External SharePoint Collaboration—Without Compromise

By Mike Hugos, CIO-at-Large, Center for Systems Innovation and **Jose Almandoz,** EVP of Business Operations, IntraLinks

According to an article on ZDNet about SharePoint, more than 7.3 million new SharePoint users are added every year, making it a multi-billion dollar business for Microsoft. But can a business collaborate with external partners outside the firewall while ensuring the security of its content? What viable solutions are out there? Mike Hugos, CIO and author of books on IT best practices and cloud computing, and Jose Almandoz, EVP of Business Operations for IntraLinks, give us their insights.

What are the key elements of a secure collaboration solution?

Mike Hugos: The right solution enables agile response, leverages but unburdens the in-house IT infrastructure, and comes with a business model that creates predictable and recurring costs, and lowers up-front investment.

Jose Almandoz: A proper solution needs to provide external partners access to the same tools and security beyond the firewall as within it. At the same time, it needs to feature a user interface that is familiar to internal users, and intuitive to external users.

Consumer-grade solutions sometimes lack the enterprise security to achieve that integrity.

MH: There are also procedural and technical parts to a good, secure collaboration solution. The technical part is assessing the ability to encrypt and de-encrypt documents, and to assign the right access to the right people. You need to be able to determine who can read content online, or read—and download—it.

Then there's the procedural aspect. What is the "need-to-know" content? What are its parameters? Administrators need to be able to set parameters to provision and support users according to their organization's information management policies.

Why is SharePoint ideal, but also challenging as a solution for external information sharing?

MH: SharePoint is ideal because many companies already use it. It's great to leverage what is already in place when working with external users.

JA: It's an ideal internal collaboration tool, but challenging for sharing information externally. Internally, it provides a stable and scalable foundation for document sharing, team collaboration, electronic forms and social enterprise portals.

In addition, IT staff has been trained in its operation and support, and business people have learned its user interface and depend on it for intra-company document sharing and content management.

MH: The value of that knowledge possessed by IT and line-of-business employees is incalculable—and it's all on top of a company's hard-dollar investment. But SharePoint was never designed to operate beyond the firewall. You need to have the right add-on because it doesn't come out of the box as an external tool.

JA: Making SharePoint secure for external content sharing can be extremely difficult. It has some weaknesses, such as inadequate auditing and access reporting, file encryption, document locking and protection limitations, and provisioning and supporting a community of external users.

The challenge for CIOs with sizable SharePoint investments is to build on it as an existing foundation, which is exactly how a platform like IntraLinks can serve as an alternative: one that integrates seamlessly into SharePoint, but with that added security for external users.

What is the cost of build versus buy on SharePoint externalization mechanisms?

JA: IT departments work under tight budgets. They need an alternative that lets them enjoy secure collaboration without buying more servers or investing in customization. When a company uses SharePoint externally, they have to maintain those external collaborators. With that comes thousands of dollars in IT costs. With a cloud-based information sharing solution, IT departments can rapidly outsource the support of external collaborators, and reduce costs.

MH: I always look first to see if there's an off-the-shelf plug-in to meet my needs before going into custom coding—which is typically the most costly solution. If you take that route, you need to make sure there are unique requirements that no off-the-shelf solution meets.

Why is a hybrid, cloud-based solution ideal to leverage your existing SharePoint implementation?

MH: The days of trying to connect everything in house to the outside world are already over. The cloud-based skills allow us to be comfortable in a hybrid environment. But the IT professional needs to guide his company through the hybrid world right now. It's already in existence. The real skill is in knowing how to respond to it.

JA: A cloud-based hybrid allows internal users to continue using their familiar SharePoint-based platform and applications with little or no change. It also helps simplify identity management tasks and takes workload off of internal SharePoint servers. Too many people performing content searches and queries can reduce performance.

What are some of the additional security benefits of a hybrid solution?

JA: For starters, virus protection—and file encryption beyond the firewall is vital. Hackers can find a way into almost any system if they are determined enough, but when a system's data is encrypted, that data remains secure.

Integrated digital rights management is also key, so IT departments can manage content after a document has been distributed. This helps ensure the user will not inadvertently lose or leak the document.

Then there's real-time monitoring: which people are looking at what documents, for how long, and the ability to create audit reports from this information to meet compliance. Administrators also need to be able to manage document access and download privileges.

These are assets that companies sometimes don't realize they're missing when they use consumer-grade products such as Dropbox or Google. A good solution adds security, compliance and information governance capabilities without requiring additional SharePoint customization, or introducing a new interface that internal users have to learn.

MH: When you have a well-architected hybrid solution, you can focus on the APIs that connect your in-house system with your cloud-based apps. In that API, you have the opportunity to put in very comprehensive data screening and identity management. The architecture that works in the hybrid environment leverages the APIs as control points for data security.

When I think about the importance of the role this plays in the security scenario, I always think of the famous scene from *The Graduate,* where Mr. McGuire tells Ben, "I just want to say one word to you... 'plastics'."

In one word, I would say, "API". ▮

IntraLinks is a leading provider of integrated Software-as-a-Service (SaaS) solutions for secure internal/external collaboration.