A HURWITZ WHITE PAPER

Enterprise Collaboration: Avoiding the Productivity and Control Trade-Off

Marcia Kaufman
COO and Principal Analyst

Daniel Kirsch
Senior Analyst

HURWITZ & ASSOCIATES
Insight to Action

Sponsored by Intralinks

Enterprise Collaboration: Avoiding the Productivity and Control Trade-Off

Introduction

Companies that collaborate effectively and securely can bring innovative products to market more quickly, improve operating efficiency, increase customer loyalty, and drive increases in sales. However, many organizations struggle to create collaboration environments that enable them to reach their goals. Why are companies finding it hard to create environments that make it easy for business stakeholders to safely share information and ideas to achieve a common goal?

There are many technology and economic trends – including mobility, globalization, big data, and cloud – that are accelerating the demand for business collaboration. For example, increasing numbers of mobile workers and globally distributed work teams are driving demand for new collaboration tools that make it easy to share large files beyond the firewall. The information shared by these enterprise teams is often highly sensitive and subject to industry or government regulation. In addition, data shared by these collaborative teams increasingly comes from varied sources, making it harder to manage. As a result, high priority data is leaving the corporate domain without proper oversight and control, exposing organizations to an increased risk of data loss or regulatory non-compliance.

To better understand collaboration challenges and how business users are sharing information, Intralinks commissioned two independent studies. More than 800 IT and business executives from around the world were surveyed for these studies. In this paper, we'll summarize key findings from this research focusing on the challenges companies face in creating secure collaboration environments. In addition, we will discuss the business and technical priorities for companies implementing collaboration platforms, from both a productivity and security perspective.

Key Research Findings

The research studies commissioned by Intralinks were directed at IT and business executives across various industries including many highly regulated sectors such as financial services and life sciences. These executives responded to surveys on the challenges of using collaboration tools and the technical and business requirements for creating a secure collaboration environment. The key challenges identified in the research are as follows:

1. **Organizations often lack visibility and control over how they share information.** Many companies are concerned about how they collaborate and share data. While 76% report having visibility and control over data shared inside their organization, this falls to only 30% when data is shared outside the firewall.

More than 800 IT and business executives from around the world were surveyed for these studies. … While 76% report having visibility and control over data shared inside their organization, this falls to only 30% when data is shared outside the firewall.

HURWITZ & ASSOCIATES
Insight to Action

2. **Employees are using consumer-grade file sharing without IT or business oversight.** Many IT departments are not aware of the extent to which employees are sharing content via consumer cloud tools. Among all the organizations included in the study, approximately 60% of employees are using consumer tools for business. This reality leaves organizations open to data leakage, inappropriate disclosures and regulatory risks.
3. **The accidental mishandling of information and data happens every day.** Most organizations focus on preventing malicious data theft and hacking. While this is critical, the reality is that the vast majority of data breaches are the result of accidental mishandling and inappropriate sharing. For example, 80% of study participants reported receiving an email not intended for them during the previous month.
4. **Securing the perimeter and infrastructure does not ensure content security.** Companies are moving to a more collaborative way of doing business resulting in an increased flow of data between parties both internal and external to the organization. Unless enterprises have a strategy to protect data that moves across boundaries, the organization may be at risk. Therefore, a data-centric approach to content security is needed in order to protect information wherever it travels.
5. **Regulatory issues around content security are real and evolving.** New, more onerous regulatory requirements are being introduced at increasing rates. With the proliferation of consumer-grade technologies entering enterprise environments, IT groups are having difficulty meeting these new requirements. Almost 90% of the organizations participating in the study expressed concerns about meeting future regulatory demands around information security in their industry.

The Current State of Enterprise Collaboration: Inadequate Control over Shared Content

One of the most significant research findings is that companies are rapidly adopting cloud based consumer-grade collaboration tools without the benefit of established IT security policies to control the flow of information.

The companies in the study report that over 60% of their employees use cloud collaboration tools such as Dropbox or YouSendIt. The majority of users gravitate to these tools based on their ease of use without understanding the increased security and regulatory risks they bring to their companies. This trend has not gone unnoticed and survey respondents are concerned about the rapid increase in the use of consumer cloud information sharing services. They worry about data leakage, IP loss, and regulatory compliance. One consequence is that many companies are instituting policies to restrict or eliminate the use of consumer cloud sharing tools. Research showed that 49% of organizations block the use of consumer file synch and share applications from being used in their companies, for fear of data loss or because of regulatory compliance issues.

