employment ceases whereas records relating to accidents at work should be retained for 3 years after the date of the last record relating to the accident. If you are passing regulated information around via email you are required to keep every one of those email messages for the mandatory retention period. In addition, an employer has obligations to be proactive in ensuring the health, safety and welfare at work of workers and this includes preventing harassment of any sort. Email is an all-too-convenient vehicle for workplace harassment; thus the retention of email can enable the employer to meet its obligations.

Modern employment law creates ample opportunity for disputes, and firms should keep records of employees and ex-employees in case of such disputes. As the newspaper headlines often highlight, email is creating a new generation of problems around harassment, bullying and defamation at work. Keeping, controlling and managing employee's email traffic could provide valuable evidence for the defence. In fact, email is increasingly the most commonly used medium of evidence in employment disputes. It will be difficult to get rid of incriminating correspondence, and the best advice to employers is to have a system for managing the retention and disclosure of email traffic across the organisation.

Employers do not have a general right to intercept and monitor employees' communications, even in a privately owned network, unless it is otherwise stated in the employment contract. However, previous legal cases have shown, they can find themselves paying out substantial damages because of an employee's misuse of email. Employers' interests are partially protected by having the right (*The Regulation of Investigatory Powers Act, 2000*) to intercept email where good business administration requires. BUT this applies only where they have made all reasonable efforts to inform staff that this will happen and to gain their consent. Having an email retention and recovery policy in place provides good evidence that you have complied with this requirement.

Best Practice

Best practice is to specify long retention periods for all email, while at the same time complying with individuals' rights under the *Data Protection Act* and associated guidelines and directives issued since 1998. This means that it is no longer possible to store email long-term in a system such as Microsoft Exchange/Outlook; as such systems were never designed to securely store data on such a granular basis. Use of a system that encrypts all data, limits access to the data, and audits any access allows the firm to keep everything for as long as the firm decides it may have liability from any one of those email messages. The firm can then retain every single email for as long as it likes. This also means the firm can quickly settle a 'who said what' dispute, or provide email evidence for a court action or Employment Tribunal. Again, there are strict rules over how you search email; it is difficult finding the correct balance between the firm's right to search its own email repository, and individuals' rights to privacy and confidentiality. Email was never expected to grow in the way that it has. But now that it is such a vital part of the way that we work, we have to find ways of managing it more effectively. This will not only help firms to comply with the law, but will also contribute to greater productivity as more mundane housekeeping activities are automated.

In a majority of law firms, users are usually the people responsible for making decisions about record retention periods, and it is unlikely they have been trained effectively to be able to address this task with any degree of accuracy. It is also common practice – illegal though it might be – to destroy email in order to avoid an unpleasant situation, even though this might be potential evidence required in an employment tribunal or in a courtroom.

Some firms are approaching this from the archiving angle, whilst others come from the document management approach. But neither provides a complete solution. Firms need a system that makes an audited copy of the email in transit in its original form, thus maximising the authenticity of the record being sent or received, and preserving the integrity of the document.

With this approach the firm sits in a unique position: it has the ability to prove a negative, for example, "I didn't receive that particular email and I can prove I didn't." Sometimes employees/organisations need to prove they were not in the loop about certain sensitive information. This is clearly something that archiving and document management products cannot achieve, because they allow the possibility of alteration and deletion.

Now, is this legal? It is, provided you have the right email policies in place. There is no law stating that you cannot keep documents forever, which includes email. The other issue that firms are concerned about is storage requirements. Today, storage is relatively cost effective at around £6 per user year for the average mailbox quota.

Cryoserver

The Cryoserver forensic compliance system is the premier solution to allow you to meet the regulatory, data management, monitoring and security problems created by the proliferation of email in the modern workplace. Cryoserver is like the trusted flight recorder in an aircraft, acting as a “black box” sitting quietly and unobtrusively on the network allowing an independent and trusted audit of the email record whenever required.

Cryoserver takes a real time audited copy of every email sent to, from and around an organisations network. Email coming into Cryoserver is *indexed* (for fast searching), *encrypted* (for security and privacy), *digitally fingerprinted* (so the stored data is tamper evident) and *compressed*. These processes are undertaken to increase the evidential weight of your email as potential evidence.

The data is held centrally in an encrypted tamper-evident environment and can be searched in seconds. Access to the system is either in the form of a *privileged* or *individual* log on.

