Eliminating the Hazards of Email

Solutions for Safeguarding Corporate Information

Since its introduction more than 30 years ago, email has become the most important electronic business communications tool. Aside from the standard messaging capability, email is often used as a collaboration tool, personal information manager and file-sharing system for workers. However, the convenience and ubiquity of email, and increased usage of web-based email accounts and mobile devices, has exposed companies to a wide variety of new risks associated with email. While some outbound e-mails contain simple messages, many contain content or attachments that may go against internal messaging policies, compromise the company's competitive position, or violate federal and/or state regulations.

Increased regulatory and public scrutiny has caused many companies to recognize the importance of adopting and enforcing a comprehensive strategy for safeguarding corporate information. This white paper highlights the key issues to be aware of regarding email security, as well as provides a perspective on how companies are trying to minimize their risk. It also offers insight on current technology safeguards and the use of secure, online document sharing as an alternative to traditional methods of communication.

> **"IntraLinks enables our members to securely share documents, in turn expediting communication and keeping confidential information in the appropriate hands."**
>
> — Frederick J. Krebs,
> President, ACC Alliance

INTRALINKS®

1 866 INTRALINKS

New York	+ 1 212 342 7684
London	+ 44 (0) 20 7060 0660
Hong Kong	+ 852 3101 7022

www.intralinks.com

85%

of privacy and security professionals claimed at least one reportable security breach in 2007, while an astonishing 63% of executives reported having 6 to 20 reportable breaches in that period.

Source: "2007 Privacy & Data Protection Survey," Ponemon Institute and Deloitte & Touche

49%

of data breaches over a 12 month period were due to lost or stolen laptops or other mobile devices.

Source: Ponemon Institute, 2007

8.3 Million

Records Spilled in Data Breaches in 2008. At least 8.3 million personal and financial records of consumers were potentially compromised by data spills or breaches in the first quarter of 2008.

Source: Identity Theft Resource Center

The Big Picture

To date, most businesses have focused on protecting their email systems from external threats, such as viruses, Trojan horses, spam and spyware. Today, risks associated with outbound email may pose a much greater threat to a company's long-term prosperity and health than inbound risks. The potential for an accidental (or deliberate) transmission of corporate information, including confidential documents, investor/client contact lists or intellectual property, outside the corporate network requires a comprehensive, company-wide initiative.

Unlike other applications and systems in an organization that have well-defined authentication and access-control restrictions, email usage goes mostly unrestricted. A 2007 Osterman Research survey found that 33% of average employees from medium and large-sized U.S. businesses use personal email accounts at least once or twice a week for business purposes and 17% admitted to daily usage of personal accounts. Furthermore, 16% of respondents admitted to using personal email to avoid corporate review or retention of their messages.

"Lots of networked devices make it more difficult to keep secrets, and even run-of-the-mill proprietary information protected, whether due to employees sending out material they shouldn't or the loss of one of those devices," said Jonathan Zittrain, Professor of Internet Governance and Regulation, Oxford University. "A company can create speed bumps or full barriers to prevent documents from being distributed through email. But it must consider how such measures will impact their employees — they could become less productive, figure out ways to get around the barriers or simply turn to non-employer-provided technologies to do their work."

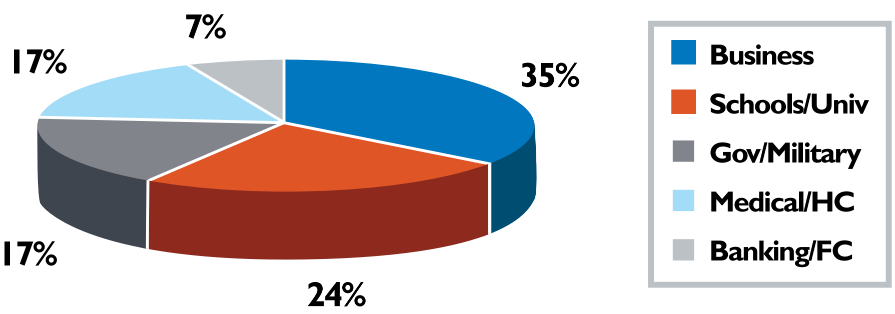
As more security breaches make headlines, state and federal legislature continues to be amended for more stringent control over the use, distribution, storage and deletion of information. Highly regulated industries, such as financial services and healthcare, have additional regulations for their members — rules and safeguards that in time are expected to influence regulations for other industries.

"Regulations, such as Sarbanes-Oxley, are creating real risks for companies," remarked Harvey Pitt, Chief Executive Officer of Kalorama Partners LLC, and columnist for Compliance Week. "They now have to keep and maintain more information than ever before. As the volume of data grows, it becomes more difficult for companies to protect their digital assets. And, if a company finds itself under investigation, it will be next to impossible to keep certain information confidential."

