



Policy-Based Content Security

An IDC White Paper Sponsored by Clearswift

Analyst: Thomas Raschke

Introduction

Information, content and knowledge within an organization probably represent its most important assets. However, how assured are you that this information is secure, and is being represented professionally, and you know where and how it is being used?

Take, for example, four business critical types of content.

- Your customer records
- Your employee records
- Your electronic communications (email)
- Your Boardroom business plans

If any of this content is used inappropriately, is damaged or stolen - your intellectual property, your brand, and therefore your competitive edge would be significantly diminished.

The need to protect and preserve an organization's information has never been greater, as these corporate assets are becoming increasingly exposed with online channels being used for business processes and information is stored electronically.

With this growing pressure, coupled with the increasing amount and complexity of legislation being passed on how organizations handle content and electronic data, companies are being well advised to implement a Content Security policy.

Why Content Security?

- To protect against threats: malicious intruders, and leaks to competitors/financial community (confidentiality).
- To improve productivity and create a trusted environment in which to conduct ebusiness and partner communications.
- To conform to increasingly complex and numerous legislation requirements.
- IDC predicts the 9.7 billion messages sent worldwide every day in 2000 will soar to 35 billion everyday by 2005.

 **IDC**
Analyze the Future



CLEARSWIFT™
CORPORATION

The use of electronic communication, email, by companies to facilitate business is widespread. It is rare these days to find a business not using email. Some 9.7 billion emails are exchanged on an average day, but only an estimated 25-30% of all companies have an enforced and communicated email policy in place. However, it is rare to find a company without plans to implement an email system in the near future. Email has changed the way in which business and personal communications take place. But email is not a panacea, in fact it has the potential to harbor great ills and, if left unchecked, can lead to dissatisfied customers, lost revenue, costly remedial action, bad publicity and legal liability. For example, the sharing of unauthorized information — either by accident or design — is a danger for any organization.

Likewise, the Internet has become an indispensable tool for employees, who — like it or not — use it both for work and non-work-related purposes. For example, researching work related information such as a competitor's news site for new product releases must be tolerated. However, social interaction in chat rooms, using web-based email services like Hotmail, and even frequent visits to news sites decrease productivity and network bandwidth dramatically. IDC estimates that cyber-loafing accounts for 30% to 40% of lost worker productivity.

Surfing non-work related web sites such as pornography or racially explicit sites could all put corporations at risk. A hostile work environment could easily be created, with sexual or racial harassment lawsuits following. Similarly, cases involving email misuse have resulted in legal liability lawsuits with multi-million dollar penalties. Demand for Content Security products is thereby driven by CEOs, corporate lawyers and human resource managers looking to block employee access to pornography and otherwise offensive material, typically as part of a broader, Internet and email policy.

Essentially, Content Security allows employees to use the Internet and Intranet email and web safely and effectively. Content Security is imperative to preserve the integrity of the brand and to maintain and increase productivity — hence achieve a positive return on investment — by addressing all of the previous communication issues effectively. Content Security thereby helps organizations protect their network and business integrity.

This White Paper written by IDC and commissioned by Clearswift, examines the importance of securing and protecting an organization's corporate resources. The White Paper identifies the issues organizations should consider, highlights the legislative changes taking place and provides insight into how companies can utilize security both as a protector and as a business enabler. Through a series of case study examples, leading companies illustrate how they have overcome the challenges they faced in protecting their organization's assets.

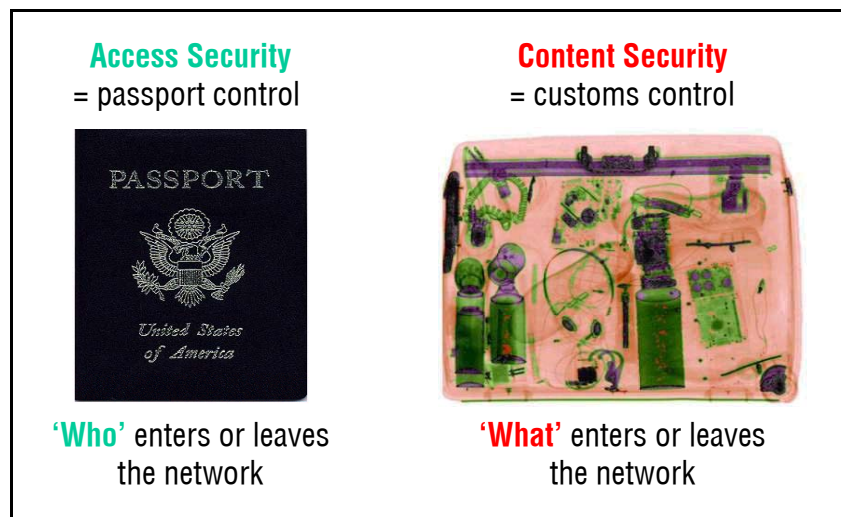
Definition

IDC defines Secure Content Management (SCM) as technologies that include Internet Access Control (IAC), Employee Internet Management (EIM), Email Scanning and Malicious Mobile Code (MMC) that work alongside Antivirus tools (AV). In a broader sense, firewalls also secure content as they check who enters the network.

What Is Content Security?

A frequently espoused, but still valid definition of Content Security is in the analogy of the traveller at an international airport. The duties of the firewall can be likened to a passport or immigration officer, namely concerned with the question of “Who” is authorized to enter or leave the organization. Content Security, by contrast, assumes the role of the Customs Official or X-Ray scanning machine, controlling “what” can be moved into, out of and around the organization.

Figure 1
Content Security Analogy



Source: IDC, 2001

Content Security can best be explained as a means of managing valuable content. This paper focuses on policy-based Content Security, defined as a solution that allows organizations to analyze, protect and manage their content in email and other communications over the Internet, in accordance with security policies developed to govern the flow of information within, to and from an organization. Content Security is the sum of parts of a series of technologies which includes Email Scanning, Internet Access Control, Employee Internet Management, Malicious Mobile Code and also antivirus tools (AV), URL filtering and firewalls — which, individually, all play a vital part in traditional security configurations.

Whereas Content Security solutions protect all points of entry to a corporate network – i.e. internal mail (Exchange, Notes), inbound and outbound mail (SMTP), Web-based email (HTTP) and other HTTP and FTP content threats – AV and firewalls fail to do so. Antivirus tools and firewalls certainly play a part in a security strategy, but they cannot protect you from all the content threats. Antivirus tools are essential for stopping viruses but they cannot prevent embedded or disguised threats in emails and attachments. Likewise, firewalls are great at providing access control — who can and can't enter the network — but they do not protect against harmful content coming in and out. Without a Content Security solution in place, organizations relying solely on antivirus tools and firewalls to provide Internet, email and web security, are seriously compromising their business and network integrity. In essence, AV and firewalls are necessary, however, they won't do the whole job — a network needs a Content Security solution to provide real security.

Protecting Confidentiality

Accidental, or deliberate, confidentiality breaches are an increasing threat to organizations and can have a devastating effect on customer and market confidence. Imagine the embarrassment if — by accident or not — executive salary information should leak out of a corporate network — as happened to a large company in the UK in 2001. Content security solutions protect you from these kinds of incidents.

Protecting company-confidential information is a growing concern in many organizations. The informal nature, and ease of use of email, contributes to both deliberate and inadvertent circulation of information. Alarming amounts of confidential corporate data can easily be sent out of the company email system at the stroke of a key, with no hard evidence such as a paper trail or a floppy disk to show for it. In many cases this is without realizing that the document contains information that should not be circulated. Such confidentiality breaches can have a devastating effect on customer and market confidence — whether deliberate or accidental. Consider the impact of a leaked email detailing your customer records, or your organization's strategic plan for restructuring the business.