A *privileged* user may be an HR manager or data controller who is carrying out proper formal investigation. Cryoserver indexes everything within an email, including attachments, so requests can be carried out with single or multiple search criteria. Privileged searches within Cryoserver are audited, logged and stored in an encrypted form. This is because accountability is not just to protect your employees from invasions of privacy as defined in the Data Protection Act, but also to ensure that someone with access to the system cannot abuse that privilege. This protects both the organisation and the employees’ rights to privacy and confidentiality. Nominated “data guardians” can also immediately be sent copies of the audit trail transcript by Cryoserver to ensure privacy & confidentiality of the stored data.

These principles make Cryoserver unique; we are the only solution that focuses on the three principles of data protection.

Individual users can also log onto Cryoserver to search just their own email archive. The same powerful searching is available to interrogate their own record and forward any email of interest back to their own inbox (for example Outlook). As these users are only accessing their own archive no audit log is kept.

THE THREE GOLDEN PRINCIPLES OF DATA PROTECTION

1. Protect the data.
2. Protect access to the data.
3. Audit any access to the data.

Data Retention

- Cryoserver traps full unbroken record of all email sent to, from and around an organisation
- Feeds can be taken from all major email platforms.
- Email is indexed, encrypted, and compressed (even attachments).
- Messages are fully indexed for fast retrieval.
- Data is securely stored and digitally fingerprinted.
- No deletion is allowed within your mandated retention period.

- Legacy data can be imported into the existing email archive.
- Decisions on data retention are not left to users.
- Messages cannot be changed or viewed without appropriate authority
- Converting the format of a message, to ensure future accessibility
- No third-party databases are needed or used.

Secure, Audited Access

- Restricts access to the data to named users as part of a formal investigation procedure.
- Full, encrypted audit trail - Data Guardians monitor correct use.
- Quick search and retrieval.
- Retrieved email is validated as being the same as when stored.
- Alerts if interference is detected.
- Reporting functions for activity patterns.
- All users have vertical access to their own email via LDAP.

Departmental Benefits

Law firms are beginning to realise that the firm is liable for the content contained within an email created in the workplace, and that this email *must* be retained for a period of time defined by the business.

Unless firms act now, and build a reliable infrastructure around their messaging systems, email will start to pose a huge financial overhead, as well as placing an unacceptable strain on existing mail server storage resources.

On the whole, firms are giving personnel the responsibility to archive the correct email in the correct places, which clearly takes time each day/week/month or year. This time spent filing email into the archive can cost an average firm £1200 per head per year. With Cryoserver the cost to retain everything is £6 per year in storage.

HR Department

- HR departments can carry out formal investigations without requiring IT departments to restore back-up tapes, in itself a breach of at least two parts of current Data Protection legislation Carry out very fast investigations, which also means false allegations can be immediately discounted.
- Ensure greater employee privacy and prevents organisation-wide abuse by generating a fully encrypted audit trail every time an authorised search is conducted.
- Comply with the long mandatory retention periods for employee records that stretch for many years after an employee may have left the organisation. Much of this data is sent via email - for example references, training records etc.
- Settle potential employment tribunal cases before going to court. By virtue of having a tamper-proof record of email correspondence, the full context of any accusations can be understood and assessed upfront.
- Facilitates the monitoring of possible workplace harassment (for example, racism, sexism, obscenity, porn, defamation, etc.) by preserving a written and tamperproof record of who said what to whom and when without expense of restoring back-up tapes.

IT Department

- No more email restorations: Email restorations from back-up tapes take a disproportionate amount of time, are expensive to carry out, and often do not produce the evidence required. You can also import all legacy PSTs and backup tapes into Cryoserver as a one-off bulk import for fast searching.
- Legal Compliance: It is a breach of Data Protection legislation for IT departments to search through email back-up tapes that may contain personal data and 'sensitive personal data' as defined by the Act. Tapes should only be used for disaster recovery purposes, *not* for any other purpose.