While attempting to protect the greater good, these regulations have added to the complexity and cost of managing data and email use. However, the cost of a breach for an organization easily outweighs the expense to implement the technology and safeguards to prevent one.

In recent news, Eli Lilly may pay more than $1 billion to federal and state governments over marketing improprieties of its antipsychotic drug Zyprexa. The investigation by authorities was prompted by a lawyer, who, believing he was sending a packet of confidential documents to co-counsel, Bradford Berenson, mistakenly e-mailed the documents to The New York Times reporter Alex Berenson.

Data Breaches in Q1 2008



Policies to Safeguard Information: Are They Enough?

Companies from all industries are acting quickly to create enterprise-wide compliance and messaging policies dictating how electronic channels should be used. Although it may seem obvious an employee should not email important company information to their home account, unless a written policy is in place and employees have signed off on it, a company may be hard pressed to penalize them. In addition, policies should be specific and give examples of what is prohibited to ensure workers understand emailing a company document as an attachment to their home account is just as much a violation of policy as copying the document to a USB drive and physically taking it out the door.

According to York Capital's Chief Compliance Officer, Mark Schein, the pervasiveness of email has caused many to forget the risks. "It's important employees understand email is a public communications channel," said Schein. "It's easy to lose control of proprietary information. A document you email can easily be sent beyond its intended recipient. Policies and procedures should be periodically updated to reflect what should and should not be sent through email."

By educating employees about the severity of state and federal regulations and providing them with a set of best practices for accessing, distributing and safeguarding data, businesses can reduce their risk.

"The most important step any company can take to protect itself is to have an educated workplace," offers Chris Marzullo, Chief Compliance Officer at Brandywine Global Investments. "As an investment advisory firm we have access to a lot of non-public information. Our employees are reminded it's their job to safeguard that information. If they get an email request from an outside party for sensitive information, it's their responsibility to not honor that request. If they take a laptop home, it's their responsibility to make sure it's secure at all times. And, if sensitive papers come across their desk, it's their responsibility to use secure receptacles, not the trash can, for disposal."

However, simply writing and distributing a document on email usage doesn't guarantee a business will get the results it wants. In fact, despite the introduction of company-wide policies restricting email usage, workers continue to use it as their primary method for communicating updates and distributing documents to external sources, according to a 2007 IntraLinks' survey of financial services professionals. The survey revealed 77% had company-wide policies against the use of email for distributing confidential or client information. Nevertheless, 70% indicated email was the most common distribution method for exchanging important/confidential documentation and information related to securitizations and other credit derivatives.

Compliance Officers Take on Role of 'Corporate Cop'

For many companies compliance and risk responsibility falls on a Chief Compliance Officer (CCO), Chief Ethics and Compliance Officer or Chief Risk Officer. While financial services firms have long had compliance officers in place, the emergence of CCOs in other industries began in 2002. Following a speech by former SEC commissioner Cynthia Glassman, in which she urged companies to designate a "corporate responsibility officer," many companies quickly heeded the call.

"Since 2002, our membership has more than doubled in size," said Keith Darcy, Executive Director of the Ethics & Compliance Officer Association (ECOA), a not-for-profit organization whose members are responsible for their company's ethics, compliance and business conduct programs. "Organizations are increasingly recognizing the importance of their ethics and compliance office, not just in a time of crisis, but as an integral part of day to day business."

According to Darcy, the ethics and compliance profession is changing as companies come to realize the value of their ethics and compliance office in building a culture of integrity within their organizations. "Mere compliance is not enough, you must produce an ethical culture," proclaims Darcy. "Being a CCO is a high risk job because you can't afford to simply be the corporate cop. You have to set a standard among employees as to what is acceptable behavior and what is not."

Your Most Valuable Intellectual Assets

A company's most valuable resources are no longer equipment and real estate, but rather electronic assets created by human minds. These include:

- Client & customer lists
- Financial/performance results
- Business plans & strategies
- Commissioned/owned research
- Training manuals
- Patents & trademarks
- Clinical test results
- Proprietary software/code
- Business & technical requirements
- Engineering plans & processes
- Contracts & partnership agreements
- Board of Directors communications

Employees have discovered ways to dupe monitoring rules to get sensitive information past corporate email safeguards.

- Rename document to eliminate key words
- Convert data into format that can't be read by filter, e.g. PDF or image file
- Copy sensitive data from one document and create new document
- Remove keywords from within document
- Capture key information with "print screen" key, creating image file
- Encrypt document (filters can't scan encrypted documents)
- Send document as self-extracted archive, i.e. Zip

This translates into a broad set of responsibilities for compliance officers. In some companies, the position is responsible for leading enterprise compliance efforts; managing audits and investigations into regulatory and compliance issues; and designing and implementing internal controls, policies and procedures. In others, the officer is the driving force behind employee compliance training and awareness.

