A MIMECAST WHITE PAPER

mimecast
unified email management

THE CRITICAL ROLE OF DATA LOSS PREVENTION IN GOVERNANCE, RISK AND COMPLIANCE

The regulatory environment means that monitoring what information leaves your organization is as vital as protecting it from external attacks. Email is one of the most likely routes by which data may leak, maliciously or more often accidentally. A successful Data Leak Prevention system will address the issue of email by policy, in a way that integrates with the systems your business has in place to address governance, risk and compliance rather than through a series of standalone tools.

CONTENTS

AUDIENCE AND REMIT

This white paper is aimed at senior staff responsible for company policy on risk, compliance and internal governance. It does not cover the technologies available for creating and implementing Data Leak Prevention (DLP) solutions in depth, but rather seeks to highlight the issues DLP is designed to solve and how these issues fit into a wider context of information security, compliance and risk.

The Mimecast Data Leak Prevention Best Practice Guide has specific information on the technologies used within DLP solutions and how these differ.

ABOUT THE AUTHOR

Dr James Blake
Chief Strategist, Mimecast

James holds a PhD in Information Security Management and an MA in Economics.

With over 17 year's commercial experience within the fields of information security, storage and clustering. James heads the strategy team at Mimecast to ensure technical leadership and positioning in its chosen markets.

EXECUTIVE SUMMARY

Security is a holistic issue; it's not your network you need to protect, it's the information inside that network and that means guarding against data leaks as well as network intrusions.

Email is where a significant amount of the knowledge, expertise and relationships within businesses is stored, although the combination of storage demands and unmanaged archives often make it as much of a problem as a resource. Email has become a critical business tool, but it is also the easiest way for information to escape from the confines of a business.

With 94% of organizations having no solution for preventing data leakage through email this represents a problem in an increasingly punitive regulatory environment, where leaks can incur fines as well as damaging your reputation and business relationships.

Turning email from a risk to a source of business value needs more than point security solutions; it requires an integrated approach that implements policies for governance, risk and compliance. Used correctly, an email Data Leak Prevention solution can correct honest mistakes, safeguard evidence in cases of malicious action, educate users in policy and best practice and help improve procedures that impact productivity and encourage inappropriate sharing of information.

Information security is a complex problem that can't be addressed by technology alone, but a successful technical solution can help by enforcing policy, supporting business processes flexibly and making it easier to manage staff without damaging productivity or adding complexity.

THE NEED FOR DATA LEAK PREVENTION (DLP)

Traditional Approach

The emphasis in many traditional security systems has been on blocking external threats that might get into the network, but in today's environment that's only half the story. Organizations need to stop the information in the network from getting out to the outside world, whether by accident, ignorance or malice. Intrusion protection systems analyse the content of incoming traffic for spam, inappropriate content, viruses and other attacks. Monitoring outbound traffic is less common and, where it is used, usually much less sophisticated. Indeed, many UK companies (38% in a recent Forrester survey) employ people to read or otherwise analyse outbound email as part of their job; 13% of UK companies employ people whose job is to do nothing but read and monitor email sent by employees. It's not an effective solution.

Accidental or Malicious Intent?

94% of IT managers in a recent eMedia survey commissioned by Mimecast, said they had no way to prevent confidential information leaving their network. Often the system is nothing but basic firewall rules designed to block access to specific services, which will miss some of the key routes through which confidential, commercially sensitive or other regulated data could be leaving the business. Although IM and social networking sites may get more of the attention, in fact it's email that is the worst culprit. This is rarely malicious and often it's not even deliberate. IDC's 2006 Security Survey[1] found that employee error was the fourth largest security issue behind only malware, spyware, spam and Forrester estimates that 80% of leaks occur because users aren't aware of data policies rather than because of any malicious intent. But deliberate or accidental, it is a significant problem.

According to Forrester[2], 66% of UK companies are concerned about email being used to disseminate company trade secrets or intellectual property and believe 12% of outbound emails contain a legal, financial or regulatory risk. 47% of companies in the survey have investigated a suspected leak of confidential or proprietary information via email in the past 12 months, 56% investigated a suspected violation of privacy or data protection regulations by email, 78% had disciplined an employee for violating email policies and 44% had fired an employee.

