ENTERPRISE FILE SHARING AND MANAGEMENT: ACHIEVING PRODUCTIVITY AND SECURITY

OCTOBER 2014

In this report, Hanover Research provides an overview of the market for file sharing solutions for large and highly-regulated enterprises based on a review of relevant secondary literature and interviews with IT and security leaders within the financial, healthcare, and higher education industries.

HANOVER RESEARCH
www.hanoverresearch.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

INTRODUCTION

In this report, Hanover provides an overview of the file sharing practices and perspectives of large and highly-regulated enterprises. Section I of the report summarizes the overall market, while Section II presents an analysis of highly-regulated industries' requirements for electronic file sharing solutions based on original interviews conducted with knowledgeable industry sources. A summary profile of these respondent experts is provided in Appendix A.

KEY FINDINGS

- Highly-regulated enterprises and companies that manage a large volume of sensitive personal or financial information view data security and risk mitigation as a non-negotiable prerequisite for any electronic file sharing solutions. While other considerations may influence vendor selection, these are secondary to the overriding necessity for top-tier security.
- Mobility is an increasingly significant driver of corporate interest in file sharing solutions. However, security concerns with public cloud services are leading compliance-focused enterprises to delay implementation and/or limit use of these services. The inability to access files via mobile platforms is a visible pain-point for large and highly-regulated companies, but the need to protect sensitive data frequently poses a prohibitive obstacle.
- The ability to integrate file sharing solutions with other enterprise software and programs is a relatively low priority for enterprise customers. It is not uncommon for different groups within a single large organization to have separate, non-integrated file sharing solutions. While there is clear interest in unified, integrated systems, the level of effort required to accomplish this goal is seen as prohibitively high, while ongoing frustration with the current state of limited integration – while real – does not rise to the level of being a determinative factor in decisions regarding file management.
- In implementing file sharing and management solutions, highly-regulated enterprises seek to avoid risks – including security lapses, illicit access, exposed files, and service outages – commonly associated with employee use of public cloud solutions.
- Regulated industries show a strong preference for on-site deployment of synchronization and sharing services. This is principally driven by security concerns; until those concerns are addressed, these industries are unlikely to make the switch to hosted file sharing and management. The typical industry perspective is articulated by one senior IT source as "if we keep it in-house, we know we're limiting our risks. I know that there are ways of mitigating the risks associated with hosted solutions, but would you rather mitigate those risks or just avoid them?"

RECOMMENDATIONS

- **The World is Moving** – For enterprises of every type and size, the evolution of work processes now demands capabilities that challenge traditional, IT-sanctioned file sharing methods.
    - If employees lack access to a file storage platform with mobile file sharing capabilities, information will increasingly be transmitted via uncontrolled and potentially insecure channels.
    - The increasing demand for knowledge sharing and productivity means enterprises without secure and easy-to-use collaboration tools may either jeopardize data security or pay a penalty in operational efficiency. **Either outcome can put these enterprises at a competitive disadvantage.**
- **Compromise is Not an Option** – IT leaders within large and highly-regulated enterprises are unanimous in stating that data security and regulatory compliance must be maintained to the highest possible degree.
    - Top-tier data security should be considered table stakes for any enterprise in considering electronic file management solutions. While other capabilities may factor into vendor selection, only offerings that provide the most robust security features should even enter into consideration.
    - Regulatory compliance support is an essential element of any data management solution. The lack of consistently up-to-date tools and systems ensuring ongoing adherence to evolving legal standards creates risks that are otherwise unavoidable and should be considered unacceptable.
- **Proceed with Caution … but Proceed** – Perhaps the greatest risk that an enterprise with outdated file sharing methods can take is doing nothing. ***Enterprise IT leaders must embrace their role as stewards of company data, and also provide essential productivity, mobility and collaboration tools.***
    - Employees demand effective and user-friendly file sharing and collaborative capabilities, and organizations that do not implement these internally will increasingly find sensitive data being transmitted via channels outside of their control – at a time when data thieves have reached unprecedented levels of sophistication.
    - By implementing mobile file sharing and collaboration platforms that leverage on-site deployment models, enterprises can keep sensitive information under supervision without compromising employee productivity, operational efficiency, and competitive advantage.