Email scanning products can check inbound, outbound and internal messages for confidential data, excessive file size, and prohibited content. They search for keywords and phrases, junk email (spam), profanities, banned file types, oversized data packets, and malicious code. Given the continuing drive toward public-key infrastructure (PKI) and ecommerce, these products must also be able to perform content analysis on encrypted and signed email.

Although the paperless office is far from being a reality in most office environments today, roughly one third of all documents are available in an electronic format only. This makes them both more accessible and more likely to be easily transmitted to recipients with no access rights to these files.

Corporations may also want to block the use of instant messaging type services, by which confidential corporate data can be sent bypassing email screening. Also, they may not want other entities to use data mining techniques to track sites that their employees have visited. In general, organizations should consider how their own information is stored and also who has access to it, especially as information is now more likely to be saved in a format that is easy to send over email.

Case Study: AT&T - Providing Customers with Secure Networks

Ensuring the security of a company's infrastructure and assets is a high priority for global organizations. But for AT&T, security is not just about its own infrastructure and assets - it is also about protecting the assets of its customers and ensuring the integrity of data being transferred over its network.

Maintaining its reputation as a market leader in the adoption and development of security solutions is vital to AT&T. "Security has always been a key part of AT&T's corporate ethos," says Mr. Bettam, AT&T's Infrastructure Consultant. As one of the world's premier voice, video and data communications companies, AT&T considers security as an integral part of its overall service offering to customers.

AT&T has taken a number of measures to protect its systems and has demonstrated that it has not yet been affected by any incidents. "Controlling the perimeter is a philosophy we follow, and we employ a number of solutions which prevent potential security threats from entering into our system," explains Bettam. These solutions have been implemented to support the company's security policy, which is communicated to all employees by the Human Resource Department. "As part of the induction process all new employees are made aware of the corporate security policy and its importance," said Bettam.

The ability to stop any potential security threat at the 'front door' rather than allowing it into the organization also results in reduced administration overheads. "Products like Clearswift MAILsweeper and Clearswift WEBSweeper allow us to funnel email and Web traffic through a central point or points to ensure that we can capture and manage any security breach in a controlled way," comments Bettam. Even a small security incident could cost AT&T a considerable number of man-hours to resolve, and have an adverse effect on customer confidence in the organization. "Even using conservative figures, each incident could cost several thousand dollars of resources," says Bettam, "it would also involve a large part of the administration team, which has an add-on effect on their normal duties."

For AT&T, being able to demonstrate to its customers that it has a very secure environment which protects the services it offers is a high priority.

Limiting Legal Liability

Corporate implementation of Content Security software was originally driven by legal concerns — at first in the USA. As the Internet became widely available in the workplace, adult entertainment sites were so frequently visited it created a significant legal liability. A hostile work environment could easily be created, with sexual or racial harassment lawsuits following. Similarly, cases involving email misuse have resulted in legal liability lawsuits with multi-million dollar penalties. Early demand for Content Security products was thereby driven by corporate lawyers and human resource managers looking to block employee access to pornography, typically as part of a broader, preemptive Internet access policy.

In November 2000, six Cable and Wireless employees were dismissed for sending offensive messages. The company's e-mail system had been largely unregulated and the content of messages between staff was unmonitored.

UK insurer Norwich Union, the Chevron Corporation and Dow Chemical have all faced litigation. Citibank and Morgan Stanley have also faced legal action from disgruntled employees who have been racially, or sexually harassed, by content contained in emails. These occurrences highlight the need for action, and responsibility by organizations, to implement a content management system backed up by a robust policy.

A further issue is that organizations are becoming increasingly liable for unlicensed copyright material on corporate servers, for example MP3 files and unlicensed software, which could lead to legal copyright damages being filed. Ultimately, the requirement is to block these downloads. Understanding the legislative situation is vital for organizations today. IDC has listed some of the key legislation for your reference at the end of this paper.

Traditionally, employers have been responsible and liable for the actions of their employees in the workplace. However, if an organization can demonstrate a 'duty of care' to reduce unacceptable employee activity, then it could minimize its potential for liability.

The above mentioned scenarios and other similar ones are likely to play out with increasing frequency as more companies suffer public outages and thefts as a result of security breaches. And they raise a crucial question that the courts have yet to decide: When information security fails, who's to blame? Obviously, the hacker is at fault, but it is only a matter of time before judges and juries have to decide whether companies, that are victims of a security breach, can be held liable for having inadequate security. Decision makers need to understand the complexity of this legal/security minefield and have the Content Security solution for their company— and thereby protect their business not only from external and internal offenders, but also from legal actions that may follow in the offenders' destructive wake.

Enhancing Productivity

The following chapter features a thorough analysis of the importance, benefits and business implications related to securing content by confronting corporations with the dangers to their business and network integrity.

Business Integrity

Table 1
Top Words Entered in Search Engines for 17th October 2001

1. yahoo	6. anthrax
2. yahoo.com	7. sex
3. hotmail	8. halloween costumes
4. hotmail.com	9. jokes
5. AC-130	10. lyrics

Source: Wordtracker.com

Lost productivity. Due to inappropriate use of a company's email system, lost productivity is becoming a growing area of concern. How organizations react to non-work related web browsing will vary from organization to organization, and many will allow employees some time for personal use. However, they may not want their employees to spend excessive time on non-work related activities, such as managing their stock portfolio, or shopping online. The current big time-wasters are web-based email, sport sites, shopping and window-shopping, on-line magazines, and share trading sites (October's top ten words entered in search engines are shown in Table 1). To counter loss of productivity through 'cyber surfing', a content management solution, that restricts web access in line with an enforced company policy on non-work related web browsing, needs to be in place.

Non-business emails. These are a time-consuming distraction that can hinder an employee's productivity. Personal emails such as jokes, chain letters, pictures, and games affect not only the productivity of the sender and recipient, they also affect business communications of other corporate users, by clogging servers, workstations, and Internet links.

Actions by disgruntled employees. Legal cases brought about by employees; or spam and spoof attacks can all lead to adverse publicity for an organization. For example, cases of email-related dismissals which come back to haunt the employer are now commonplace. More often than not, the inappropriate usage of email results from either lack of awareness of the potential security threats that email poses, and/or lack of communication between the employer and employees, about the appropriate and inappropriate use of the system.

The long-term consequence. The overall damage of any threat is to the reputation of the organization. The resulting negative publicity could damage company brands, reduce consumer confidence, and even cause share prices to collapse. Again, legal and financial resources are tied up as part of limiting these negative results. Content Security products 'foresee' and protect companies from the above issues.

Mistakes. Not all information leaking through corporate walls, however, has been maliciously communicated. The prevalence of email, and the lack of controls in place in most organizations, mean that mistakes are commonplace, leading to the accidental distribution of sensitive information. The informal nature of email communications means that employees often fail to realize the significance of the document. This means that traditional terminology — such as quote, offer etc — is as important via email as in a printed document. For all organizations, it is the company directors that are legally responsible for the actions of their employees whilst at work. Furthermore, Content Security educates organizations to protect corporate information and help maximize the investment they have.

IDC estimates that more than 50% of all Internet porn traffic occurs during 9-to-5 working hours.

Pornography. By checking the content of each website visited, content security products take the simple blocking of a database of URL addresses (which depend on being updated literally on an hourly basis) a step further. Pornographic images, offensive language, or even sound and video archives on the Net can be identified and thus consequently banned for employee use.

Theft of Data. Another way to obtain the data is to send a mail message to a recipient, which appears legitimate — except that during the process of opening and reading the message, a hidden code is secretly obtaining information and sending the data outside of the organization, We call this threat a “cyberwoozle”. A recent example of this was the SirCam virus, which would send out documents found within the “My Documents” folder of Microsoft Outlook, via the viruses’ built in mail routines, completely bypassing security. It certainly can be that the victim company may never know that it has been ‘woozled’.