MOST COMMON INAPPROPRIATE EMAIL CONTENT

- **30%** Adult, obscene or potentially offensive content
- **26%** Confidential or proprietary business information about your organization
- **17%** Personal healthcare, financial or identity data which may violate privacy and data protection regulations
- **13%** Valuable intellectual property or trade secrets which should not leave the organization
- **14%** Don't know

Source: Forrester Consulting

Human Error

How often have individuals accidentally replied to all instead of simply replying to the sender? And how often was the message something the sender wished everyone hadn't seen? The auto-complete features in email clients like Microsoft Outlook save a lot of time, but they also make it easy to accidentally send a message to somebody outside the company when it was meant to be sent to a work colleague. Microsoft Word 2003's Reading Pane and Microsoft Outlook 2007's attachment preview automatically display any tracked changes in Office documents that are made to the original draft; that's a time-saver for collaborating on documents, but it can be embarrassing if comments, corrected mistakes and changes of plan have been hidden rather than actually changed in the final version.

Sending attachments can reveal information employees didn't realize was in the file, from names of internal servers and printers, to the original version of an image in the thumbnail preview; as well as who opened, saved and edited a document, what a file was previously called and who it has been emailed to. Speaker notes in presentations and tracked changes in Microsoft Word documents can be hidden rather than removed. And while conscientious employees can easily remove all this metadata when they plan to send a file outside the company, that won't be done if the email is accidentally sent to the wrong address.

Borderless Business

Almost all employees from the receptionist to the CEO have access to corporate information and sensitive data that could harm the organization or prove useful to competitors. It's not always clear who information should be shared with as business relationships get more complex. If employees are working with a mix of OEM partners, channel partners, sub-contractors, outsourcing services and off-shore colleagues, an email exchange can easily turn into an accidental disclosure, especially if they use a mix of applications and access methods with different interfaces.

Mobile messaging devices keep employees in touch with colleagues and customers wherever they are. But constant connectivity also blurs the line between personal and business use. It is common for employees to be using personal email accounts for work-related messages and sending personal messages from their work email, which makes it easier to send an embarrassing description of their weekend antics to a key partner, or forward a sales plan to a friend who happens to work for a competitor.

Maintaining Employee Productivity

Sometimes the problem is employees deliberately sending information by email that is expected to travel by a different route, even when it's going to people who are supposed to see it. Automatically encrypting such information is one solution, but if employees are routinely resorting to email, this is often a sign that existing lines of business applications or business processes aren't serving their needs. The vast majority of data leaks come down to someone trying to get their job done, needing to find a way around an inflexible process and not understanding the security risks this can raise. As well as making sure those data leaks are blocked, being able to track who is trying to send unsuitable information by email is a valuable tool for understanding where productivity and employee satisfaction can be improved by revising tools and procedures.

While a majority of disclosures will be accidental, they can still cause businesses embarrassment or more serious damage. And one can't ignore the possibility of fraud, industrial espionage or malicious acts by disgruntled employees. Deliberate disclosure is far less common, but if it does happen it is far more dangerous to the business.

FORRESTER REPORT

- 66% of UK companies are concerned about email being used to disseminate company trade secrets or intellectual property
- 12% of outbound emails contain a legal, financial or regulatory risk
- 47% of companies in the survey have investigated a suspected leak of confidential or proprietary information via email in the past 12 months

DATA LEAK PREVENTION AS PART OF A WIDER PROBLEM

Information security isn't new. Businesses have always put in place tools and systems to prevent unauthorized access to critical business information. Often they've become part of existing processes and policies, and are used to help manage risk, to implement business governance, and to ensure regulatory compliance. Any DLP system put in place needs to be considered as a part of an overall information security policy, and integrated with existing systems. Deploying DLP tools alongside effective email hygiene techniques, continuity services, centralized policy controls and a central unified data store is one way of enforcing governance policies – whether they're internal company policies or policies required for regulatory compliance.

Information-centric Security

The result will be an information-centric security solution. Unlike traditional security models, information-centric security ties security policies to both stored data and to anyone who works with it.

The result is a flexible system that gives authorized users access to the information they need, no matter when, and no matter how. Information managed using this approach will always be secure and available – but only to the right user.

Risk Management

Managing business risk is becoming increasingly important – whether it's for compliance with general regulatory frameworks like Sarbanes Oxley, or with industry specific initiatives like Basel II. In all cases, information security is a key component of a balanced risk management approach. Balance requires an end-to-end solution, and this means that DLP systems must be aware of the contents of any document, along with who can use the information it contains – and just how, when and where they can use it.