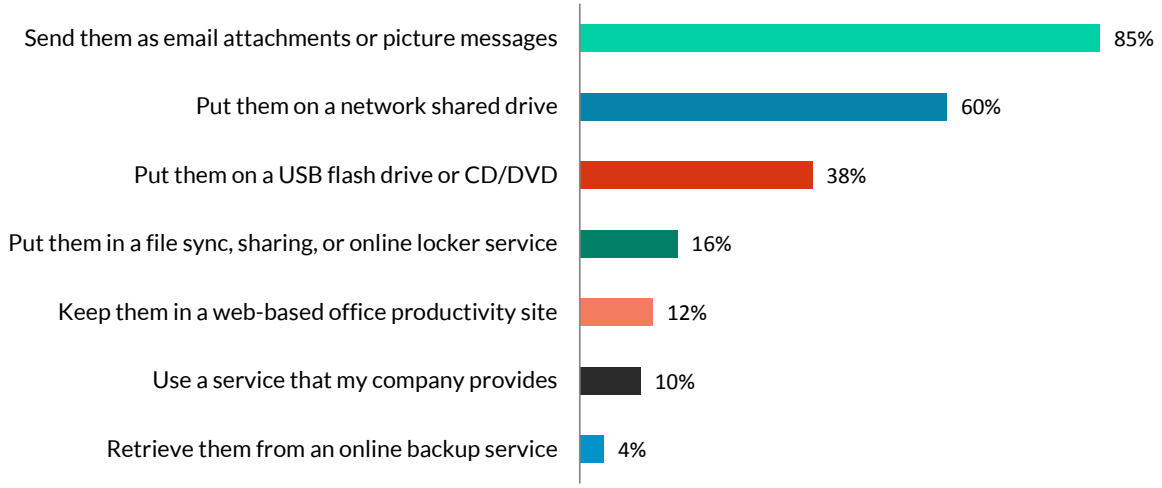
SECTION I: MARKET LANDSCAPE

OVERVIEW

Global demand for enterprise file synchronization and sharing (EFSS) solutions is experiencing rapid growth, with projections suggesting that the market will reach $2.3 billion by 2018.[1] In mid-2013, approximately 25 percent of the global information workforce used consumer-grade file synchronization and sharing services – a dramatic 400 percent increase in utilization since 2010.[2]

File sharing and synchronization software has become an essential productivity-enabling resource for increasingly mobile information workers. According to Forrester, about two-thirds of information workers share files with others on a routine basis.[3] However, in the absence of widespread enterprise EFSS solutions, a majority of information workers share documents and files via email and other unsecure methods.

Figure 1.1: How Information Workers Share Documents



Source: Shey, H.[4]

IT security decision-makers are faced with a dilemma: how to provide employees with a functional file sharing solution while minimizing the risk of data leakage.[5] Though this matter carries particular urgency for large companies and companies in highly-regulated industries, roughly 60 percent of IT security decision-makers note that they are concerned about consumer-oriented communications and file sharing tools running on non-corporate resources. However, while 88 percent of enterprises have security policies in place, only 41 percent have both security policies and tools to enforce such policies.[6]

[1] "New IDC Worldwide File Synchronization and Sharing Forecast Shows Market Will Grow to $2.3 Billion by 2018" IDC, October 2014. http://www.idc.com/getdoc.jsp?containerId=prUS25192614

[2] Koplowitz, R., and Ted Schadler. "What File Sync And Share Customers Have Learned." Forrester Research, July 24, 2013.

[3] Shey, H. "Technology Spotlight: Enterprise File Sharing, Policies And Security." Forrester, December 20, 2013.

[4] Ibid.

[5] Ibid.

[6] Ibid.

