



Secure File Delivery

Secure Information Exchange in an Insecure World



www.biscom.com

321 Billerica Road, Chelmsford, MA

phone: 978-367-3612

email: sales@biscom.com

EXECUTIVE SUMMARY

Ask a group of office workers how they would send a file securely from one person to another (with the recipient being able to easily receive and view the file), and there is a likelihood that they will not know how to accomplish that task. With current federal and state mandated compliance regulations and additional concerns about protecting personal privacy, it is becoming increasingly important to send information, data, and files securely. It is not uncommon practice today for many companies to send confidential or sensitive information, files, and data across a medium that is insecure – namely email, FTP, and the Web – technologies that were not built to address security or robust reporting requirements. Worse still, even with the proper technology and tools in place, complexity and lack of proper training can render those tools useless. Businesses and consumers alike realize the need to adopt and embrace easily understandable and usable technologies that will minimize the threat of accidental exposure of sensitive information.

SECURITY

Locking down information is a difficult task. The Internet, highly connected corporate networks, and a multitude of information delivery and sharing applications, including email, have made companies extremely permeable with respect to the inflow and outflow of data. Of particular importance is the potential transfer of sensitive information to unauthorized recipients. Two ways data leaks out are from intentional removal of data and from a malicious hacker. The intentional removal of sensitive information, usually by someone internal to the organization, is hard to prevent – there are many ways to take information out of an organization, including uploading it to an external site, storing it on a flash memory stick or CD, sending it out via email, and printing it out, to name a few. Organizations can also be hacked by malicious users who look for security holes in the network or through poorly protected applications and interfaces. Hacking goes beyond the scope of this paper, but a full security audit can help identify and prevent potential breaches before they happen. Aside from the acts of intentional and malicious users trying to extract confidential data, organizations should examine ways they can minimize or prevent accidental exposure of sensitive information. This is most easily achieved through the use of tools, proper user training, definition and enforcement of security policies, and potentially a change in user behavior.

Ensuring security is as much a technology deployment matter as it is a user training issue. It is possible to implement an extremely secure system, but it may require exceptional knowledge on behalf of both the sender and the recipient of the data. If the tools are complex or difficult to learn and apply, it is likely that people will refuse to use them. If tools and applications exist that are easy to learn and simple to use, people will be more likely to adopt them.

The other side of security must focus on the recipient of the delivery. To maximize the reach of any delivery tool, it is imperative to make sure the recipients of a secure delivery need no special software to install or run to retrieve a delivery – using ubiquitous technologies, such as Web browsers, as opposed to specialized applications, ensure maximum compatibility and make the retrieval of information as simple as possible. Requiring a recipient to run client-specific software or have a specific computing environment set up is difficult except in highly controlled environments, and makes ad-hoc delivery to new recipients difficult.

COMPLIANCE

New federal and state regulatory compliance requirements are forcing the hand of many organizations to implement strategies and policies that are meant to protect sensitive information from unauthorized access. Health-care organizations must follow strict guidelines when working with or transmitting a patient's protected health information (PHI) 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. With "phishing," "pharming" and other highly publicized examples of large-scale financial information theft and abuse receiving attention, companies of all sizes are under increasing scrutiny regarding their compliance with GLBA.

Fines and penalties for not complying with these regulations can be significant. Enforcement of these regulations is also on the rise – the first year after Sarbanes-Oxley became law, two hundred and fifty investigations were launched and twenty-five CEOs were convicted. GLBA violations call for both civil and criminal penalties, up to \$100,000 in civil penalties for each violation. Officers and directors are personally liable for up to \$10,000 per violation and face up to ten years in prison. Financial institutions that violate GLBA can be fined up to \$1 million and officers and directors can be barred from working in the banking industry. HIPAA violations for an individual who fails to comply can range up to \$25,000 per incident; if the individual knowingly discloses identifiable health information, the fine can rise to \$250,000 and up to a ten year jail sentence.

LIMITATIONS of EMAIL

Many people using the Web or an email system are unaware of the risks they take when sending or receiving confidential or sensitive messages or files. Email has significant risks associated with it, particularly because the route an email takes from sender to recipient may not be as straightforward as one might imagine. Email, developed in the early 1970s, was not architected with security in mind, but rather it was designed as an open and resilient communications system. This included mechanisms that automatically re-routed emails through various servers or "hops" based on the availability of intermediate servers between the sender and the recipient. This was useful during the Cold War when network nodes were targeted by ICBMs, but these days, that same resiliency opens a very large security hole – messages and data could potentially be stored and downloaded off intermediate servers without a sender's knowledge. Other techniques and tools, such as network sniffers, allow email messages and data to be extracted from the data stream en route.