- Centralised location for Personal Data: Users will use Cryoserver to find older email instead of hoarding them on desktops because of mail quotas. It is a breach of Data Protection legislation and security directives such as BS7799 to store sensitive data on PST files dotted around the organisation.
- Exemption from criminal penalties: IT personnel have been prosecuted for carrying out orders from management to destroy electronic evidence. Data on Cryoservers in Data Centres cannot be destroyed or altered, thus removing IT personnel from deciding whether to carry out what may be a criminal act.
- Eliminate restorations of individual email for users: IT personnel can simply give the user a URL, then users can login with their existing network login (via LDAP, so zero maintenance for IT), access their own email records, and restore the email they need back to their inbox - all with zero training.
- Save valuable mail server storage space: Users learn to go to Cryoserver to search old email (usually because it's so much faster and offers advanced features) so IT mail server administrators can delete older mail on the servers much earlier, making mail servers run faster and needing less storage.
- Real-time Replication: Cryoserver has RTR built in at the application level, which means messages can be sent to two or more Cryoservers at the same time, with full mirroring. This removes the danger of depending on a daily back-up which will only be able to restore data stored up to the point that the back-up was made.
- Minimal staff training: The training to administer Cryoserver technical features (for example disk management) takes 10minutes, as does training for privileged users. Ordinary users simply use the URL you supply them, which requires zero training.
- Minimal technical support: Cryoserver is a Forensic Compliance System; integrity is paramount. It is sealed with tamper-evident seals, so no maintenance from the IT department is required. The application can be supported and upgraded remotely directly by Cryoserver, who have no access to the data.

Compliance Officer

- Compliance with existing and current regulatory, legal and operational mandates in global jurisdictions.
- Appropriate methods of capture and storage of data that meets both retention AND privacy legislative requirements.
- Search email records in a variety of ways, such as date range, by user, by keywords, by random sample, by 'sounds like' words, by stemming etc., in order to comply with. For example, SEC regulations.
- Ensures a complete record of all email correspondence by removing the ability to delete or alter email.
- Set a single retention period (suggested minimum seven years) to provide assurance that you will be able to produce ANY email records sent or received during this period.
- Comply with short statutory discovery times (for example SEC 36hrs, FSA 24hrs, DPA 40 days, FoI 20 days etc.).
- Validates records by digitally fingerprinting the data at the instant of storage, and validated again when retrieved to prove that it is in the same state as when it was stored.

Data Protection

- Immediate compliance with your legal duty to protect personal data in email as required by the DPA. (How are you storing personal data in email? Is it secure? Encrypted? Or is it in plain text on a back-up tape?).
- Immediate compliance with your legal duty to limit access to personal data in email as required by the DPA. (Have you carried out a risk assessment specifically on email, and established who has access to those records?).
- Immediate compliance with your legal duty to audit access to personal data in email as required by the DPA. Can you guarantee that no-one is able to access email records without leaving an audit trail that is a mile wide?
- Put full controls around your management of personal data contained within email messages
- Minimise the time and cost of processing Subject Access Requests (SARs) from the general public or disgruntled employees taking the firm to an employment tribunal.
- Minimise the time and cost of processing Freedom of Information Act requests from the general public or media.

Legal

- Record employees making ad hoc contracts: these may legally obligate the firm or incriminate the employee.
- Create a forensically compliant record of email (including attachments) that can be used as admissible evidence in court.
- Acts as a deterrent, preventing the likelihood of criminal activity on corporate premises when employees know their email activity is being captured. Also enables Legal Counsel to easily spot confidential documents leaving the business.
- Facilitates the monitoring of possible workplace harassment (for example, racism, sexism, obscenity, porn, defamation, etc.) by preserving a written and tamperproof record of who said what to whom and when.
- Provide the evidence needed to resolve any contract dispute: Contract actions are time-expired after six or more years after the date of breach, so organisations must keep everything - even when it's an ad hoc contract (for example, "We'll get that to you by Friday").
- Contracts are very often altered, often unknowingly, by email. Again, retention for at least six years of all email is essential to be able to establish the facts.
- Track and validate your own Intellectual Property: sending an email to yourself containing the firm's latest IP provides an unalterable validated record of when that IP was created.
- Refute false IP claims: Cryoserver can also be used to refute any false allegation. For example, claims such as "we emailed that IP to you three years ago and you've stolen it" can be immediately dismissed.