SOLUTIONS

While demand for secure EFSS solutions is higher than it has ever been, IT decision-makers face significant challenges in vendor selection. Monica Basso of Gartner states that the market for electronic file sharing solutions is "immature but crowded," and market players present varied and difficult-to-assess claims regarding the features of their EFSS offerings. Gartner notes that the emerging market for enterprise file synchronization and file sharing focuses on six types of capability: (1) social and collaboration; (2) storage and backup; (3) content management, managed file transfer and collaboration; (4) mobile devices; (5) cloud virtualization; and (6) enterprise mobility. While all of these areas are receiving significant promotion, however, very few vendors actually operate across these different sectors.

There are more than 120 vendors active in the EFSS market, with "nearly all of them [leveraging] the public cloud … for storing files on behalf of enterprise users."[7] While this deployment method may be acceptable for organizations that are not working with particularly sensitive information, highly-regulated enterprises do not have the luxury of trusting such unsecure solutions. This difference in the capabilities required by large or highly regulated enterprises is illustrated by the success of Dropbox, considered a "Challenger" in Gartner's EFSS Magic Quadrant report. Dropbox "has been so successful to date by being end user friendly and largely ignoring IT"[8] – this indicates a clear discrepancy between general enterprise file sharing and synchronization solutions, and the caliber of EFSS solutions required by highly-regulated industries.

[7] Scearce, T. "The Public Cloud – Is it Safe for Enterprise Files?" Attachmate, July 31, 2014. https://www.attachmate.com/blogs/datainmotion/public-cloud-safe-enterprise-files/

[8] Miller, R. "Dropbox Looks to Shed 'Dropbox Problem' Image." TechCrunch, June 6, 2014. http://techcrunch.com/2014/06/06/dropbox-looks-to-shed-dropbox-problem-image/

SECTION II: FILE SHARING SOLUTIONS FOR REGULATED ENTERPRISES

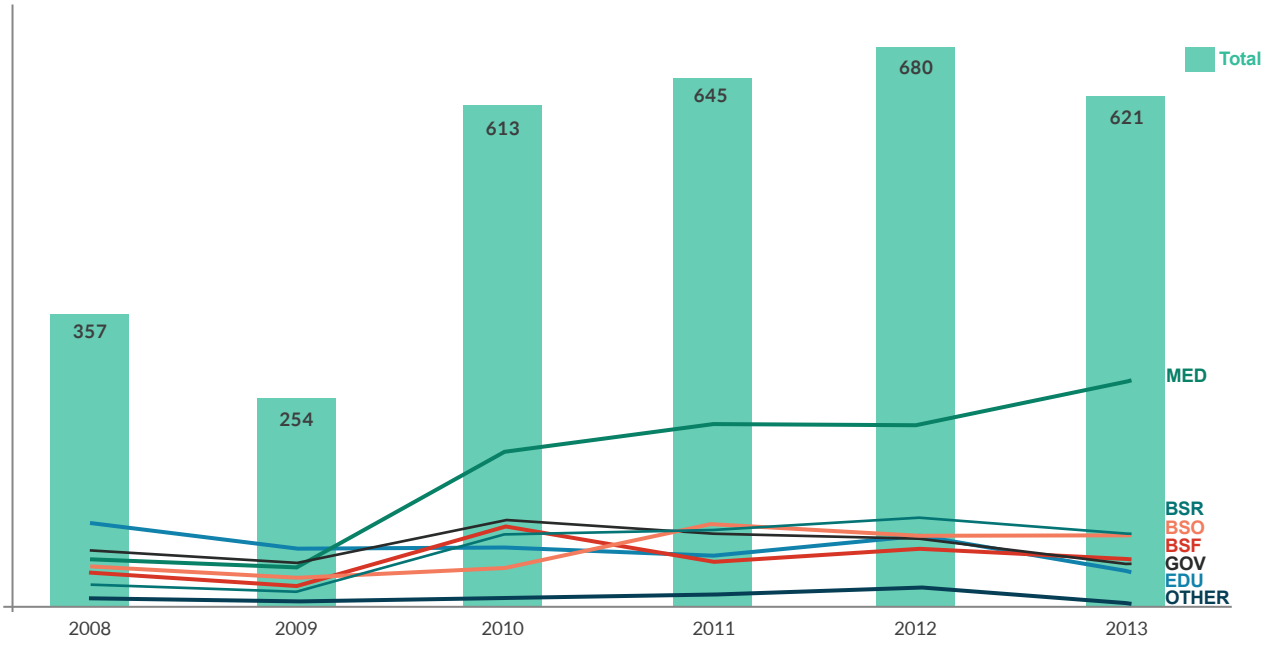
In this section, Hanover summarizes the observed market dynamics for electronic file sharing solutions in highly-regulated industries based on primary interviews with industry experts and a review of relevant industry publications.