The result will be a mix of risk management policies and solutions that enforce three key information security tenets: confidentiality, integrity and availability.

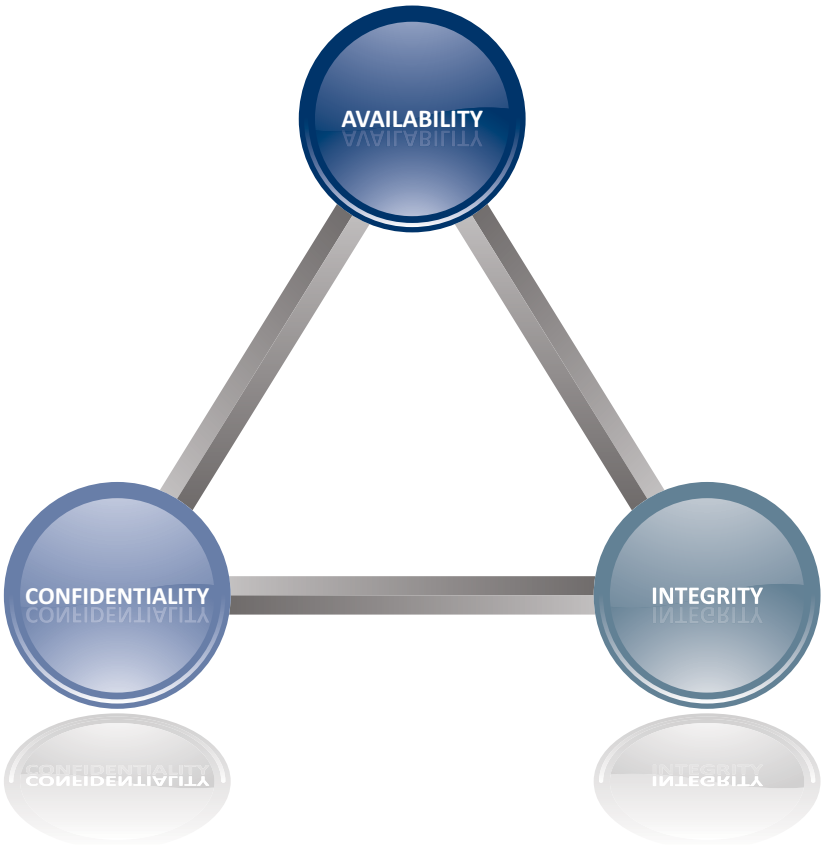
Information-centric security ties security policies to both stored data and to anyone who works with it.

Implementing an effective governance process is a key part of any DLP strategy, as any governance body responsible for compliance will also be responsible for ensuring data confidentiality. A single governance solution also simplifies setting organization wide information management policies that can be enforced across business processes. It's important to remember that any solution needs to be as simple to use as possible, and preferably automatic, as only a small proportion of the user base will be technically aware. The lessons of many failed CRM and ERP deployments are important, as any solution deployed must avoid adding complexity to existing business processes. The result should be a DLP solution that's easy to deploy and manage, easy to use and makes it easier to comply with policy.

Cornerstones of Compliance

Key features of any solution should be role-based access control, effective encryption and a well-defined audit trail. The combination of these features will help maintain the confidentiality of data – especially when implemented as part of an information-centric security solution. They also form the foundation of any DLP service, helping build a mix of solutions that assist in controlling the organization's overall compliance and risk management. It's important to remember that along with governance, risk management and regulatory compliance, these tools are more than just another set of technologies: they're essential business requirements.

CORNERSTONES OF COMPLIANCE



THE COSTS OF LEAKAGE

Regulatory Environment

In the past, a business might have worried about the threat of confidential information reaching a competitor or the embarrassment of letting a customer see unflattering comments about them made by its staff. Today's regulatory environment makes the consequences of data leakage severe, whoever sees it. The Data Protection Act, HIPAA, The Companies Act Combined Code, the Financial Services Act, Sarbanes-Oxley, EuroSOX, MiFID and GLBA all mandate the confidentiality of information and, therefore, the prevention of leakage.

In some sectors these are complemented by a whole raft of additional governance requirements set out by industry bodies and business partners like The Law Society and the Payment Card Industry.