IDC research shows that 95% of respondents would not think to question the origin of an email purporting to come from their manager or supervisor.

Spoofing. An increasing phenomenon is email spoofing, which disgruntled employees, if bitter enough, may want to use. Spoofing is a usually malevolent email where the identity of the sender is disguised to appear that it has come from elsewhere. It can have disastrous consequences in terms of loss of trade secrets, betrayal of client confidentiality, or theft of data. While the basic checks can be made on the message, such as message source, the only real way to authenticate that the message really did appear to come from the originator, is with digitally signed messages.

Network Integrity

Corporate users are either blissfully unaware, or completely ignorant, of the network bandwidth consumption associated with downloading large graphics files, playing online games, or accessing streaming audio/video. The large file transfers can degrade network performance for all users.

As people use graphics and multimedia more for documents and presentations, the size of the average email will increase. An average 3-5 minute MP3 music track is around 3-5Mb, while a single movie clip in MPEG format would start at around 20-30Mb.

Consider a company of 100, with every employee having downloaded and stored just one of each – a MP3 or MPEG file - during the period of one year. Reality exceeds these amounts by at least 50%!

Do you know how many non-work related files are entering your company? Content security solutions enable an organization to monitor this situation.

When these large messages are sent internally or externally, they will consume precious bandwidth. It may be sensible to consider sending large messages at more appropriate times when there is more network capacity, otherwise the legitimate business users will suffer poor performance. Unsolicited commercial email entering the organization can have a calculable effect on productivity. While uninvited email may only seem like a few messages, per person, per day, there are costs associated with:

1. Time spent reading the message;
2. The bandwidth consumed during the delivery;
3. Data storage on the file server.

Calculate the costs above for an individual, then multiply this number by the number of employees and — you'll see that even a single piece of Spam mail carries a cost.

Content Security's manageability and reporting capabilities allows the corporate IT department to explain easily poor network performance by identifying employees that abuse corporate Internet privileges with MP3 downloads; streaming video; stock trading; shopping; online gaming; and other activities.

It enables corporate policies to be set up to provide groups of users with varying allotments of personal Internet time and bandwidth. Therefore, a policy can be set to monitor overuse only. Also, the internal charge back for network costs can be fairly allocated to specific cost centers.

Meeting Legislation Requirements

Government regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) in the USA will require companies to adopt monitoring, blocking, and reporting capabilities to comply with corporate policies and regulatory guidelines. Although HIPAA is focused on the health care industry (physicians, hospitals, and health care insurance providers), the financial industry is also grappling with a parallel set of privacy mandates (GLBA), and we believe that both sets of regulations will have an impact on other industries as well.

IDC believes IAC and Email Scanning software will enable corporations to protect intellectual property, and networks, by automatically applying content filtering, access control, and virus scanning to all internal, plus inbound and outbound messages. With these technologies in place, financial and healthcare institutions can safely exchange sensitive information, while ensuring compliance with government regulations.

Organizations are increasingly being affected by legislation of countries in which they operate, and which legally bind organizations to taking responsible for the content held on and

passing through their network. Again, implementing a Content Security solution that ensures that legislation is not breached is imperative to avoid legal liability.

Security Policies

Content Security is about defining an email and web employee usage policy to cover what is, and is not, acceptable content in email and email attachments, and Web uploads and downloads. Policy-based Content Security relies on an organization being able to **establish** an acceptable email and web usage policy; **educate** its employees on the policy; and **enforce** the policy with a suitable software solution. In brief, it means an organization needs to be able to understand and manage what data has been moved, or accessed by whom, and where it has been moved.

The first step is to establish an email and web-usage policy. Such a policy clearly defines what is acceptable and unacceptable business and personal use, and enables a business to achieve return on investment and increase business growth. A policy helps create a trusted environment so that employees can communicate freely, and securely, in addition to opening up parts of their networks to partners and clients. Crucially, this environment allows companies to exploit new channels and markets. This can lead to business improvements and a return on investment. Costs are lowered, as opening up networks reduces the cost of purchasing, and the safer environment means that companies will not have to compensate clients for incidences such as loss of corporate information. Business revenues can be improved, as they can take advantage of new sales channels, and in the long term, companies will see the benefits of an improved reputation and brand.

It is important that an Internet usage policy offers employees guidelines on what they should and shouldn't be using the organization's Internet connections for. This should be driven from the top down, and seen as part of an overall business security policy rather than something that belongs to the IT department — Content Security is a people problem, not a technical one. When defining such a policy, it should be remembered that threats are more likely to be internal than external, and are just as likely to be unintentional as malicious. Four key areas should be assessed when drawing up an Internet usage policy:

- How to protect information;
- How to maximize operational effectiveness;
- How to minimize corporate liability;
- How to protect the corporate image.

The next step is to ensure that all employees are educated on the policy, and the last step — but arguably the most important and the most difficult to do — is to enforce that policy. That means regularly communicating the policy to employees, monitoring email and Web traffic for potential Content Security breaches, and disciplining those who breach the policy. By effectively establishing, educating and enforcing policies, it not only means

In a 2001 survey, IDC found that although 83% of all European businesses have a formal security policy in place, most policies are supposed to provide safety by deploying antivirus tools (93%) and firewalls (74%).

A 2001 IDC survey indicates that enterprises are concerned with bandwidth consumption by unwanted or excessively large email files. Bandwidth problems rank #4 among email filter users' worries. Most users buy email filters and related products for increased security; followed by concerns for limited legal liability; increasing employee productivity; and conserving network bandwidth.

that organizations are less likely to suffer from Content Security breaches, but will be able to demonstrate 'reasonable due care' should any breaches become exposed.

Recent legislation is also driving companies to develop and implement policies. For instance, the Regulation Of Investigatory Powers Act (RIP) and the Lawful Business Practice Regulations within the UK decree that companies are permitted to monitor employees' communications to prevent or detect crime. However, businesses doing this could be infringing the new Human Rights Act (HRA) in Europe, which codifies a person's right to privacy and private correspondence. Although it will make it easier for the State to monitor and prosecute criminals, RIP also enables a company to legally monitor its employees if it suspects them of misusing the Internet. The HRA and the RIP seem to be the main area of contradiction. Companies, however, can clarify this, by obtaining employees' consent to intercept or monitor their use of email and the Internet. This should be laid out in a company policy, detailing the parameters for email and Internet usage which employees are then educated on.

Business Enabling

Content Security should be considered a business enabler, enhancing the brand and promoting trust in the company. This includes making the Internet a trusted environment in which to conduct partner and customer relations and ecommerce via the web, extranets and intranets.

Incoming emails at a company's helpdesk, for example, can be automatically checked for certain words or phrases - e.g. product brochure, contact information, annual report, etc. All email requests can then be automatically categorized and re-rooted to the respective point of contact within the organization. Likewise, emails containing specific requests can trigger an automated response email, with the requested information, which could read "We have attached the information you requested on product xyz..." Both examples display strong cost & time saving benefits that can be deployed within a Content Security solution.

Content Security is not a stand-alone solution and corporations of all sizes and shapes must live up to their responsibilities regarding the e-ecosystem. Business partners such as suppliers, resellers, attorneys, and external PR companies should be educated about likely problems resulting from not having a comprehensive Content Security solution in place. Press releases communicated between HQ and the external PR agency, for example, can be interfered or altered.

Case Study: Symphony — Protecting Intangible Assets

The misuse of data and company equipment can have serious financial implications for an organization. The damage that a security breach can inflict on a company's reputation and brand image is something that cannot be readily quantified but the potential impact could have a long lasting effect.