Finance and Accounts Department

- Cost savings: The cost of implementing a technical solution like Cryoserver is less than the cumulative costs of legal fees, fines and reputational damage. The savings in HR alone justify purchase; however there is also a very fast ROI in IT, Data Protection and Compliance departments.
- Compliance with the 150+ different regulations and legislation covering records retention (for example Accounts departments are passing regulated data around in email; there is mandatory retention of business and accounting data for varying periods up to twelve years for the average limited firm.).
- Compliance with cross-border and transatlantic financial regulations that now cover electronic data for example the *Securities and Exchange Commission (SEC)* requires that all financial organisations retain all documents for a minimum of five years; these documents must be easily accessible by the SEC within this period.
- Spot confidential financial documents passing out of the firm: Financial documents can be 'seeded' with keywords which Cryoserver will trap if emailed to anyone outside the firm (even if the attachment name has been changed, or all the content has been pasted into another document).
- Due Diligence Data Freezing: The accounts department, by sending financial documents through the Cryoserver system, can demonstrate at any later date that the record could not have been altered in any way.
- Save time and money by giving Cryoserver access to External Auditors: This can be as part of your corporate governance programme, or simply as a cost-saving measure.

Client Service Benefits

- Client dispute resolution: Clients occasionally come back many months after a transaction claiming that email made a particular undertaking or promise or constituted legal advice. The firm can immediately call up a full list of all email traffic between a client organisation and anyone at the firm to determine what was agreed between the parties.
- Irrefutable court evidence: The firm can demonstrate, for example, that an email produced by a third party has been faked, or has been altered. The firm can also prove a negative, in that it can demonstrate that it did not send a particular.
- Cryoserver is particularly useful at law firms for speedy dispute resolution, where mail is increasingly used by clients to give instructions, and used by lawyers to give advice to clients.
- Allow clients secure, audited access to their own email since their systems for storing and finding email and attachments is often not as sophisticated as those at the average law firm.

Employees

- Increased privacy: No-one can access the employee's email except as part of a formal investigation: It is not possible for others to casually read an employee's email, as access to the whole repository of data is restricted to named users carrying out a formal investigation.

- The Data Guardian system provides a dual check on the security of personal data: Employees are assured that checks and balances are in place to prevent anyone snooping their email without good reason.
- Employee rights under the Data Protection Act are protected by ensuring the data is kept physically secure, electronically secure via encryption, cannot be accessed except by named users, and an audit trail is kept.
- Comfort that an exhaustive, tamper-evident record of all email allows a true and complete picture of an employee's email usage should it ever be needed, for example a court, or employment tribunal.
- Fast searching of every email ever sent or received since the employee joined the firm: Allows the individual employee to retrieve any accidentally deleted email and immediately find knowledge hidden in old email without having to resort to IT or cumbersome Exchange Search to fulfil this request.

Conclusion

This document has outlined some of the pertinent issues that firms must address in relation to email retention.

With the increasing media coverage of businesses demonstrating bad corporate governance, governments are reviewing and enforcing new regulations to bring businesses in to line. In the United States, the governmental response to this situation was clearly manifested in the *Sarbanes-Oxley Act (SOA) of 2002*, with harsh penalties to those who do not comply.

Although you may have heard of American firms getting it wrong, regulations here in the UK and Europe are similar and as harsh. We must note, organisations are exporting and communicating globally with no thought of national boundaries and need to comply with international and local laws with whom they trade.

With the invention of email, sending electronic correspondence can be legally binding documents, anywhere across the globe. These pieces of correspondence are defined as documents, and will have a legal and retention period requirement associated with them.

As email is unstructured and the volumes of email sent to, from and around an organisation today are immense, there is no possible way that a full proof appraisal/sorting process can be used to retain the necessary documents. There is only one option to comply with the strictest retention requirements, and that is to keep all email. It is not acceptable for employees to be responsible for the record retention periods

Many organisations have questions and uncertainties on how to manage email to meet all the regulatory, legal, operational, administrative, fiscal, and historical needs. The key message from legal is that electronic records must achieve compliance, by preserving the original record, prevention of fraudulent changes, and full audit trail of any access. If these are achieved then organisations will automatically meet the regulatory and legal requirements for retention for email.