The Data Protection Act in particular requires that organizations prevent the disclosure of any personal data stored by the business and the Payment Card Industry's Data Security Standard requires that if a business handles payments by credit card (or just store the card information) then all outgoing communications must be screened for credit card data. The Financial Services Authority fined Nationwide Building Society £980,000 in 2007 for losing a laptop with 11 million customer details, but this year it also fined a stockbroking firm for having poor security controls and inadequate protection for client details even though no information had been lost or stolen[3].

Losing Confidential Data

A fine isn't the only way letting information out can cost businesses dearly. Confidential information is confidential for a reason: sending a press release about new products out before launch can ruin a marketing campaign and the disclosure of intellectual property can instantly destroy a competitive advantage. Revealing confidential information about a partner can lose business: Hertz Global Holdings dropped Deutsche Bank from its underwriting team after "several emails" discussing its imminent $1.5 billion initial public offering were inadvertently sent by the bank to about 175 institutional clients[4].

Reputational Risk

In a world where customers and partners have many choices, reputation and customer service are ever more important. An internal email that reveals an individual employee's attitude towards a particular customer can be construed as corporate policy if revealed to the outside world – and if that attitude is uncomplimentary, it could be very embarrassing. Inappropriate language and offensive jokes paint a poor picture of the business, even if it can point to policies that show the behavior contravenes them.

The Financial Services Authority fined Nationwide Building Society £980,000 in 2007 for losing a laptop with 11 million customer details.

And simply letting out information that ought to be kept secure makes companies look careless and inefficient. After a flood of personal data exposures throughout 2007, 90% of British consumers believe organizations are failing to keep their personal data secure, according to an SMSR survey[5], and as many as 94% are concerned that organizations are selling their personal data without permission.

Enforcement of Law

Even Marks & Spencer, a British institution with an enviable reputation among customers, was placed under an enforcement notice from the Information Commissioner due to data leakage from an unencrypted laptop[6].

At the time, that was the only sanction available but in light of recent data breaches, the Office of the Information Commissioner has gained new powers under the Criminal Justice and Immigration Bill to impose fines on organizations that deliberately or recklessly breach the Data Protection Act[7]. This applies to all businesses, not just those covered by industry-specific regulations.

The ICO has also proposed that knowingly and recklessly flouting the Data Protection Act should be a criminal offence and asked for the right to inspect operations that process personal data, which it can currently only do with the consent of a business, and the Ministry of Justice is currently undertaking a consultation on those inspection powers[8]. The regulatory environment is becoming more punitive as the scope of regulations widens, making it more important than ever to follow best practices for protecting any customer and employee data held within the business.

THE REGULATIONS:

- HIPAA
- Data Protection Act
- Financial Services Act
- MiFid
- Sarbanes-Oxley
- The Companies Act Combined Code
- EuroSOX
- GLBA

THE COMPONENTS OF A DATA LEAK PREVENTION SOLUTION

DLP may appear to be just another buzzword, but it's actually a mix of well-understood security techniques and tools. The underlying components of DLP solutions aren't new, and have been around in various forms within the information security industry for years.

What we now call DLP brings together these technologies and adds a specialized policy engine. While the features aren't new, what has changed is the attitude of companies, along with an improved understanding of the threat and the environment.

DLP solutions can be classified as:

- **Solutions that provide host-based protection**
- **Solutions that offer network-based protection**
- **Products that are designed around DLP**
- **Products that solve other problems but have DLP features**

There's no truly safe place for data. It's at risk when it's stored in files, when it's being used by applications, and when it's moving around private and public networks. That's why there's no one-size-fits-all DLP solution, and a mix of host and network-based DLP solutions are required.

DLP Solutions

Host-based DLP solutions run on desktop PCs and servers, and aim to prevent unauthorized copying of data. Using these tools, data cannot be transferred to USB sticks or burned to a CD-ROM – and even if data escapes through the boundaries it's protected by strong encryption. Encryption is an important part of the host-based DLP story, as it helps reduce the risk of data leaks through stolen laptops or mislaid USB memory devices. Without the correct keys encrypted data is useless, and attempts to retrieve the information stored in files are uneconomic.