Conscious of the need to maintain its reputation and brand equity, the Symphony Group, has put the security of its email and Web communications and transactions on the top of its list of priorities.

Based in the UK, the Symphony Group is a leading manufacturer of fitted kitchen, bathroom and bedroom furniture, with a turnover of over £100 million and employing over 1,300 people.

For the Symphony Group, tightening the security solutions in place and closing any loop holes has had a positive impact on the business, not only in terms of increased productivity, but also ensuring the integrity of the corporate image and general reputation of the business. As Craig Monument, Technical Manager at Symphony explains "we look at it from a border strategy — we try wherever possible to make sure that the perimeter is secure, so whatever happens on the inside, is relatively minor."

The Symphony Group has also noticed a reduction in administration time as a result of implementing perimeter control security solutions. "We lock down all desktops so employees can not make any changes or delete vital files, or bring in viruses. We have basically eliminated the possibility for them to sabotage their own machines, which has made things more stable and allows us to concentrate on more important IT issues," said Monument.

Recent virus attacks like the 'Melissa Virus' and the 'Love Bug' has shown that Symphony's security solutions are working and reaffirm the company's image as being security conscious. As Monument explains, "Clearswift MAILsweeper intercepted all of these viruses, which gave our suppliers and customers the confidence that we were not passing corrupt information or content onto others."

The Symphony Group conducts regular security audits to ensure a complete understanding of the implications on the business of any potential security breach.

The management of content as well as access is an issue. It is one thing to limit employees access to the internet ensuring that non-productive sites are not visited, however, employees may still be able to visit internet based email sites such as Hotmail because, in the companies eyes, the information coming in is not seen as 'risky'. However, sensitive information, such as company files, can still go out this way.

Table 2
Costs of Non-Business Internet Use and Spam

Costs of Non-Business Internet Use	Costs of Spam
A 1,000 employee company: <ul style="list-style-type: none"> • Every employee spends 1 hr online for non-business purposes = 1,000 hours An hourly wage of \$25 x 1,000 hours = <ul style="list-style-type: none"> • \$25,000 per day • \$125,000 per week • \$6.5 million per year 	A 1,000 user email network: <ul style="list-style-type: none"> • Receiving 39% SPAM based on 24 messages per day = 9 SPAM per day • 9 SPAM x 1,000 = 9,000 messages per day • 9,000 x 240 (approx working days) = 2,160,000 messages per year

Source: Coalition Against Unsolicited Commercial Email (CAUSE)

In this context, **flexibility** can be introduced to boost employee morale — for example, employers can allow employees visit websites for personal use within defined guidelines — e.g. Hotmail allowed after 6pm. However, confidentiality and security protection — and employee privacy — can still be maintained.

Case Study: Syntegra — Making Informed Decisions on Security

Organizations are faced with the difficult task of deciding what security solutions to implement to safeguard their systems from any potential security breach. This is made all the more difficult with the ever increasing complexity of the type of security risks which could potentially affect any part of a business.

For Syntegra, the systems integration and consultancy arm of BT, the main drivers for the company's current security solutions are very clear. As Mark Sanders, Head of Security explains, "the security solutions we have in place at the moment enable us to contain and reduce the risk of any potential security breach".

But with the increasing volume and sophistication of security risks, organizations like Syntegra, must constantly re-evaluate their security solutions and provide higher levels of protection. "Its about trying to keep the bad guys out," says Sanders, "we look at the risks we face and take a pragmatic decision on how we are going to counteract those risks".

The company uses firewalls at both the outer areas to protect themselves from the Internet and also internally to help segregate some of their networks. This is complemented by intrusion detection software both in front and behind the firewalls. Syntegra are concerned about content security and in particular what sites their employees visit on the internet and what gets sent out in emails. "If somebody spends all day just surfing the Net it is not an appropriate use of a company supplied resource. We are not getting the productivity out of that employee that we would like but also Syntegra's reputation is at stake because our name is associated with the various sites employees visit or what is contained in emails they send," commented Sanders.

Every organization faces the difficult challenge of anticipating a security breach but some will already have solutions in place to minimize the risk.

Cost Benefits

Estimates on the cost of information loss, loss of productivity, and damage to brand reputation vary hugely between companies for a number of reasons. There is a natural reluctance to acknowledge that 'intruders' have used email, and Internet, to access company systems. Then there is an inconsistent area of the law, where organizations are unsure if a crime has been committed, so intrusions go unreported. Adding to this fear is the fact that organizations themselves may fall foul of the law, for having failed to protect customer information. Many organizations even remain unaware that that information has been lost.

A Major North American Airline – Securing the Network

Information Technology security is something that is taken very seriously in the airline industry. It is of the utmost importance to have the right solutions in place, not only to protect against security breaches, but also to prevent deliberate intrusion by outside parties, with the aim of damaging a company's reputation.

Two years ago one of North America's leading Airlines was the target of malicious attacks from adult content spammers. "They were using us as a mail relay, and we were getting some embarrassing e-mail from people who were receiving this spam, and seeing our company name in the message header." explained the airline's Workgroup Applications Manager. "So we installed Clearswift MAILsweeper, and this prevented these people from using us as a relay."

Brand reputation is something that is hard to quantify in monetary terms. However, when viruses attack and affect the IT infrastructure, the costs can be counted. The airline has spent much time and effort, especially in light of the virus threats of recent years, shoring up their defences and ensuring that risks are minimized. This is particularly noticeable in the e-mail environment where there had previously been some significant impact.

"After the 'I Love You' Virus we estimated \$312,000 in technical effort was needed to get the systems back up and running again, which didn't even count productivity losses," said the respondent. "We were down for almost two full business days. During that time we had around 50,000 e-mail users in the company pretty much standing around in the hallways, unable to do anything. When we tried to quantify the cost of that in lost dollars the case to invest in the software was compelling."

The e-mail outages have escalated procedures within the company to an extremely sophisticated level, so that there are now several lines of defence in place, both in the workstation environment on our internal network, as well as the quarantining of attachments, and additional protection at the gateway.

These technologies have been implemented to ensure that the environment is secure and to uphold the reputation of the brand.

Conclusion

Content Security Checklist

An organization's Content Security solution should be able to address all of the issues covered in this white paper. In addition, it should be able to give you the flexibility to vary policy for individuals and departments, and not apply a "one for all" setting. To check your organization's security, ask your IT department to review your procedures and capabilities against the checklist below. If 'no' is the answer at any of the questions one to fifteen, there is a need to review your organization's security policies and solutions.

Table 3
Content Security Checklist

- | |
|--|
| <ol style="list-style-type: none">1. Do you have an email and web usage policy?2. Have you defined different policies by user, department and time and must users authenticate?3. Have all employees been trained on this policy and are updates communicated?4. Who is responsible for the Content Security of your organization — is the board involved on a regular basis?5. Do you have the ability to check content in web uploads and downloads?6. Do you have the ability to check email circulating internally as well as coming into and leaving your network?7. Do you have the ability to remove/quarantine attachment types?8. Are you able to dismantle all file formats?9. Are you able to allow or disallow HTTPS sessions, and create a policy by site?10. Do you have selective alerting or informing of exceptions?11. Do you have support for virus checking tools, for SMTP, HTTP, FTP and Intranet email?12. Do you have the ability to control ActiveX and .exe downloads and Java Applications, scripting, HTML and FTP?13. Do you have the ability to control offensive content, unproductive surfing and cookies?14. Are you able to check Web email such as "Hotmail" and "Yahoo"?15. Can you generate reporting in network email and web usage down to employee level?16. Has your organization been victim to any of the malicious attacks described in this paper within the last 12 months? |
|--|

