



Encryption Subtracts Risk From The Email Equation

Data Loss Prevention (DLP) poses a serious problem for companies as the numbers of incidents continue to gain momentum. Recent headlines have only served to illustrate the gravity and pervasiveness of this issue.

A hacker attack on T.J. Maxx for example led to the largest ever data breach, possibly exposing more than 100 million credit cards to potential fraud. In April 2010, authorities uncovered a China-based cyber-espionage network perpetrated by various government organizations that stole 1,500 emails by infiltrating 1,295 computers in 103 countries, including computers belonging to entities associated with the United Nations, the Embassy of Pakistan in the U.S., and the Office of the Dalai Lama.

Many organizations may not realize that one of the biggest areas of data loss is through email as employees distribute confidential information to third parties such as vendors and customers. Forrester Research reports that email in fact is the second most common source of data leakage storage behind portable storage.

The leakage of sensitive data that results from email communications however, is an often underrated issue. As a result, in most cases email travels unprotected from the sender to the receiver and then stored and forwarded many times over. Yet at any point the message can be intercepted making the contents an easy target for fraudsters and newsmakers.

One high profile warning signal was a Wal-Mart incident in 2009. When a team member was reprimanded for sending an unencrypted email update to other employees, the ensuing exploration revealed that at least four years' worth of customer purchasing data, including names, card numbers and expiration dates were housed in unencrypted form and vulnerable to attack.

Given the sensitive nature of much of the email information being transmitted today, there is every reason to be concerned. Forrester Research states that one in five outgoing emails contains content that poses a legal, financial or regulatory risk. According to Enterprise Strategy Group, up to 75% of intellectual property resides in email data stores. It is clear that organizations need to adopt comprehensive encryption strategies in order to protect their email communications - and their livelihoods.

The Importance of Encryption

Among other security strategies, it is essential that companies encrypt all confidential information that is transmitted electronically and stored on servers, desktops, laptops and other portable storage devices.

In simple terms, encryption transforms plaintext from a readable to an unreadable format in order to hide or disguise the message from people other than the intended recipient(s). With encryption, plaintext is converted to "cipher text" in order to secure the integrity of the data. This text is then "decrypted" to its original plaintext using a private or encryption key.

While the principles of encryption are relatively straightforward, the infrastructure to support encryption can be significant for organizations to implement in-house. A successful encryption solution must be based on proven standards, controllable and ubiquitous, and apply to all data at rest and in transit.

The Managed Approach

For many, the most effective approach is a software as a service (SaaS) managed model built on a secure services platform. This approach reduces encryption complexity and costs, while enabling organization to protect their data without changing their email software or the way they use email.

Integral components of a successful service model include:

- A secure, “strong” encryption services platform that uses industry standard PKI (public key infrastructure) and S/MIME technologies
- Encryption at the desktop and mobile device level
- Encryption across all confidential information on laptops, network drives, removable USB keys
- Encryption at the server level to support policy-based workflows
- Encryption of instant message exchange
- Encryption of document distribution and presentment

Implementing an encryption solution requires significant expertise and extensive partnerships with industry-leading security specialists. As such, more and more enterprises are turning to industry leaders to address their encryption needs. As the demand for encryption capabilities grows, so do the sophistication and availability of resources. The key is choosing solution providers that have the platforms, processes and support resources to address the most complex encryption needs on an enterprise-wide basis.

Legislation at Work

A growing number of jurisdictions implement legislation to protect the storage, transfer and usage personal information. With the introduction of privacy legislation, organizations have no choice but to comply and take steps to protect their confidential information. These include:

- Health Insurance Portability & Accountability Act (HIPAA)
- Sarbanes-Oxley Act (SOX)
- Gramm-Leach-Bliley Act (GLBA)
- California Security Breach Notification Act (CB 1386)
- Payment Card Industry Data Security Standards (PCI DSS)
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- EU Data Privacy Protection Directive

The consequences of non-compliance can be severe, from significant fines to loss of business. T.J.Maxx for example was ordered to pay more than \$40 million in settlement payments with Visa and the credit card processing bank, and the hacker given a 20 year prison sentence. The Information Commissioner’s Office (ICO), the UK’s independent authority responsible for data privacy, has the power to issue penalties of up to £500,000 to organizations in breach of Data Protection Act.

About Echoworx

Echoworx Corporation is the leading provider of managed encryption services for complete enterprise email and data protection. The company is an encryption service provider of choice for Symantec, AT&T, Verizon, BT and Apptix among other global enterprises. Echoworx provides a SaaS (software as a service model); it is built on best-of-breed technology and reduces encryption complexity for the end user. With Echoworx, organizations can protect their email and data without changing their day to day workflow and can easily send encrypted documents and digitally signed email messages to anyone in their address book. For more information: www.echoworx.com