BISCOM

Secure File Transfer

Tracking and Reporting

www.biscom.com

321 Billerica Road, Chelmsford, MA
phone: 978-250-1800
email: sales@biscom.com

EXECUTIVE SUMMARY

The Internet has made it easier than ever to transfer information from person to person. Documents, images, applications, and other data can be sent around the globe instantaneously at the touch of a button or the click of a mouse. While such rapid-fire communication has revolutionized the way business is done, it has also raised a number of questions: What is being sent? To whom? By whom? When? And, most importantly, how do you know?

Files can be delivered in a variety of ways, but the essential business requirement of tracking these files and reporting on their delivery remains identical. Organizations receive data, create data, and send data, and someone has to keep track of this process. Reporting and tracking tools not only improve business efficiency and directly impact the bottom line, they also increase an organization's transparency, necessary for responding to auditor requests.

The need to deliver files securely is increasingly important, not only to organizations that are required by law to protect confidential information, but to any organization that wants to take greater control of who receives critical files and data. With the increased enforcement of compliance regulations, a growing number of hackers attempting to steal confidential data, SPAM filters removing valid messages, and additional strains put on current communications servers such as email, a system with better security and more efficient communications is becoming more valuable and necessary.

SECURE FILE and DOCUMENT DELIVERY

Documents and files can be delivered by a bewildering variety of systems, but what makes one system better than another? For the purposes of this document we will consider a secure file delivery system one that:

- Easily sends files of any size from one person to another person or group of people
- Requires no additional client software at either end of the transaction (or uses ubiquitous software such as Web browsers or email clients)
- Delivers files securely and can track security breaches
- Maintains a complete audit trail of all activity, and notifies the sender when the document was received

While these criteria can encompass a wide variety of document delivery systems, it is important to note that standard email and FTP solutions cannot meet these challenges unaided. Neither is easily secured, and tracking and confirmation is either limited or easily circumvented. Email and FTP are two extremely common methods of delivering files and documents, and as security and reporting become more important for organizations, new solutions must be considered to address these systems' limitations.

COMPLIANCE

New federal and state regulatory compliance requirements are forcing the hand of many organizations to implement strategies and policies to protect sensitive information from unauthorized access. When working with, or transmitting, a patient's Protected Health Information (PHI), healthcare organizations must follow strict guidelines mandated by the Health Insurance Portability and Accountability Act (HIPAA). Financial services firms are gearing up to meet requirements for the Gramm-Leach-Bliley Act (GLBA), which helps protect consumers' private financial information. Sarbanes-Oxley (SOX) is another regulation that requires almost every company to account at any time for the legitimacy of their financial activities. Fines and penalties for not complying with

these regulations can be significant, and enforcement of these regulations is on the rise.

An example of how these regulations affect businesses can be easily seen in the healthcare industry. Under HIPAA, a patient's health information must be protected, and access given only to those who are directly treating the patient. Healthcare organizations are audited regularly to determine how well they are maintaining the privacy of their patients. Healthcare organizations are also vulnerable to lawsuits from individual patients if their information is made available to non-healthcare personnel. In either case, an auditor will want to see every detail of every activity that involved the patient and his/her records. The organization must be able to show the auditor when each record was created, who created it, who else saw it, when they saw it, how that information was passed on to the next person, and how it was protected in transit. Modern healthcare methods can involve multiple practitioners in multiple locations, so this record tracking is often a significant challenge!

Compliance with government regulation is easily facilitated by a file delivery system that maintains detailed records of every transaction. A system that reports on all activity provides the audit trail that investigators look for. The ability to instantly provide detailed information on user transactions can go a long way towards satisfying the demands of an auditor.

LEGAL VULNERABILITY

The government isn't the only potential threat to a business that can be remedied by a comprehensive tracking and reporting tool. Lawsuits against organizations are constantly increasing, not only in frequency, but also in the costs required to deal with them. Many organizations have found themselves liable for lawsuits for which they may not have been responsible – often because they lacked evidence proving their innocence. A reliable system that tracks and reports upon all file and document transactions can be an essential tool in preventing such lawsuits. When an organization can produce a detailed audit trail that refutes a plaintiff's claims, many legal costs related to lawsuits can be avoided entirely.

TRACKING and REPORTING ADVANTAGES

File delivery tracking and reporting also provide benefits that go beyond protecting the organization. A system that tracks all activity is an invaluable monitoring tool that can help administrators in a number of ways:

- Process Improvement – an overall look at how files are delivered over time can pinpoint bottlenecks and delays. Inefficiencies that may not have been obvious before are easy to identify when viewing a report of deliveries over a specified period.
- Abuse Prevention – sensitive data can be monitored to ensure that it's not being sent to unintended recipients. A detailed report of file delivery traffic can also expose misuse of the system for personal reasons.