Network-based DLP solutions sit in the network and monitor traffic looking for protected data – preventing the transmission of unauthorized data into the wider network. Often used to implement regulatory compliance, network-based DLP systems are typically installed at network boundaries, and build on familiar firewall platforms and techniques. Policy-enforcement rules monitor network packet content, and ensure that protected information only routes between authorized recipients and systems.

DLP products focus purely on the technology of DLP, and often implement strict rules that are hard to manage in the context of a modern flexible business.

Encryption is an important part of the host-based DLP story, as it helps reduce the risk of data leaks through stolen laptops or mislaid USB memory devices.

Complexity of Integration

The result is an island of protected data, where as soon as information leaves the boundaries of the DLP environment it becomes unprotected and unmonitored – putting the business as much at risk as if it had no DLP solution at all. Integration is a key issue, and standalone DLP systems can be hard to combine with other security systems, increasing the complexity and reducing the effectiveness of any overall information-centric security policy.

DLP features can also form part of a point product, such as an anti-virus or End Point Security tool, or they can be a feature within a much larger multi-faceted governance, risk and compliance solution. Point products may help solve some problems, but integrated solutions have the added advantage of bringing together information from multiple systems, giving a clearer view of just what's going on in the network and within business processes.

Holistic DLP Solution

Look for a solution that allows the implementation of policies and procedures fully rather than dumbing them down. The result should be a holistic solution that avoids having to bring all policies down to the lowest common denominator of what one point solution can support. One can increase governance by catching internal email leaving the organization, or reduce operational risk by removing credit card numbers from messages – with the added bonus of increasing regulatory compliance. While it's still necessary to manage the integration of specific solutions to minimize overall risk, this is much easier to do with business-focused services or solutions than dozens of technology-focused enablers.

Solutions also need to consider business continuity – and any implementation needs to cover all aspects of security and document management in order to maintain governance, risk management and compliance policies. A continuity system for email must also cover continuity for archiving, anti-spam, anti-virus and DLP. The resulting systems should provide a unified framework for managing policy, provisioning rules and a reporting interface for all aspects of governance, risk and compliance around the specific business issue the solution is trying to solve. For instance, an email governance, risk and compliance solution will incorporate hygiene, policy, continuity, retention and discovery. Using a DLP solution, the same policy for the confidentiality, integrity and availability of the data will be applied across the entire organization for the data's entire lifetime.

DEALING WITH DATA LEAKS VIA EMAIL

The easiest way for information to escape from a business is the way that most of us exchange information legitimately every day: email.

Because email is at the heart of so many business workflows and internal processes, it's very common for it to carry sensitive information. That's all well and good, as long as the email stays internal, but it's easy to forward a message inappropriately (or maliciously). Detecting and preventing that is one key part of an email DLP system – but it's not the only important feature.

Email persists more than many other forms of data. If a user works in a line of business application or follows tasks in a workflow, unless they specifically choose to create and save a report, the information involved stays in the application and is both protected and updated automatically. The information in email stays on the user's system so they can refer back to it, as long as they or the business' email policies determine. That's good for productivity and business intelligence, but if the information is left on user systems it's a risk as well as a resource.

Email Growth Challenge

The explosion in email volume and size causes storage demands that IT managers struggle with on a daily basis and many companies implement draconian mailbox restrictions, with rolling 30-day deletions. Users want to keep their emails longer than that and messages often need to be retained for compliance purposes; an email archiving solution is a better approach than leaving users to create local PST archives that can't be used for discovery and can't be protected if a laptop is stolen or compromised.

DLP systems need to integrate with email archives as well as with live email servers to fully support retention issues.

Email Security and Hygiene

Email hygiene requires a holistic view of DLP, including anti-spam, anti-phishing and anti-malware technologies. It's not enough to think about blocking incoming spam; outgoing replies or links have to be blocked as well. Spammers have moved from peddling goods to directing users to 'linkfarms' (web pages with hundreds of links to pages containing malware). These attacks are targeted through phishing techniques that trick users into thinking they're seeing a legitimate message from a bank or a friend. Trojans, keyloggers and other malware let the spammer transfer confidential information out of the organization and use an organization's computing resources to send more spam.