The need to quickly and easily find ways to share information with individuals outside the firewall has been a key driver for the move to cloud based consumer

Research showed that 49% of organizations block the use of consumer file synch and share applications from being used in their companies, for fear of data loss or because of regulatory compliance issues.

HURWITZ & ASSOCIATES
Insight to Action

sharing platforms. Although many organizations have enterprise collaboration tools in place, these tools were not designed to support content sharing outside the firewall. It is easy to see why platforms like Dropbox or YouSendIt have become so widely used in enterprises even though they expose the company to security risks. Many companies have inadequate alternatives. Email and messaging, still the most widely used collaboration tool in many enterprises, falls short when employees need to exchange or share large files, manage tasks in work streams, or deal with multiple versions of documents with a large team.

For example, a salesperson may choose to use DropBox or YouSendIt to send a proposal to a prospect because the files are too large to send via email. Once the proposal is submitted the salesperson loses all control over the content. An email attachment can be printed, saved to the recipient's desktop or forwarded to others. The files sent by the salesperson could easily be passed to many other people, perhaps even a competitor. If such data were to fall into the wrong hands during sensitive negotiations, a deal might collapse. Worse yet, data leaks can have long lasting effects, such as long-term financial and reputational damage.

Email and messaging, still the most widely used collaboration tool in many enterprises, falls short when employees need to exchange or share large files, manage tasks in work streams, or deal with multiple versions of documents with a large team.

Priorities for Enterprise Collaboration Platforms

It is important to find the right balance between two critical priorities when evaluating an enterprise collaboration solution. IT needs to ensure that the employee's expectations for usability and productivity are met in order for the collaboration solution to be adopted across the enterprise. At the same time, there needs to be a layer of control and security in order to protect sensitive information from getting into the wrong hands. Survey respondents recognized that without a high level of usability, secure collaboration platforms fail to gain broad adoption, leading employees to seek alternatives.

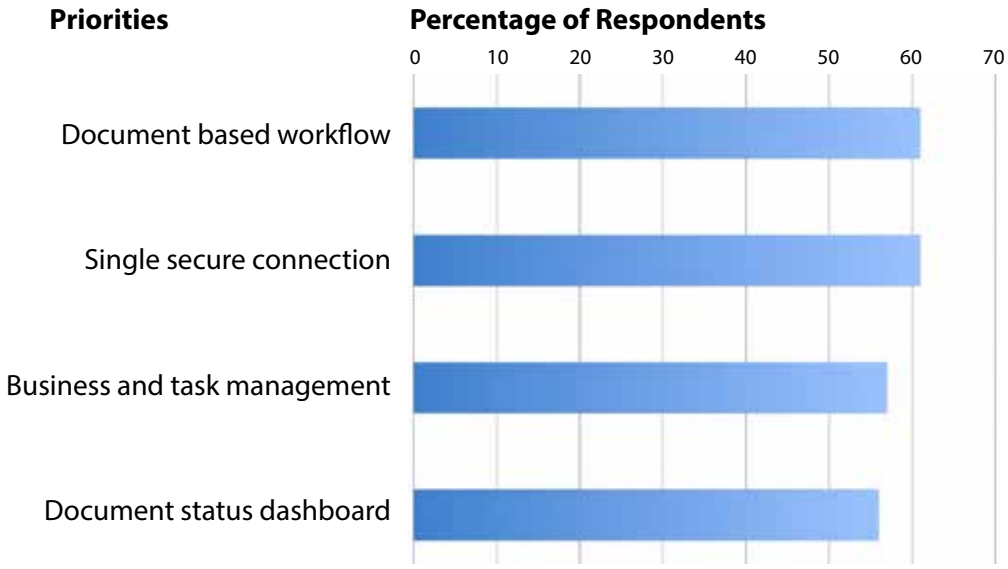
The survey indicates that IT executives have very limited visibility and control over content being shared once it leaves the firewall. While nearly 75% of organizations reported having adequate visibility and control into content being shared within their organization's firewall, only 30% reported the same levels of visibility and control once content was shared with individuals outside of the firewall. Correcting for this limitation is a high priority for companies evaluating enterprise collaboration platforms. Priorities for usability and security are detailed below.