Source: IDC/Clearswift 2001

SCM Market Drivers

The following table lists a number of Secure Content Market drivers and presents examples as to what kind of negative results could be expected when not implementing SCM products:

Table 4
SCM Drivers and Negative Examples

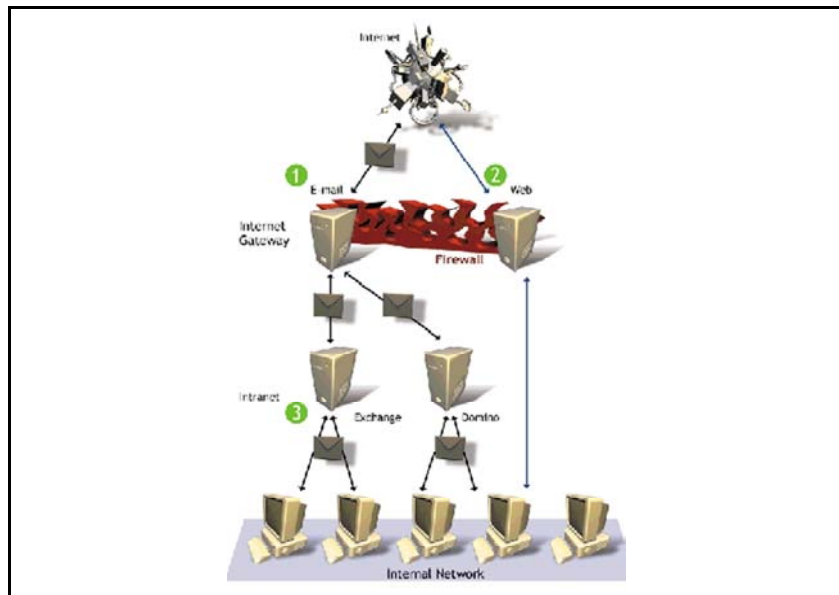
Drivers	Negative Examples
Virus based threats	Estimated cost of Love Bug virus related repairs at \$700 million
Breaches of confidentiality	A leading software company finds employees sending trade secrets via internal email system
Legal liability and copyright infringement	A leading insurance company out of court settlement of £450,000 after alleged defamation
Damage to reputation and lost productivity	Fraudulent email cost a computer networking company \$2 billion following fake press release
Spam attacks	Leading international IT and travel companies have suffered outages
Degradation in service	Proliferation of multimedia attachments strains system capability
Offensive content	Sexual harassment claims against staff at global automotive and petroleum companies
Malicious web downloads	Ability to bypass traditional security mechanisms to prevent applications and loading of data

Source: IDC/Clearswift, 2001

Outlook

IDC believes that Content Security is a boardroom issue. It is an issue which has an impact on all areas of an organization, hence most departments — e.g. IT infrastructure, marketing, HR, legal, finance, etc — should be included when establishing a Content Security policy. While antivirus and firewall products certainly play their part in a security strategy, they fall short in a number of areas outlined in this white paper. Only Content Security solutions — in combination with other software and hardware security products — provide holistic and effective protection against the wide range of modern security threats. Keeping in mind that 60% of all security breaches come from within the network, and considering the complexity of data moved across the Internet, IDC believes that Content Security software is an essential component for organizations that use the Internet and email as part of their daily business operations. Figure 2, overleaf, and Table 5 (see page 18) display and explain where Content Security solutions fit in at the center of an organizations security strategy.

Figure 2
Where Content Security Solutions Fit in



Source: IDC/Clearswift 2001

Furthermore, we see Content Security becoming an integral part of a modular architecture known as Secure Content Management (SCM). Today, SCM software focuses on email and messaging systems that are based on PCs and servers. Over the next one to two years, SCM software will move onto wireless, mobile, and non-PC devices. With rapid proliferation of browser-equipped Web phones expected in Europe, Asia/Pacific, and the United States, IDC expects that the corporations that pay for these services will want to exercise an even greater level of control over these devices.

Table 5
Where Content Security Solutions Fit into an
Organization's Security Strategy

<p>(1) Gateway: SMTP email and email content security provided by ISP/ASPs on a hosted or distributed basis which:</p> <ul style="list-style-type: none">• Analyze incoming and outgoing email and enable organizations to implement security policies to detect, block or quarantine inappropriate or threatening emails and attachments.• Add encryption and digital signature features to stop coded secrets, offensive material and viruses from entering and leaving a network in S/MIME encrypted email.• Avoid damage to reputation and exposure to legal liability by intelligently analyzing images for pornographic content.
<p>(2) Web: Provide network protection by barring access to selected categories of web sites and by constantly monitoring web, http and FTP transfers for inappropriate activity.</p>
<p>(3) Intranet: Internal email Content security solutions provided for intranet infrastructures like Microsoft Exchange and Lotus Domino.</p>

Source: IDC, 2001

Customer demand is growing rapidly for SCM products that protect corporate networks and intellectual property from viruses; malicious code; and also offer businesses legal protection from employees violating company policy when sending or receiving, downloading or uploading prohibited materials via email or the Web - e.g., racial, hateful, and sexually graphic files.

As email demand grows, corporations will also wish to ensure that their employees use their increasingly overburdened mail for productive business purposes only, not for personal communications.

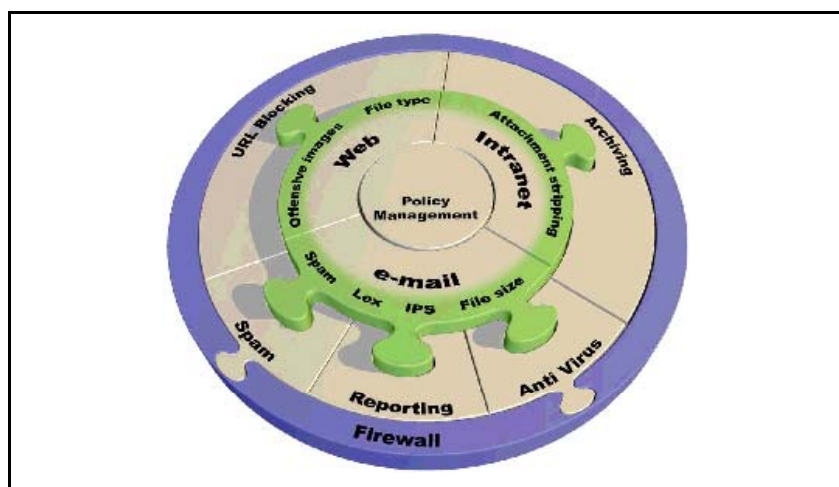
In the future, organizations will look to SCM products to streamline ecommerce transactions. IDC believes that over the next year vendors will start to roll out SCM software that identifies ecommerce objects that contain transactions, authenticates both the user and the transactions, and decomposes the message so that different parts, such as invoices, are routed more effectively.

As secure organizations enter into this period of increasing electronic transactions with partner organizations, it becomes increasingly important that these partners employ similar security measures. It will no longer be sufficient to secure your data within your own organization. Data exchanged with a partner without adequate security, will significantly increase the potential for security breaches, and for critical data to be lost through intentional or unintentional means.

Understanding the legal requirements that your organization needs to fulfil is also necessary when implementing a Content Security policy.

In the near term, companies want a consolidated console for managing all the SCM applications along with aggregated reporting, analysis, and control function (as shown in Figure 3). Organizations want this capability so that they can reduce the IT administration chores and costs, as well as personnel costs. SCM vendors will also benefit from a single management interface to many SCM applications because they receive economies of scale in software updates and managed security services.