HOLISTIC EMAIL LIFECYCLE

Detect Email Loss

Detecting a potential data leak is only half of the problem; the other question is how to respond to the incident. This is where governance, risk and compliance policies are put into practice and close integration is key for this. Most standalone DLP solutions offer only one option – to hold the data in a queue and inform an administrator, the recipient, the sender or any combination of these parties that the message is being held. But while that makes life easier for the writer of the message, it doesn't help enforce company policy correctly. Supposing the sender has malicious intent? They have just been informed that the business is aware of their message and they can now work to cover their tracks and look for other ways to extract the information. Company policy to managing data leaks will vary depending on what information and which employees are involved, and the technical solution used should allow for implementation in a granular fashion, but through a single policy interface for simplicity (and where there is no defined company policy, it should implement industry best practices by default).

Investigating Data Leaks

Whether the attempted leak is deliberate or accidental, it can't be investigated fully without seeing it in context and being able to see details of other email conversations to find out who the message was going to and whether there is possible collusion or a history of too much information being passed.

That means the DLP system needs to be integrated with the wider systems that manage governance, risk and compliance issues. That integration is also needed so that the system can preserve the integrity of the evidence while investigations are carried out.

If the leak proves to be accidental, it's vital to have the emails and metadata available to work through the issues with the employee or decide how to refine the business process in question to avoid future leaks. And if it proves malicious, it's essential that the message is forensically preserved so it's available to use in an internal disciplinary proceeding, civil or even criminal prosecution as appropriate.

Any emails and metadata from the DLP system will need to be of evidential quality and held in a system with strong chains of custody. Prosecutions for deliberately leaking confidential information are rare and the embarrassment of a public court case will account for some of that. But according to Computer Emergency Response Team (CERT), in 62% of the cases that are not successful the problem is insufficient evidence and not being able to identify exactly who was involved in passing the information. That's a problem that can be solved by integrating DLP tools with existing directory services and governance, risk and compliance solutions in a way that preserves the quality of the evidence and allows policy to be followed as the incident is dealt with.

Appropriate Policy

DLP isn't about stopping employees from talking to colleagues, partners and customers and it isn't about making it harder for them to do their job. In fact a well-designed system should make their lives easier by catching honest mistakes and dealing with them automatically, and it should do it according to the policies the business lays down.

If potentially sensitive information like credit card numbers, sort codes, National Insurance Numbers or Social Security Numbers are found in an email, these can be changed into placeholders so that the mail doesn't have to be blocked. Messages containing sensitive information that are going to someone on an approved list of contacts can be automatically encrypted without the user having to learn a complex procedure. Disclaimers noting that a message or attachment is confidential and should not be forwarded form an enforceable contract, but plastering them onto every message can make the sender look paranoid or self-important; attaching them automatically when appropriate gives a much better impression, especially if they adjust automatically to suit the content of the message.

Where policy is to allow inoffensive personal email messages, these can be detected, branded with the term [PERSONAL] in the subject line and sent without the usual company logo, to ensure they can't be mistaken for official communications.

Correcting Behavior

Automatic encryption, redaction and remediation prevent accidental data leaks and notifications can be used from the DLP system to educate users on company policy and the procedures they should be following. Enforcing these in a way that helps users rather than penalizing them will make it easier to change attitudes. And while users who ignore policy is as much a management issue as a technological one, the deterrent effect of good policy and procedure enforcement will help minimize abuses and any 'shortcuts' taken by employees. As well as detecting data leaks, this helps develop a self-correcting mechanism for bad business processes and poor procedural compliance.

Some issues can't be dealt with automatically; depending on the information it may be best to have the sender look again at the message – or have their manager look at it instead. A DLP solution needs to support rules and policies that can specify what actions to take in different cases, so that potential breaches can be managed and governance and compliance procedures can be followed.