OVERVIEW

Unlike individual knowledge workers, or even small-to-medium businesses, larger and more regulated enterprises have unique and critical requirements for file synchronization and sharing solutions. According to Gartner, chief information officers (CIOs) are interested in implementing enterprise file synchronization and sharing solutions to "improve employee collaboration and mobile access to information assets."[9] However, IT security decision-makers in highly-regulated industries place greater importance on security and risk mitigation than on improving employee collaboration and mobile access.

According to the Privacy Rights Clearinghouse, the total number of known data breaches increased by almost 74 percent from 2008 to 2013. In the healthcare industry alone, breaches have risen by 24 percent.

Figure 2.1: Number of Data Breaches, by Industry



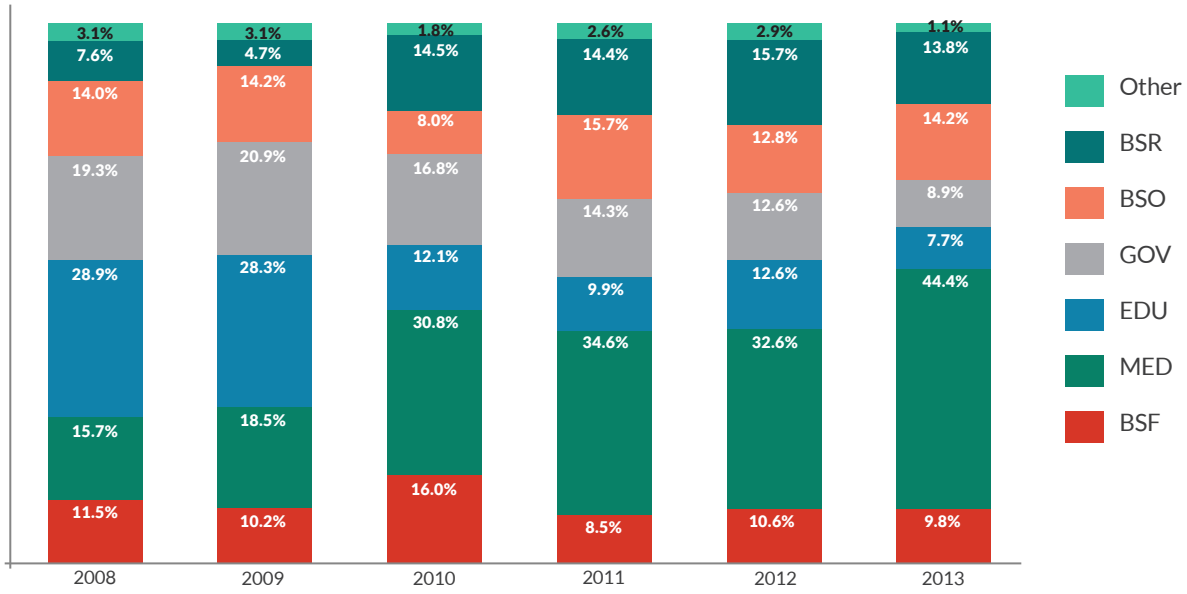
*BSR = Businesses (Retail/Merchant); BSO = Businesses (Other); GOV = Government and Military EDU = Educational Institutions (All); MED = Healthcare; BSF = Businesses (Financial and Insurance Services)

Source: Privacy Rights Clearinghouse

[9] Ruth, G., and Alan Dayley. "EFSS Changes How Users Deliver Data Services." Gartner, May 29, 2014.