Figure 3
Consolidated Security Management



Source: IDC/Clearswift 2001

Approach

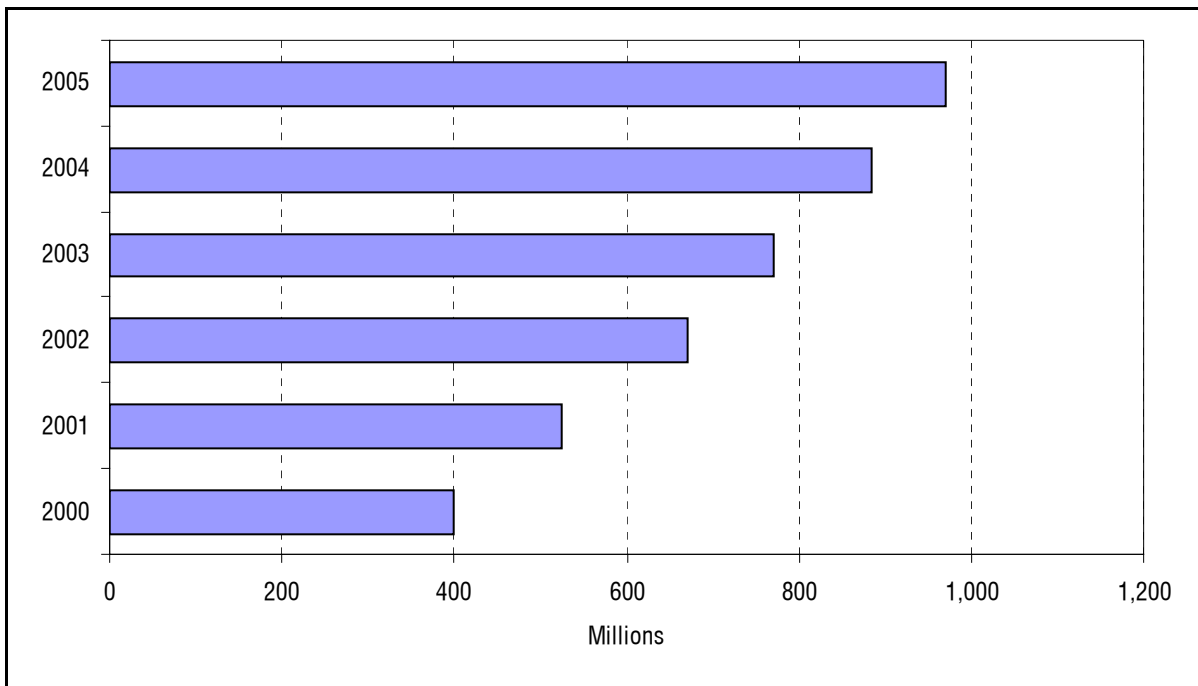
This White Paper was independently written by IDC and sponsored by Clearswift. It has been developed from published IDC research. The case studies were developed through in-depth interviews conducted by IDC with organizations provided by Clearswift.

Appendix - SCM Market

Internet Penetration

As shown in Figure 4, IDC believes that 977 million people worldwide will use the Internet by 2005. We also believe that over 50% of worldwide Internet users will access the Internet from business locations by 2005. (Source: IDC's Internet Commerce Market Model, version 7.1, April 2001) This leads us to believe that the market for Secure Content Management products is just getting started.

Figure 4
Worldwide Internet Users (Business and Consumers)



Source: IDC, 2001

Worldwide SCM Market — Outlook

IDC believes the SCM market will grow from \$1.7 billion in 2000 to about \$4.2 billion by 2005, as shown in Table 1. This figure represents a compound annual growth rate (CAGR) of 20%.

IDC believes that the proportion of future revenue from the **xSP** channel will be substantial. We expect that subscription will rise from less than 2% in 1999 to roughly 30% by 2004. Moreover, this channel will not just deliver these services to large corporate customers; we anticipate that xSPs will deliver SCM to small and medium-sized businesses and potentially to home users. In this area, we expect SCM services from ISPs, ASPs, and MSPs to become popular alternatives to product purchases.

The types of devices people use to access the Internet will change dramatically over the next few years. In 2000, 75% of the

worldwide devices used to access the Internet were PCs. The number of PCs used to access the Internet will more than double by 2005, while their share will drop to 41% of all devices used to access the Internet, as other Internet access devices proliferate. IDC believes that many vendors also recognize that their applications must support wireless Internet access and Web pages as well. In that environment, the wireless service vendors may be required to provide Email Scanning, much like ISPs are increasingly asked to provide basic Internet Access Control (IAC), service to users in the home environment.

Table 6
Worldwide Secure Content Management (SCM) and Firewall Software Revenue, 2000–2005 (\$M)

	2000	2001	2002	2003	2004	2005	2000 Share (%)	2000–2005 CAGR (%)	2005 Share (%)
IAC/EIM	160.2	272.0	408.0	520.0	636.0	739.4	9.7	35.5	17.6
Email scanning	101.4	165.9	257.6	395.5	525.0	689.0	6.1	46.7	16.4
MMC	24.6	39.9	56.2	69.7	78.8	86.4	1.5	28.5	2.1
Antivirus	1,365.8	1,572.9	1,814.6	2,081.8	2,373.9	2,685.2	82.7	14.5	63.9
Total SCM	1,652.0	2,050.7	2,536.5	3,067.0	3,613.7	4,200.0	100.0	20.5	100.0
Firewall Software	735.8	934.4	1,112.0	1,278.7	1,432.2	1,561.1	-	16.2	-

Key Assumptions:

- IDC believes that the proportion of future revenue from the xSP channel will be substantial.
- Over the next one to two years, SCM software will move onto wireless, mobile, and non-PC devices.
- Security spending will increasingly become part of an organization's IT budget.
- European government regulations will fuel the growth of security products and services.
- Security is considered the most important Web site attribute, with high uptime in second place.
- European companies and consumers alike continue to regard security issues like insecure payments, viruses, DoS, email fraud, authorization and authentication as extremely crucial corporate/private factors.
- New wireless/mobile technologies and devices will both boost and need new security solutions.

Messages in the Data:

- The fastest-growing segment of SCM will be the email scanning market. IDC believes the email scanning market will grow at a 47% CAGR and reach \$690 million by 2005.
- The next fastest-growing segment of SCM will be the IAC market. IDC believes the IAC market will grow at a 35% CAGR from 2000 to 2005 and reach \$740 million by 2005.
- IDC believes the market for MMC will grow at a 29% CAGR from 2000 to 2005 and reach \$86 million by 2005.
- The largest segment of SCM, AV software, will grow the slowest over the forecast period. We believe the market for AV software (excluding MMC) will grow at a 14% CAGR from 2000 to 2005 and reach \$2.7 billion by 2005.
- Firewall software (16.2%) will outgrow antivirus software (14.5%), while falling significantly short to email scanning (46.7%) and IAC/EIM (35.5%).