Priorities for Usability and Business Productivity

Survey respondents are looking for enterprise collaboration platforms that enhance and extend the capabilities of their existing platforms, while improving employee productivity. The ability to create workflows, enable users to manage tasks, and provide a dashboard to quickly view the status of work streams are all important. Figure 1 lists several of the top usability and productivity-enhancing requirements that IT executives are searching for in a collaboration platform.

HURWITZ & ASSOCIATES
Insight to Action

Figure 1: Priorities for Usability and Business Productivity



Source: Intralinks independent research, 2013

Survey respondents are looking for collaboration platforms that will help them maintain control over content even after it has been broadly shared.

Priorities for Security: Lifetime control of content

Survey respondents are looking for collaboration platforms that will help them maintain control over content even after it has been broadly shared. As shown in Figure 2, over 60% of respondents identify permission pullback (or the ability to unshare) as a top priority when looking for a collaboration platform.

Why are IT executives interested in a collaboration platform that provides the capability to maintain lifetime control over content? Certainly companies want to maintain control over shared content to protect against intentional theft of IP or other sensitive information. However, the requirement to maintain control is not always directly tied to data theft. Often, data is simply sent to the wrong person inadvertently. For example, over 80% of respondents say they've receive an email not intended for them, and 53% actually confess to making the same mistake themselves, with an astonishing 43% saying they make these kinds of mistakes on a monthly basis. If the content contains highly sensitive or regulated information such as supply chain details, product schematics, pricing data or personally identifiable information, then the simple act of sending a file to the wrong person can have serious consequences.

Data loss due to accidents and mistakes far outweighs data theft due to malicious activity. Unfortunately, there is no practical way to protect against loss of sensitive information from a miss-sent email. Even if an email system has a recall option this is often voluntary and has limited impact. In fact, once the recipient opens the email, recalling it is no longer an option and that content is no longer under the organization's control. Therefore, IT organizations see great value in technologies that can guard against this with the ability to retract files at will, even after they have been broadly shared and copied.