Point Solutions Keep Data in Check

To further guard against a data breach, most companies invest in technology solutions to minimize the chance that user error will lead to a problem. The range of technological approaches for managing email is broad. The functionality these solutions deliver can be as confusing as the categories to which they subscribe. From data leak prevention (DLP) to information leak prevention (ILP) to extrusion detection and prevention (EDP) — all are synonymous with technologies used to address outbound email security. The most appropriate solution for a given organization will depend on the type of data to be protected, how data is used, existing points of vulnerability and corporate security policies and procedures.

Point solutions — security safeguards installed at the computer, email server or corporate firewall level — seek to make email "safer." The most common technologies are email content monitoring/filtering and data encryption.

I. Email Content Monitoring/Filtering

Content monitoring/filtering technology, which was originally designed to block spam and external threats, can be applied to outbound e-mail content. Most content filtering solutions employ pattern matching and exact data matching techniques, whereby email content is matched against a library of terminology, words and phrases. If a match occurs, an alert is generated and the message is flagged or blocked.

The most common weakness of this technology is inaccuracy in the form of false positives and false negatives. False positives occur when harmless emails are flagged as security risks, and result in network managers or compliance departments wasting time and money reviewing safe emails. When a filter too often blocks erroneous emails, frustrated workers begin to employ "work-arounds" — using webmail accounts or sending data in a format that cannot be monitored — to avoid delays. False negatives create a mistaken sense of security leading an organization to believe there are no policy violations while, in fact, they are occurring. To minimize both types of occurrences, organizations must continuously update and refine their keyword library and supporting rules.

II. Data Encryption

Another option is the use of data encryption, which entails scrambling stored or transmitted data using a "key." The result can only be decoded, read and understood by the intended recipient. Encryption programs can be instituted at the corporate database level, whereby periodic system scans identify and encrypt documents that match content management rules. The difficulty of any encryption solution is the on-going management of these keys. If keys are mismanaged or lost, encrypted documents can be lost indefinitely and your encryption plan turns into a costly and ineffective investment.

Despite the advances in technology, no single approach is complete. The ideal solution should address a range of potential leakage points instead of point solutions that target a single area of vulnerability. A company could invest in several different technologies to create a more comprehensive solution. However, a complex network of different applications, hardware and security systems can itself become a risk factor for businesses.

As an example, according to IT experts, the recent exposure of 4.2 million credit and debit card numbers by supermarket chain Hannaford Bros. is believed to have been caused by a poorly configured network and security systems that were not regularly maintained.

Compliance experts warn against over-reliance on quick product fixes for problems as serious and diffuse as information security. When it comes to the security of vital business information, nothing can be left to chance.

Looking Beyond Point Solutions

Given the inadequacies of point solutions and the complexities of managing and maintaining multiple technologies, companies should consider a true end-to-end solution that actually controls user access to corporate information. An online workspace acting as a centralized repository for secure storage and exchange of sensitive business information eliminates the need for documents to be sent via email, and ultimately, provides a comprehensive solution for data security.

The use of online workspaces emerged in the mid-1990s to facilitate mergers and acquisitions and loan syndication transactions. Some providers, such as IntraLinks, offer sophisticated functionality for managing access to corporate information, enabling companies to safely share confidential materials without the security and compliance risks inherent in sending documents via email.

When dealing with sensitive data, it is important to manage user access to certain files and keep certain information on a need-to-know basis, advises Frank Brunetti, IntraLinks' SVP of Product Marketing. "Once a document is sent through email there is no way to pull it back," says Brunetti. "With our On-Demand WorkspaceTM solution businesses have full control over who sees what documents and how those documents are handled."

IntraLinks' online workspace is a cost-effective, turn-key solution requiring no additional hardware or software, no expensive training programs and no new demands on internal IT resources. An easy-to-use interface provides authorized users access to the information they need, anytime, anywhere, through any standard web browser. Unlike point solutions, IntraLinks provides companies with best-in-class user control, document security, knowledge preservation, business continuity and disaster recovery, and compliance management features.

User Control

A powerful permissioning system governs access to each document in the online workspace. When a document is posted, the administrator determines which users are permitted to see and update it. And, unlike traditional access controls, which require IT staff to modify user access, workspace permissions can be easily managed by business users.