Definitions:

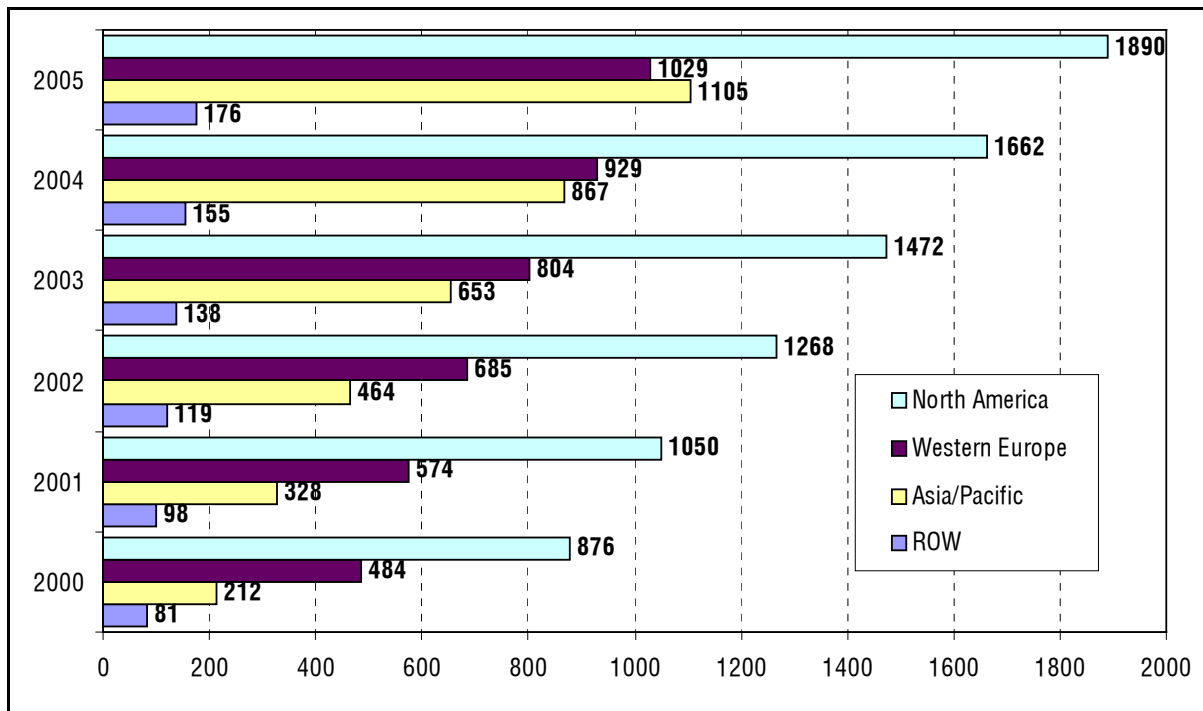
IAC (Internet Access Control), EIM (Employee Internet Management), MMC (Malicious Mobile Code)

Source: IDC, 2001

The security software market, like many other sectors in the economy, is facing a temporary slowdown as companies cut back spending. Although other sectors felt the pinch earlier, the weakened economy has had an effect on this hitherto strong growth market. IDC believes that spending on security has slowed somewhat, but that customers are already starting to return and purchase security as expected. We expect the security market to rebound strongly when economic conditions improve.

Given that much of the slowdown is associated with upgrades, subscriptions, and managed services, the software business should be in a strong position when customers come back for the most recent products. IDC also believes that new growth opportunities will then arise, especially as these products play a critical role in business, where upgrades are an operational necessity rather than a deferrable option for future consideration.

Figure 5
Worldwide Secure Content Management Revenue by Region, 2000-2005 (\$M)



Source: IDC, 2001

Table 7
Worldwide Email Scanning Software Revenue by Vendor 2000

	Revenue (\$M)	Share (%)
Clearswift *	31.0	30.6
Tumbleweed Communication Inc.	24.0	23.7
Symantec Corp.	8.6	8.5
Trend Micro	6.5	6.4
Elron Software	3.0	3.0
Subtotal	73.1	72.1
Other	28.3	27.9
Total	101.4	100.0

Messages in the Data:

- * Clearswift acquired Content Technologies from Baltimore Technologies in March 2002
- Worldwide email scanning revenue increased 95% from 1999 to 2000.

Source: IDC, 2001

LEGISLATION OVERVIEW

Understanding the legal requirements that your organization needs to conform to is essential. Outlined below are some of the key legislation in place today:

THE CYBERCRIME TREATY: Countries will have to create a minimum set of laws to counter cybercrime. This will include unauthorized access to a network, data interference, computer-related fraud and forgery, child pornography, and digital copyright infringement.

<http://cryptome.org/cycrime-final.htm>

FINANCIAL SERVICES MODERNIZATION ACT OF 1999

(Gramm-Leach-Bliley): Allows banks to merge with other firms such as health insurance companies and stock brokerage firms. Contains two sections on privacy: 1) Requires banks to offer "opt-out" of the disclosure of individual's personal information to unaffiliated entities, but provides no protection when banks share customer data with affiliates or with third parties for joint marketing activities. 2) Allows the sharing of sensitive medical information between banks and insurance companies without the individual's knowledge or consent.

<http://www.senate.gov/~banking/conf/>

MILLENIUM DIGITAL COMMERCE ACT (Abraham/Eshoo):

Promotes and sets standards for the use of digital signatures.

<http://www.ccls.edu/eclip2news/topics/esignature/2-6-00.htm>

ELECTRONIC SIGNATURES IN GLOBAL NATIONAL

COMMERCE ACT (Bliley): Provides that in any commercial transaction affecting interstate commerce, a contract shall not be denied legal effect or enforceability solely because an electronic signature or record was used in its formation. Sets forth procedural guidelines affecting: (1) electronic signatures and records; (2) electronic record retention; and (3) interaction of electronic agents.

<http://www.ncua.gov/ref/IST/E-SigAct.pdf>

HEALTH INSURANCE PORTABILITY AND

ACCOUNTABILITY ACT (HIPAA): This act imposes a three-year time limit for the passage of health privacy legislation. Failing to enact any such laws in that period, the provisions in HIPAA mandated that the Secretary of Health and Human Services decree final regulations to protect the confidentiality of electronically transmitted health information. HIPAA's reach extends well beyond the protection of electronically transmitted information, however, and it put into place regulations that govern health care standards for patient record privacy, electronic transactions, security, code sets, etc.

<http://www.hcfa.gov/medicaid/hipaa/>

CHILDREN'S INTERNET PROTECTION ACT: To require the installation and use by schools and libraries of a technology for filtering or blocking material on the Internet on computers with Internet access to be eligible to receive or retain universal service assistance.

<http://www.ala.org/cipa/>

EU DATA PROTECTION DIRECTIVE: Companies across Europe are responsible for the personal data they hold on individuals. Companies are held responsible, even if their employees send information out illegally or accidentally.

Companies which use central mainframes outside of Europe must take steps to make special agreements to avoid breaching the Act.

http://europa.eu.int/eurlex/en/lif/dat/1995/en_395L0046.html

SAFE HARBOUR AGREEMENT: The Safe Harbour Agreement is a joint European Union and US scheme that helps US companies satisfy the EU Data Protection Directive.

<http://www.export.gov/safeharbor/>

EUROPEAN CONVENTION ON HUMAN RIGHTS:

Companies have to protect their employees' right to privacy. Country specific laws such as the HR Act in the UK support this.

<http://www.coe.fr/eng/legaltxt/5e.htm>

THE EU E-COMMERCE DIRECTIVE (EU DIRECTIVE ON INFORMATION SOCIETY SERVICES):

EU countries cannot prevent the delivery of online services from other EU countries. Ratification is set for 16 January 2002.

http://europa.eu.int/eurlex/en/lif/dat/2000/en_300L0031.html

THE EU ELECTRONIC SIGNATURES DIRECTIVE:

Digital signatures can be used for signing contracts in electronic format, aiding e-commerce.

http://europa.eu.int/comm/internal_market/en/media/sign/

EU STATUTE: (name TBC): Companies based in more than one European country will be able to set up as a single European company in 2004.

www.dti.gov.uk/consultations/

REGULATION OF INVESTIGATORY POWERS ACT

(RIP)/Lawful Business Practice Regulations: UK companies have to check that communication networks are not used for criminal activities. The act also formally regulates covert surveillance of all new communications, including all types of mobile phone messages, pagers and e-mails — surveillance cannot violate human rights. Companies are legally responsible for any criminal misuse of their IT networks and can monitor employees' communications to prevent or detect crime. According to the Act, this must not contravene human privacy rights.