The heavily regulated financial services and insurance industry accounted for about 10 percent of total data breaches in 2013, while medical/healthcare breaches represented 44 percent. When retail and education breaches are considered, the total swells to 75 percent of all breaches in 2013, up from 63 percent in 2008.

Figure 2.2: Number of Data Breaches, by Industry (in % share)



*BSR = Businesses (Retail/Merchant); BSO = Businesses (Other); GOV = Government and Military EDU = Educational Institutions (All); MED = Healthcare; BSF = Businesses (Financial and Insurance Services)

Source: Privacy Rights Clearinghouse

In light of workers' rapid adoption of file sharing, the rising number of data breaches in highly-regulated industries underscores the need for systems that can support efficient workflows without compromising data security.

Given the nature of information commonly shared in these industries, IT policy prioritizes different requirements to govern employees' use of file sharing software. The healthcare, financial services, and insurance industries (among others) view data security and loss prevention as key requirements, while end user needs like mobility and ease-of-use are given secondary consideration.

Enterprise file sharing and synchronization "is a growing category of services and applications that provide Dropbox-style functionality, while also addressing the security and manageability needs that go along with handling personally identifiable information (PII)."[10] Industry experts expect that EFSS adoption will increase in the future, due not only to the convenience advantage over older file sharing tools like email and FTP, but also because of the ability to provide access, authorization, and audit controls. **Particularly among security-conscious enterprises, "adoption will be contingent on vendors successfully convincing customers of the security model."**[11]

"A MINORITY OF FSS TOOLS IN USE ARE TRULY ENTERPRISE GRADE."
- Osterman Research

[10] Ho, B. "Enterprise File Synching For Sharing Financial Information." Credit Union Times, September 17, 2013. http://www.cutimes.com/2013/09/17/enterprise-file-synching-for-sharing-financial-inf

[11] Ibid.

SECURITY AND COMPLIANCE

Enterprise CIOs and CISOs are expected to protect vital information assets from internal and external threats; however, most file sync and share solutions do not meet the compliance and security requirements of highly-regulated enterprises. According to Osterman Research, "[content] shared using most FSS tools is normally not encrypted unless the user specifically chooses to do so and installs additional software to encrypt the content."[12] While smaller companies in certain industries may adopt public cloud file sharing services, use of such services is uncommon in large, highly regulated industries. And, Gartner notes, "[security] and compliance requirements may slow down the adoption of cloud-based EFSS" because of industry and regulatory distrust of the cloud.[13]

One key regulation that applies across industries is the Sarbanes-Oxley Act (SOX), which was implemented in 2002 "in order to hold chief executives and chief financial officers of public companies accountable for certifications of their financial reports from their companies."[14] IT and security managers must also address SOX requirements for information security, as the law includes a provision requiring CEOs and CFOs attest to their companies' proper internal controls. "It's the IT systems that keep the books… If systems aren't secure, then internal controls are not going to be too good."[15]

HEALTHCARE

The healthcare and life sciences industry faces some of the most stringent information security regulations. Healthcare companies must mitigate risks of noncompliance with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act.