Tracking and reporting can also improve the way an organization does business, thus increasing the return on investment (ROI) of the file delivery system. Some areas that benefit from better control and view of data management include:

- Reduction in manual compliance checks
- Electronic tracking may replace the need for an overnight courier service
- Retain existing systems and applications and augment them with a secure delivery module
- Reduce or eliminate fines for compliance violations
- Save IT involvement in time and manpower and let content owners securely deliver files

CUSTOMER MANAGEMENT

An understanding of how documents are delivered, when, and to which customers, enables organizations to improve their customer management practices. By monitoring when files are sent and when customers receive them, enterprises can be more proactive and efficient when it comes to file delivery. By tracking the files and documents that have already been sent to the customer, internal users can provide much faster support, and have a much better understanding of a customer's needs and requirements, which in turn leads to better customer service.

An example of such a use might be a software enterprise providing support for their products. When a customer calls in with a problem, the technical support person knows exactly who the customer is, what version of software he is running, when it was last updated, and what software updates have been recently installed. The technical support person does not need to query the user (who may not know this information anyway) and the support call can be resolved much more efficiently.

LEVELS of REPORTING and TRACKING

When assessing the tracking and reporting capabilities of a secure file delivery system, consider the realities that activity must often be reported in a variety of formats, and that many users who require a report may not themselves have access to the actual data being delivered. Organizations require a file delivery system that enables users to view all activity without also being able to view the files/documents being sent/received. These realities require that reports be generated without details on the contents of each transaction. In addition, because users may not have access to the system, or training in its use, these reports may also be automated. Examples of such users are:

- Senders – need to know what was sent and when the file or document was picked up, but only for their own deliveries.
- Managers – require a more detailed report that indicates what was sent and how long it took for deliveries to be picked up, i.e., a snapshot of user activity.
- Executives – require a higher-level statistical data summary revealing delivery trends and patterns.

In fact, there are some privacy policies that prohibit certain users with aggregate data access to view the specific files, documents, or content delivered.

SECURE FILE TRANSFER vs. EMAIL and FTP

Both email and FTP are often used to deliver files today. Both methods, however, are unsuitable for organizations requiring secure file delivery systems. Neither is easy to secure without additional training or software at both ends. In addition, email systems often limit file deliveries according to file size or file type. For example, many email systems do not handle files larger than 5 MB, or files with .exe or .zip extensions. FTP, on the other hand, is difficult to secure and difficult to use without training or additional software. FTP access is also often blocked by corporate firewalls.

When it comes to tracking and reporting capabilities, both email and FTP fall far short of the requirements met by secure file delivery systems. Email users can only request a read receipt – there is no way to require the recipient to send this notification and most email systems allow this function to be easily shut off. There is no way to determine how email is sent, and which systems had access to the message during the delivery process. Without extensive, administrator-level access to both the email system itself and the content of all email messages, it is also difficult to report on email. FTP, on the other hand, provides almost no tracking capabilities at

all. Senders have no easy way to determine whether the recipient logged on to the FTP server, or whether the file in question was downloaded.

A secure file delivery system can provide much more detailed and accessible tracking capabilities than either email or FTP. Recipients cannot refuse read receipts (as with email) and the sender is always able to determine what deliveries have been accessed, when, and how often. Not only does such tracking better meet the organization's requirements, there is also the capability to maintain a version or update history for permanent packages. For example, if a set of files was required for a software installation and made available via a secure file delivery system, administrators could update that package at will with an automatic record being made of this activity. This automation makes it easy to determine when these files were updated and which users accessed the updated files, a determination that cannot be made via email or FTP without additional software or customization.

BISCOM Secure File Transfer

Biscom offers solutions to help organizations keep their confidential information private. Biscom secure file transfer provides a solution for sending and receiving files and messages from point to point over a secure connection. Authentication and tracking features provide system administrators with fine-grained reporting capabili- ties. Biscom secure file transfer was designed from the ground up to provide a secure message and file delivery system with built-in tracking, reporting, and data and user management. Reports can be generated at any time to provide summary data and analyses on usage, and even customized to report on only data relevant to the customer.

CONCLUSION

Tracking and reporting is an essential part of regulatory compliance but it is also useful to organizations that simply want to have better control over their data. Biscom secure file transfer can help organizations meet these requirements using methods that are unavailable via email or FTP. With increased scrutiny of document and content access and delivery, especially in light of recent compliance regulations, tracking and reporting will be a necessary part of any organization's data management practices.