<http://www.hmsso.gov.uk/acts/acts2000/20000023.htm>

THE DATA PROTECTION ACT (DPA)

The UK DPA 1998 hands legal responsibility for all personal data to the company, or more pertinently, its directors.

THE EMPLOYMENT PRACTICES DATA PROTECTION CODE – CODE OF PRACTICE: MONITORING AT WORK

The UK Information Commissioner released draft 3 of this Code of Practice in March 2002. The code is based upon the UK Data Protection Act and places responsibilities on any organisation to process personal data that it holds in a fair and proper way. It provides benchmarks on monitoring email and Internet communications.

<http://www.dataprotection.gov.uk/dpr/dpdoc.nsf>

HUMAN RIGHTS ACT (HRA)

Implemented in October 2000, the UK HRA supplements the European Convention on Human Rights (ECHR), guaranteeing the right to privacy and freedom of expression.

<http://www.hmsso.gov.uk/acts/acts1998/19980042.htm>



NORTH AMERICA

Corporate Headquarters
5 Speen Street
Framingham, MA 01701
508-872-8200

IDC Canada
36 Toronto Street, Suite 950
Toronto, Ontario
Canada M5C2C5
416-369-0033

IDC Irvine
18831 Von Karman Ave, Ste 200
Irvine, CA 92612
949-250-1960

IDC Mtn. View
2131 Landings Drive
Mountain View, CA 94043
650-691-0500

IDC New Jersey
120 Wood Ave South, Suite 509
Iselin, NJ 08830
732-632-9222

IDC New York
2 Park Avenue
Suite 1505
New York, NY 10016
212-726-0900

IDC Ottawa
36 Helena Street
Ottawa, Ontario
Canada K1Y 3M8
613-728-3999

IDC Texas
100 Congress Ave, Suite 2000
Austin, TX 78701
512-469-6333

IDC Washington
8304 Professional Hill Drive
Fairfax, VA 22031
703-280-5161

ASIA/PACIFIC

IDC Asia/Pacific (Hong Kong)
12/Floor, St. John's Building
33 Garden Road
Central, Hong Kong
852-2530-3831

IDC Asia/Pacific (Singapore)
71 Bencoolen Street, #02-01
Singapore 189643
65-226-0330

IDC Australia
Level 4, 76 Berry Street
North Sydney
NSW 2060, Australia
61-2-9922-5300

IDC China
Room 611, Beijing Times Square,
88 West Chang'an Avenue, Beijing,
P.R. China, 100031
86-10-8391-3456

IDC (India) Limited
Cyber House
B-35, Sector 32 - Institutional
Gurgaon - 122002
Haryana, India
91-124-6381673 to 80

IDC Japan
10F The Itoyama Tower
3-7-18, Mita Minato-ku
Tokyo 108-0073, Japan
81-3-5440-3400

IDC Korea Ltd
Suite 704, Korea Trade Center
159-1, Samsung-Dong, Kangnam-Ku
Seoul, Korea 135-729
82-2-55-14380

IDC Malaysia
Suite 13-03, Level 13, Wisma KiaPeng
No. 3, Jalan Kia Peng
50450 Kuala Lumpur, Malaysia
6-03-2163 3715

IDC New Zealand
Level 7, 246 Queen Street
Auckland, New Zealand
64-9-309-8252

IDC Philippines
7F, SEDCCO 1Bldg
Rada Street Corner
Legaspi Street, Legaspi Village
Makati City, Philippines
632-894-4808

IDC Taiwan Ltd.
10F, 31
Jen-Ai Rd, Sec 4,
Taipei 106, Taiwan, R.O.C.
886-2-2731-7288

IDC Thailand
27 Soi Charoen Nakorn 14
Charoen Nakorn Road, Klongtongnai
Klongsan Bangkok 10600, Thailand
66-2-439-4591-2

IDC Vietnam
37 Ton Duc Thang Street
Unit 1606
District-1 Hochiminh City Vietnam
84-8-910-1235

EUROPE, MIDDLE EAST, AND AFRICA

IDC Austria
c/o Loisel, Spiel, Zach Consulting
Mayerhofgasse 6
A-1040 Vienna, Austria
43-1-50-50-900

IDC Benelux (The Netherlands)
A. Fokkerweg 1
1059 CM Amsterdam
The Netherlands
31-20-669-2721

IDC Central Europe (ECE)
Male Namesti 13
Praha 1 110 00, Czech Republic
420-2-2142-3140

IDC Central Europe (Germany)
Nibelungenplatz 3, 11th Floor
60318 Frankfurt, Germany
49-69-90502-0

IDC Central Europe (Switzerland)
Niederlassung Zuerich
WTC, Leutschenbachstrasse 95
CH - 8050 Zuerich
Switzerland
41-1-307-1000

IDC France
Immeuble La Fayette
2, Place des Vosges, Cedex 65
92051 Paris la Defense 5, France
33-14-904-8000

IDC Hungary
Nador utca 23
5th Floor, Door #5
H-1051 Budapest, Hungary
36-1-473-2370

IDC Israel
4 Gershon Street
Tel Aviv 67017, Israel
972-3-5611660

IDC Italy
Viale Monza, 14
20127 Milano, Italy
390-2-284-571

IDC Nordic (Denmark)
Jagtvej 169B
DK-2100 Copenhagen, Denmark
45-39-162222

IDC Nordic (Finland)
Jarrumiehenkatu 2
FIN-00520
Helsinki, Finland
358-9-8770-466

IDC Nordic (Norway)
Postboks 102, Stovner
N-0913
Oslo, Norway
47-22-10-12-89

IDC Nordic (Sweden)
Box 1096 Kistagängen 21
S-164 25 Kista, Sweden
46-8-751-0415

IDC Poland/ProMarket
Wrobla 43
02-736 Warsaw, Poland
48-22-754-0518

IDC Portugal
Av. Antonio Serpa, 36 Piso 9
1050-027 Lisbon
Portugal
351-21-796-5487

IDC Russia
c/o PX Post, RDS 186
Ulitsa Zorge 10
Moscow 125525
Russian Federation
7-501-929-9959

IDC South Africa
c/o BMI-TechKnowledge
3rd Floor, 356 Rivonia Blvd.
PO Box 4603, Rivonia, 2128
South Africa
27-11-803-6412

IDC Spain
Ochandiano, 6
Centro Empresarial El Plantio
28023 Madrid
34-91-7080007

IDC Turkey
Tevfik Erdozmez Sok. 2/1 Gul Apt.
Kat 9D; 46 Esentepe
Istanbul, Turkey
90-212-275-0995

IDC U.K.
British Standards House
389 Chiswick High Road
London W4 4AE
United Kingdom
44-20-8987-7100

LATIN AMERICA

IDC Miami
Latin America Headquarters
8200 NW 41 Street
3rd Floor
Miami, FL 33166-6200
305-267-2616

IDC Argentina
Trends Consulting
Rivadavia 413, 4th Floor, Suite 6
C1002AAC, Buenos Aires, Argentina
54-11-4343-8899

IDC Brasil
Alameda Ribeirão Preto, 130 cj 41
01331-000 São Paulo
SP Brazil
55-11-3371-0000

International Data Corp. Chile
Luis Thayer Ojeda 166 Piso 12
Providencia, Santiago 9, Chile
56-2-231-0111

IDC Colombia
Carrera 40 # 103-78
Bogota, Colombia
571-533-2326

IDC Mexico
Select - IDC
Av. Nuevo Leon No. 54 Desp. 501
Col. Hipodromo, Condesa
C. P. 06100 Mexico, D.F.
52-5-256-1426

IDC Venezuela
Calle Guaicapuro
Edif. Torre Seguros Alianza
Piso 6, Ofc. 6-D, El Rosal
Caracas 1060, Venezuela
58-2-951-1109