Appendix A. Questions to Ask

- Q.** Who in the firm is responsible for:
- Risk
 - Compliance
 - Data Protection
 - Email usage policy
 - Data retention policy.
- Q.** Who within the firm is responsible for advising staff at the firm on how to handle e-mail in relation to regulatory compliance and privacy legislation?
- Q.** What does the firm's email policy recommend regarding the personal use of the firm's domains for private email?
- Q.** Does the firm have a system that prevents employees from deleting or altering email?
- Q.** What size limit is currently applied to users' mailboxes?
- Q.** What is the firm's policy for storage of email?
- Q.** IS email stored on backup tapes?
- Q.** If tapes are used what encryption is applied and how does the firm ensure that they are securely stored?
- Q.** What measures are in place to ensure that unauthorised backups are not made?
- Q.** Has the firm ever had to do a restore from backup? Why? How long did it take?
- Q.** Is the threat that portable back-up tapes can be restored on another exchange server considered to be security risk?
- Q.** What happens to the email store of people who leave the firm?
- Q.** How much time do your lawyers currently spend searching for email?
- Q.** How frequently do users request copies of email that has been lost or accidentally deleted?
- Q.** What is the firm's policy for dealing with such requests and has the process been costed?
- Q.** Does the firm regard e-mails as legally binding documents that are the same as all other business document?
- Q.** What is the firm's policy regarding employee's authority to make and alter contracts over email?
- Q.** Has any member of the firm ever been in a dispute with a client regarding receipt of an email?

- Q.** Can it be proved that an email was not received? In other words, prove a negative.
- Q.** Has the firm ever had to produce email evidence in court and in what format?
- Q.** If the firm was required to produce email evidence in court would its current level of validity would be acceptable?
- Q.** What is the view of the firm regarding the evidential weight of email v paper copies?
- Q.** Has the firm ever had to restore PST files as part of a case?
- Q.** What has the firm communicated to users regarding the retention period of email?
- Q.** Who in the firm has been given training as defined under the Data Protection Act regarding investigation of individuals email store?
- Q.** How does the firm communicate to employees the conditions under which their email may be investigated?
- Q.** What is the current process for formally recording email investigations?
- Q.** Does the firm currently have the ability to audit all BCC communication?
- Q.** Data Subject Access requests require that personal data within e-mails be delivered up on request. Would the firm be able to deliver up the information within 40 days in a cost effective manner?
- Q.** Do you have a method in place to identify confidential documents leaving the premises via e-mail?
- Q.** Does HR use e-mail to transmit personal data of your employees around the firm?
- Q.** Has the firm ever had employees or ex-employees formally ask for records?
- Q.** How often is e-mail a component of disciplinary action?
- Q.** If an email audit system was in place, would this change employees behaviour around email usage?

Appendix B. Client Testimonials

Paul Morgan**Group IT Manager, William Ransom & Son plc, December 2003**

"Since being introduced to Cryoserver, via one of Corporate Internet's excellent one-day seminars, I've not looked back.

As a fairly cynical IT Manager (who incidentally, has never before bought anything as a result of a supplier-run seminar), I tend to shun ultra new technology in favour of tried-and-tested systems. That changed when Cryoserver was demonstrated to me by the highly motivated, knowledgeable – and maybe as important in IT – personable, Corporate Internet team.

The product itself is outstanding, not least for the fact that it occupies an utterly unique segment in the mail storage/forensic compliance market. Cryoserver has no peers... yet. I predict a glut of inferior "copies" will surface in the not-too-distant future, all (of course) promising the earth. In the same way that James Dyson's Dual Cyclone vacuum cleaner was the first - and still the best - Cryoserver is a simple, yet revolutionary product, which I am confident will deservedly dominate the market for a very long time to come.

I strongly advise any IT Manager, Finance Director or HR Manager who is serious about protecting their firm's integrity, to take a long look at what Cryoserver can do for them. It might just save your business. At the very least, you'll make a new friend in Corporate Internet. I did."

Ann Elia**Head of IT, Derek Fox- Senior IT, Travers Smith Braithwaite**

Travers Smith Braithwaite is a high-powered, mid-sized, premium-brand, City-based law firm. It has been ranked among the top dozen UK firms in the corporate field by the lawyer's league-tables. Established more than two centuries ago, the firm currently has about 200 lawyers (including 52 partners) and around 200 support staff working out of offices in London, France and Germany. The broad client base is comprised mainly of quoted and private firms, financial intermediaries, financial institutions, institutional investors and professional firms based in the UK, the EU and the US. The firm has built an enviable reputation based on offering a corporate-driven, partner-led service, placing a premium on quality. Originally the IT department was looking for the email equivalent of a robust records management system, but one which was not policy-based or subject to user intervention.

In Nov 2002 they installed a beta test version of Cryoserver, and it has already proved itself a robust/reliable system. "As far as compliance solutions go, Cryoserver does everything we want it to do. We suggest that everyone should have a system like this," said Ann Elia, Head of IT, Travers Smith Braithwaite.