Email also suffers from increasingly strict policies enforced at the corporate or ISP level, such as message size limits, bandwidth caps, restrictions on file types, and potential network clogging due to spikes in traffic when sending large attachments to many recipients. Email recipients may never receive valid messages that SPAM filters incorrectly discard. One common complaint of email and Web-based downloads is the lack of receipt notification, or that return receipt of email is not mandatory on the recipient's part. Many companies impose limits on attachment sizes below two megabytes, or remove "zip" or "exe" attachments for fear of viruses.

If an organization does not impose size limitations, users sending large file attachments over email to a large recipient list can bog down email servers as they try to send the email messages out immediately. Information Technology departments also grow concerned when storing files both sent and received through their email systems, as it increases the support and maintenance of their critical communications systems.

LIMITATIONS of FTP

FTP is another early technology that has been a staple file delivery protocol for over thirty years. Again, designed primarily as a simple file transfer system, most security features have been built around FTP or “bolted on” to lock it down – the protocol is not inherently secure, nor was it designed to fit in a secure environment. Usernames and passwords are sent to FTP servers in clear text – anyone watching network traffic can see these passwords. In addition, many companies block the FTP protocol at their firewall or deny access for their employees to FTP sites, thus making FTP downloads impossible.

Other message and file delivery systems such as Web download are also commonly used to deliver information. If not properly secured, these also provide significant risk of exposure of data.

TRACKING, REPORTING, and NOTIFICATION

One of the major requirements of many compliance regulations is the need to view and audit transaction records for deliveries, notification, and pickup by recipients. Transactions involving the content creation and editing process are also important in understanding who has created, updated, or deleted data.

Tracking email that is sent out by individuals is a difficult task, and one that is not easily monitored; items in sent folders can be easily deleted. FTP logs are cumbersome and not easily deciphered by a typical user. Usually it requires involvement by the IT department to download the logs, and even then, FTP logs may not provide enough details to be useful, or are not easily filtered to extract the relevant data. Web server logs are similarly difficult to get, and contain a large percentage of potentially irrelevant transactions. Web servers do not track actual users requesting pages either – and may not be able to give any details on the actual user downloading files. As FTP and Web server logs are essentially text files, other tools are usually required to filter and generate useful reports.

SHARING the NETWORK

Some companies are willing to open up their network through secure tunneling solutions such as virtual private networks or other remote access technologies. This is useful in many cases, but the danger of exposing critical servers and portions of the network that should not be accessible by outsiders is greatly increased. In addition to that, these types of network accesses may require specialized software and a certain level of network knowledge that many people may not be able to put into practice.

FILE DELIVERY through BISCOM DELIVERY SERVER

Biscom offers solutions to help organizations keep their confidential information private. Biscom's Delivery Server product provides a solution for sending and receiving files and messages from point to point over a secure connection. Authentication and tracking enable system administrators fine grained reporting capabilities. An open, standards-based API provides easy integration with existing applications and databases.

Biscom Delivery Server 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. It is a Web-based platform with a rich API set that exposes the entire breadth of features to developers and integrators. Instead of opening up an organization's internal network to outside users, including third party contractors, customers, or partners, Biscom Delivery Server provides a safe “sandbox” environment that only allows access to specific messages and files.



Biscom Delivery Server solves many of the issues from which email, FTP, and other Web delivery methods suffer. Managing deliveries and delivery parameters is a significant aspect of Biscom Delivery Server as it provides the ability to specify a window of time that files are available, limit the number of times a file may be accessed, and enables password protected access on a per-delivery basis. Deliveries can be scheduled to go out in a staggered fashion, thus minimizing network bandwidth spikes. Unlike “fire and forget” email, the sender can retract deliveries. Almost every email user has accidentally sent an email to an unintended recipient, or perhaps sent inappropriate content. If that accidental email violated any compliance regulations, the sender, the directors, or the entire organization may be liable and held responsible for the consequences. Outbound notification alerts recipients of new deliveries without clogging their inboxes with large file attachments, and notifications to the sender when someone opens a delivery acts as a return receipt – it cannot be bypassed. SPAM is never an issue as email is used to notify recipients of new deliveries only – the content and files associated with a delivery are always stored and available through the Biscom Delivery Server Web interface. 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.

The security and tracking features of Biscom Delivery Server are available to users through simple and intuitive user interfaces. Biscom Delivery Server may be accessed through any Web browser, or integrated with email systems that provide the new secure delivery features in a well known computing environment – sending email and attachments securely is as easy as sending an email message.

CONCLUSION

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 assume 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 like email, a system that can provide better security and make communications more efficient is becoming increasingly more valuable and necessary.

Email, FTP, and Web downloads are susceptible to several problems, many that are inherent to the technology upon which they are based. Whether you are looking to change existing policies and behavior by introducing new tools, or are trying to lock down existing applications, Biscom Delivery Server’s management, reporting, and auditing capabilities help organizations achieve the levels of security and confidence they need as part of larger efforts for a more secure communications infrastructure.