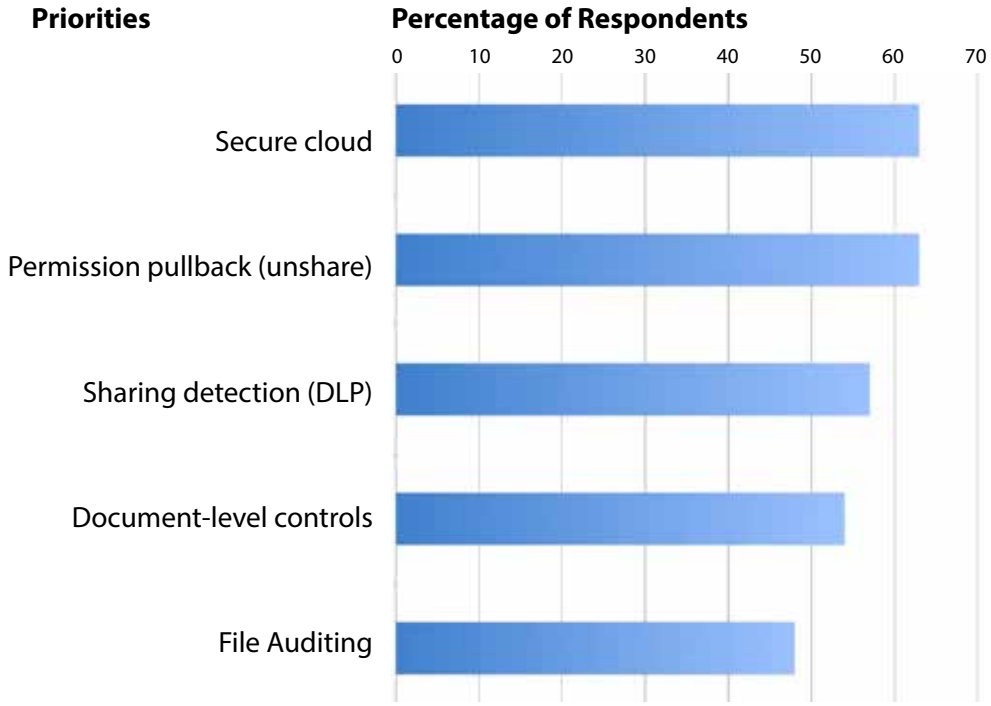
HURWITZ & ASSOCIATES
Insight to Action

Another reason companies need lifetime control over content is to help maintain version control. Without long-term versioning control, teams may base decisions on inaccurate information. If the company has the ability to maintain control over the document no matter where it is stored or if it is copied, the risk of introducing errors is reduced significantly.

The survey included many companies from highly regulated industries such as financial services, law firms, life sciences and governmental agencies. Respondents from these sectors understandably placed a high priority on additional security requirements such as information rights management and encryption.

Today, this control and visibility over IP has expanded outside of IT. It has become critical that managers and line of business owners protect content while enabling collaboration across teams.

Figure 2: Priorities for Security



Source: Intralinks independent research, 2013

Enterprise Collaboration in Practice

Effective collaboration requires that organizations reach across geographical and corporate boundaries so that teams can easily and safely work with customers and partners. The organization must at the same time be able to adequately protect IP and meet regulatory requirements over the lifecycle of the shared documents. Today, this control and visibility over IP has expanded outside of IT. It has become critical that managers and line of business owners protect content while enabling collaboration across teams. There are a variety of business cases that lead companies to identify security as a top concern for collaboration environments. Many organizations are already taking steps to better manage

how they collaborate. Over 55% of the companies surveyed now employ a Chief Information Security Officer (CISO) tasked with managing these risks, and over half of respondents are planning to upgrade their secure collaboration capabilities within the next 18 months.

There are a variety of use-cases that lead companies to identify security as a top concern for collaboration environments. Two of the most common business cases are described below:

- **Ad-hoc collaboration - Sharing sensitive or proprietary data for a specific project over a set time period.**
  A manufacturing company just received approval to participate in a highly competitive bidding process on an important new project. The deadline for bids is in two weeks and the company needs to quickly form a work group of its most experienced technical designers and engineers from multiple divisions. The company needs an environment that will enable its technical designers and engineers to collaborate with contractors, suppliers and the customer. They need to start work on the project immediately and need an easy way to share large documents, in many cases containing highly sensitive information. Some people on the team will need access to all documents, whereas others will participate intermittently and should be granted access to only certain documents for a limited time. This extended team needs an environment that will support its requirement to work quickly and maintain strict control of versions of key documents. Due to the highly confidential nature of this project, the company wants to ensure that access to the information can be revoked from third parties upon project completion or contract termination.
- **Meeting regulatory requirements for data handling and confidentiality.**
  A team of physicians and scientific researchers has been working on a genetics research project. They have recently expanded the scope of their research and are seeking additional funding. Additional researchers and a grant writer joined the team to work on the grant proposal. Given the highly confidential nature of the project and associated documentation, the team needs a collaboration environment that supports the sharing of information with a high degree of confidentiality. The team is based in a university research hospital and all patient lab and clinical data must be protected according to HIPPA (Health Insurance, Portability and Accountability Act). In addition, research notes and other content needs to be kept confidential.

Recommended Steps for Secure Enterprise Collaboration

Having a strategy for secure enterprise collaboration will ensure greater productivity and efficiency, while guarding against security and regulatory risks. Hurwitz & Associates recommends the following approach:

- **Understand what collaboration tools are already being used.** You should assume that consumer-grade file sharing tools are in current use in your organization. Conduct an audit to understand what tools are being used, including what features are valued and why.

… a strategy for secure enterprise collaboration will ensure greater productivity and efficiency, while guarding against security and regulatory risks.