As a law firm, Travers Smith Braithwaite has a Best Practice policy which covers the filing and retention of client-related documents. Whilst documents held within their document management system are easily filed/retained/retrieved because of the system parameters, the very nature of email and its lack of natural filing/retention make it much harder to deal with.

The integrity of the electronic document is vital for both content and metadata, since electronic documents are now recognised as legally valid and binding items. A contract can be entered into – or changed – via email, so greater emphasis is now being placed on demonstrating that the email or attachment that was received is precisely the same as the

one that was sent out, and that a secure forensic audit trail can be produced if discrepancies exist between the two.

Travers Smith Braithwaite's IT department was initially looking for an email archiving tool that would reflect the firm's current business processes. They wanted a system that would give the users a certain amount of control over what mail they kept and what they didn't. The firm's current mail infrastructure (Outlook) is set up to allow users to selectively archive email pertinent to cross departmental projects in centralised public email folders designated by project.

Email storage and policy are problematic to define, as well as implement, as many firms are finding. It is too difficult to differentiate personal from professional when dealing with unstructured documents like email. If an organisation wants to be completely compliant, it cannot rely on any sorting process, manual or automatic, to effectively distinguish between the two.

As Travers Smith Braithwaite found, traditional archiving systems are policy based – they presuppose some method of sorting the wheat from the chaff. And sorting is inherently subjective: someone has to determine rules to sort by – but in real life, not everyone will abide by "the rules" on every occasion. So a rule or policy based system is very much vulnerable to mistakes and even abuse. "When you introduce choice, you lose integrity of the data," said Derek Fox, Senior IT Support, Travers Smith Braithwaite. Compliance tools have to be indiscriminate and comprehensive: therefore non-policy based. They presuppose an "all or nothing" underpinning. By default, then, a policy-based archiving solution will not provide the necessary infrastructure to permit a firm to say it is compliant.

So Travers Smith Braithwaite implemented an email archiving system as intended, but also discovered in Cryoserver the perfect complement to such a system: an email compliance tool which securely retains all email sent into, out of and around a firm. "It is not the end of the world if someone doesn't archive something properly or accidentally deletes something that was supposed to be archived. But if a firm has Cryoserver in place as well, then those improperly filed or deleted items can be retrieved and restored using Cryoserver. It's a safety net," said Elia.

Travers Smith Braithwaite also recognises operational benefits with Cryoserver. Speedy indexing and robust performance are just two. For example, they probably receive about 250,000+ email messages in the space of a month, and Cryoserver has maintained an extraordinarily good track record at consistently handling this volume. Original concerns about an increased load on the mail server haven't materialised: they haven't had any overhead on the mail server's performance at all. During the beta phase, when it is normal to expect glitches, to Cryoserver's credit, problems were quickly rectified when the point of trouble was identified. Cryoserver amazingly crunched through 4 gigs of data very rapidly. "This gave one comfort that in a normal environment it would perform above standard as well. It is a very, very sound solution," said Fox.

Travers Smith Braithwaite uses Cryoserver as a bulwark against the hiccups of an ordinary email infrastructure as well. For example, when some HTML attachments became corrupted in Exchange, IT was able to retrieve them intact thru Cryoserver. "Exchange has its own vagaries, it's like walking a high wire and Cryoserver is the safety net underneath," said Fox.

In a similar context, the issue of backup tapes also has become moot for Travers Smith Braithwaite. The trouble with backups is that they are dependent on what was on the tape at the time the backup is run. If someone deletes an email during the day then it won't make it onto the backup tapes that run during the night. This automatically means you don't have a compliant audit record of all email received into a firm. With Cryoserver in place, however, a forensically compliant picture of a firm's email use can be demonstrated.

Elia and Fox forecast ROI in Cryoserver by offering a generic example of the effort necessary to restore email if the system weren't available. A technician would have to be sent out to the disaster recovery facility where the back-up tapes are stored; build a version of the email server; restore the tapes; create PST files; bring those files back to the office where the email server is located; and put them back into the system. This

might involve several days worth of work, plus travel expense, let alone costs incurred due to decreased productivity if the users can't access the information in the "lost" email until it is restored. And that's if everything goes right with the restore in the first place. In conclusion, Travers Smith Braithwaite has tackled the "email problem" in a number of ways and Cryoserver is an essential part of the solution. The use of email continues to grow unabated and the problems of filing/retention/retrieval are growing too. As Fox said, "Better to do something about it now, because it's not going away" – which is what prompted Travers Smith Braithwaite to take the first step towards compliance.