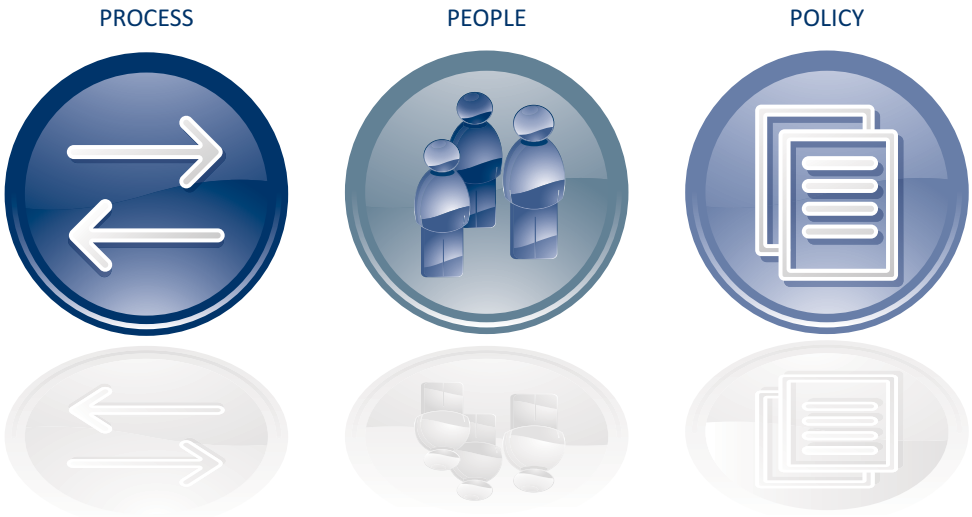
People, Process and Policy

The data protection problem goes beyond what can be achieved with technology alone; policy, processes and people management are all key. No technology can prevent every leak or ensure that nothing ever leaves the company that should be contained. But the policies on what information should remain inside the business, and the DLP system chosen should implement them to reduce accidents, catch malicious behavior and cultivate a culture of taking care of information.

And DLP offers benefits beyond pure security as well. It can help uncover where employees are endangering security because business processes aren't flexible or don't match the job that actually needs to be done. Information classification is becoming more important as companies seek to mine the wealth of knowledge, expertise and relationships within a business; the same tools that help prevent key data from leaving the business can help make more use of it inside the business too.

---

3 P's OF DATA PROTECTION



NEXT STEP

Mimecast provides a complete email lifecycle management solution designed to provide the best platform to manage the governance, risk and compliance issues related to email.

By integrating security and hygiene, policy, continuity, retention and discovery services through a single management and reporting interface customers can get an instant snapshot of their most critical communications platform.

The Mimecast offering is Software-as-a-Service that can be deployed in hours, providing a unified governance, risk and compliance solution and replacing dozens of independent point solutions.

SOURCES

1. IDC Enterprise Security Survey, 2006: The Rise of the Insider Threat
2. Forrester Data Loss Prevention in Today's Enterprise 2008
3. FSA fines Nationwide £980,000 for information security lapses
   http://www.fsa.gov.uk/pages/Library/Communications/PR/2007/021.shtml
4. Hertz Global Holdings drops Deutsche Bank
   http://www.iht.com/articles/2006/11/08/business/ibrief.php
5. SMSR Report on Information Commissioner's Office Annual Track 2007
6. ICO takes enforcement action against Marks & Spencer
   http://www.ico.gov.uk/upload/documents/pressreleases/2008/mands_en_final.pdf
7. ICO welcomes new powers to fine organizations for data breaches
   http://www.ico.gov.uk/upload/documents/pressreleases/2008/criminal_justice_and_immigration_act.pdf
8. Ministry of Justice: Consultation on inspection powers and funding arrangements of the Information Commissioner

ABOUT MIMECAST

Mimecast Services for Microsoft Exchange, Outlook, Windows Mobile and Blackberry provide enterprise level email continuity, archiving and security for any size of company. 'Unified Email Management' requires no hardware or software, integrates with an organization's existing IT, offers complete control to the IT administrator and takes just hours to set up. Every day Mimecast takes care of millions of emails and documents for thousands of companies around the world. Founded in 2002, Mimecast has operations in North America, Europe, South Africa and Offshore.

mimecast
unified email management

North America
275 Grove Street,
Building 2, Suite 400,
Newton,
MA 02466
tel: +00 (1) 800 660 1194
email: info@mimecast.com

UK & Europe
2 - 8 Balfe Street,
Kings Cross,
London,
N1 9EG
tel: +44 (0) 207 843 2300
email: info@mimecast.com

South Africa
Morningside Close Office Park,
Block G, 1st Floor 222 Rivonia Road,
Morningside
tel: 0861 114 063 (S.A local)
tel: +27 (0)112 585 300 (intl)
email: info@mimecast.co.za

Offshore
The Powerhouse,
Queens Road,
St Helier,
Jersey, JE2 3AP
tel: +44 (0) 153 475 2300
email: info@mimecast-offshore.com

WWW.MIMECAST.COM