HURWITZ & ASSOCIATES
Insight to Action

- **Identify specific use-cases and user requirements to ensure your enterprise collaboration solution will be effective in meeting the needs of your organization.** Understand which environments are most likely to require the sharing of sensitive data. Make sure your solution will address the security requirements of these environments.
- **Give employees a viable collaboration solution that meets their specific needs and satisfies the organization's requirements for security and control.** Once you understand your organization's current collaboration requirements and what tools are already in place, deploy an acceptable solution that gives users the freedom to share while providing the business with visibility and control. Key issues to consider for the solution are:
  - **Put the end-user first.** You need to gain enterprise wide adoption of your collaboration solution or you will not achieve the desired level of security and control. In order to achieve acceptance, your solution needs to be easy-to-use and simple to provision and deploy.
  - **Don't compromise on security and control.** There doesn't need to be a compromise between pleasing end-users with a simple and elegant product and ensuring that you can support the most rigorous use-case for security and level of control. Features like digital rights management (DRM) and the ability to control access at the individual file level can be found in solutions that have the same ease-of-use as consumer products.
  - **Keep lifetime control of documents.** Make sure that even if a file is shared outside the firewall, it always remains inside your control. Having lifetime control, so that a file can be revoked at will, or at a predetermined time, is a critical requirement.
  - **Move beyond sharing.** Effective collaboration requires far more than sharing of documents. Your enterprise teams need to be able to work collaboratively on information in simple work streams, while easily managing tasks and roles.
- **Build on your existing and proven solutions.** Collaboration solutions should work with your current solutions such as Microsoft Outlook. This is a sound economic decision and will encourage adoption by supporting existing processes and familiar ways of working.
- **Educate, manage and then control how employees collaborate.** Most employees are unaware of the security risk associated with their use of consumer-grade collaboration solutions. However, simply blocking these solutions without offering a viable alternative is going to backfire. Your employees will keep looking for a workaround. The best defense against high-risk consumer-grade collaboration tools is to provide a secure solution along with education on how users and the company will benefit from its use.
- **Stay ahead of regulatory requirements.** Work with your legal and security teams to fully understand the regulatory environment and make sure that existing collaboration practices are fully compliant.

Having lifetime control, so that a file can be revoked at will, or at a predetermined time, is a critical requirement.

HURWITZ & ASSOCIATES
Insight to Action

Conclusion

Companies are facing many challenges when it comes to creating environments that support both effective and secure collaboration. Collaboration at the right time and with the right information can help your organization improve productivity and improve business results. On the other hand, if employees share sensitive content without the proper level of security and control, your company may risk losing valuable IP or fail a compliance audit. Intralinks sponsored research of over 800 IT organizations showed that many companies do not have collaboration tools that are both easy to use and secure enough to protect sensitive information. Today, many IT organizations have limited insight and control into what content is being shared, when it is being shared, and by whom.

Given the increasing need of companies to collaborate with customers, partners and other third parties that exist outside the firewall, there is an urgent need to deploy enterprise collaboration environments that satisfy requirements for ease of use and security. Companies should begin by understanding what collaboration tools are already in use at their organization. In addition, an education campaign is a priority to ensure that employees understand the risks of using consumer grade file sharing tools.

Given the increasing need of companies to collaborate with customers, partners and other third parties that exist outside the firewall, there is an urgent need to deploy enterprise collaboration environments that satisfy requirements for ease of use and security.

About the Research

Intralinks commissioned two research reports to investigate the challenges organizations face to securely and effectively collaborate. In 2012 Intralinks commissioned a global strategic consulting firm to investigate the market requirements for enterprise collaboration. Over 650 senior business and IT decision makers were asked to describe their current approach to collaboration and their anticipated requirements. In 2013 Intralinks commissioned a second independent survey with SC Magazine/Haymarket of 200 enterprise IT and business executives to understand the risks they face with existing collaboration technologies.

HURWITZ & ASSOCIATES
Insight to Action

About Hurwitz & Associates

Hurwitz & Associates is a strategy consulting, market research and analyst firm that focuses on how technology solutions solve real world customer problems. Hurwitz research concentrates on disruptive technologies, such as Big Data and Analytics, Cloud Computing, Service Management, Information Management, Application Development and Deployment, and Collaborative Computing. Their experienced team merges deep technical and business expertise to deliver the actionable, strategic advice clients demand. Additional information on Hurwitz & Associates can be found at www.hurwitz.com.

13A Highland Circle • Needham, MA 02494 • Tel: 617-597-1724
www.hurwitz.com