Document Security

Even with traditional document security settings applied, unscrupulous individuals can find ways to edit and print protected documents. And, any document sent via email can continue to be distributed beyond the intended recipient. IntraLinks' online workspace provides Document Locking & Protection to prevent unauthorized printing, copying or forwarding. A watermarking feature can also be used to mitigate the risk someone will print or disseminate materials without permission. In addition, access to any document, even after it has been distributed, can be revoked at any time.

Knowledge Preservation

Rather than have important documents reside on multiple servers or desktops, an online workspace provides a single knowledge repository. Having intellectual assets safely reside in one location provides improved versioning control and reduces incidences of outdated documents continually circulating throughout the company. In addition, companies see increased efficiencies when employees are able to easily and quickly locate the documents they need.

Your Challenge	How IntraLinks Can Help
"Once a document is emailed I have no way to know who opens it or prevent them from copying it."	• Allows you to manage individual access on a per document basis • Prevents unauthorized printing, copying or forwarding to hard drive with Document Locking & Protection feature
"Since most documents get distributed via email I try to manage projects with my email folders, but it's not easy and very inefficient."	• Provides an efficient, central repository for all documents • Delivers versioning control and reduces incidences of outdated documents being circulated
"To save time we use email distribution lists, but sometimes this causes documents to be sent to the wrong people."	• Eliminates the need for email distribution • Ensures confidentiality by limiting access and hiding user identities; rather than sending emails, alerts can be generated automatically to notify authorized Workspace users that new documents have been added
"With email I don't always know if people opened a document."	• Saves time by distributing documents online, instantly • Provides detailed tracking and recording of user activity on the Workspace at the document level
"Because my company has file size restrictions on emails, I often have to break documents into multiple emails just so they will get through."	• Eliminates the need for email distribution • Enables file uploads of any size • Offers a single, categorized repository for employees, suppliers or clients to access
"My company sends 1,000s of emails a day. As a Compliance Officer, it's difficult to manage training and legal issues if I'm reviewing flagged emails all day."	• Reduces email usage for a company's most strategic information resulting in reduced incidences of flagged emails • Provides detailed reports of user activity at the document level

Conclusion

The growing number of companies facing potential financial trouble due to leaks of sensitive information is causing many companies to take action by instituting departments, policies and procedures for safeguarding their intellectual assets. Despite policies restricting the use of email, employees continue to use it as their primary channel for distributing important documents to external parties, putting their companies at risk. Most companies turn to point solutions, such as email filtering, monitoring and encryption technologies, to keep employees in check, however, none provide a comprehensive solution. When dealing with sensitive data, the best approach is one that manages user access to certain files and eliminates the need for documents to be sent via email. IntraLinks On-Demand WorkspaceTM for secure online storage and exchange of sensitive business information provides a comprehensive solution for data security.

Featured Experts

Chris Marzulla

is Senior Counsel and Chief Compliance Officer at Brandywine Global Investment Management. He is responsible for overseeing and managing all investment compliance matters within the organization. Chris was named by Institutional Investor as one of its 2007 Top 20 Rising Stars of Compliance.

Mark D. Schein

is Managing Director and Chief Compliance Officer at York Capital Management. He is responsible for the compliance program for the $12 billion hedge fund. Mark was named by Institutional Investor as one of its 2007 Top 20 Rising Stars of Compliance.

Harvey Pitt

is the Chief Executive Officer of Kalorama Partners LLC, a global consulting firm headquartered in Washington, D.C. He is also a featured columnist for Compliance Week. Previously he was chairman of the Securities and Exchange Commission.

Keith Darcy

is Executive Director and President of the Ethics & Compliance Officer Association (ECOA). ECOA is the largest association of ethics and compliance executives worldwide with over 1,400 members across six continents.

Jonathan Zittrain

is Professor of Internet Governance and Regulation at Oxford University. He researches and lectures on cryptography, electronic privacy, Internet governance, and digital property & content controls.

Terms of Use

Although IntraLinks has made every effort to provide accurate information in this document, IntraLinks makes no representations as to, and does not warrant, the accuracy and/or completeness of the information herein or its suitability for any particular purpose. The reader assumes all risk and responsibility for his or her reliance on, or use of, any of the material contained in this document.

ALL INFORMATION IS PRESENTED "AS-IS," AND INTRALINKS DISCLAIMS ALL EXPRESS OR IMPLIED WARRANTIES AND CONDITIONS WITH REGARD TO THE INFORMATION, INCLUDING THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NONINFRINGEMENT. IN NO EVENT SHALL INTRALINKS BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOST REVENUES OR LOST PROFITS, THAT MAY RESULT FROM THE USE OF THIS DOCUMENT.

1 866 INTRALINKS

New York	+ 1 212 342 7684
London	+ 44 (0) 20 7060 0660
Hong Kong	+ 852 3101 7022

www.intralinks.com