[12] "File Synchronization and Sharing Market Forecast, 2012-2017." Osterman Research, May 2013. https://owncloud.com/wp-content/uploads/2013/07/OR-FSS-Market-Report.pdf

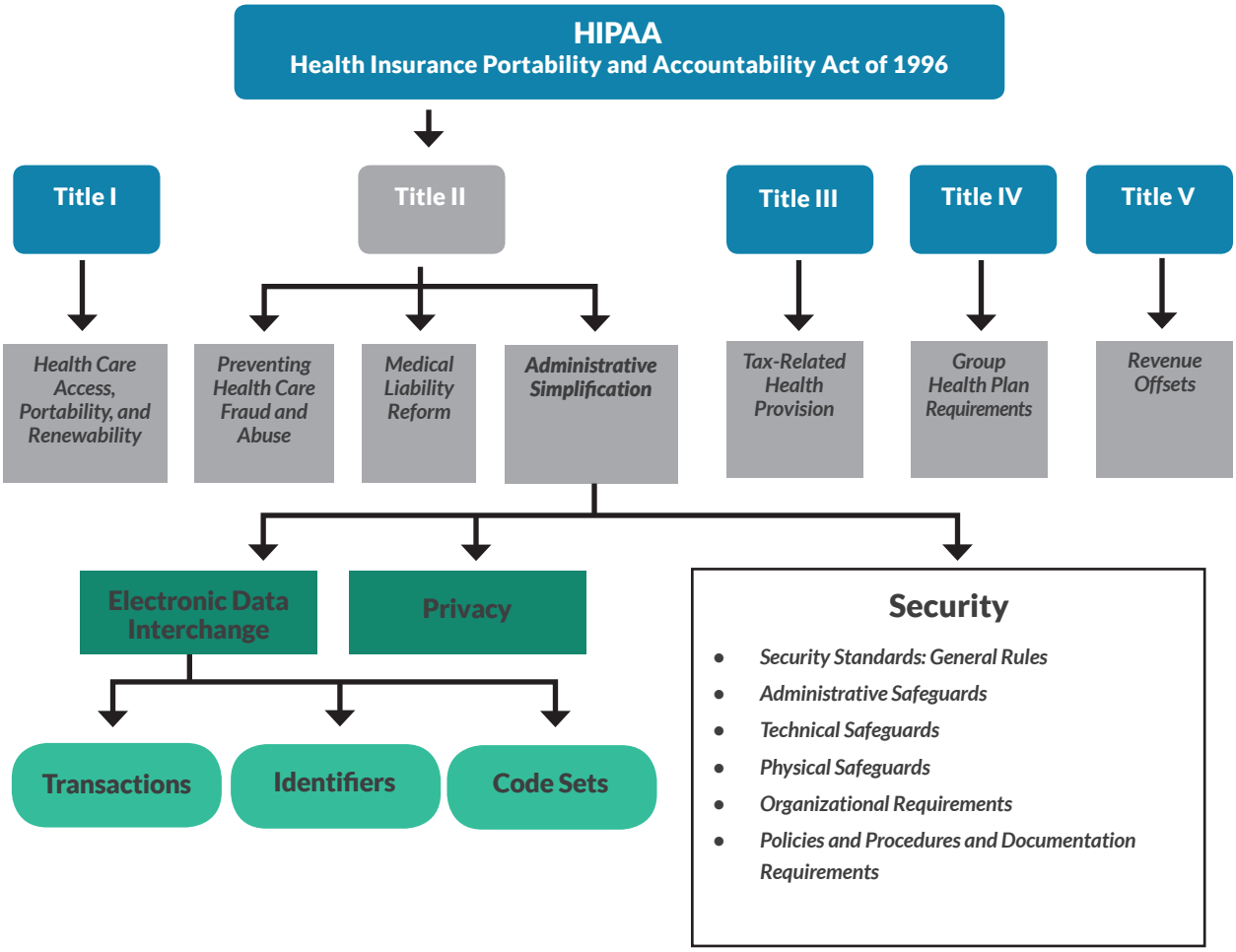
[13] "MarketScope for Enterprise File Synchronization and Sharing," Op. cit.

[14] Sabett, R. "The real deal with Sarbanes-Oxley: Perspectives for the security manager." TechTarget. http://searchsecurity.techtarget.com/tip/The-real-deal-with-Sarbanes-Oxley-Perspectives-for-the-security-manager

[15] Hurley, E. "Security and Sarbanes-Oxley." SearchCIO, September 25, 2003. http://searchcio.techtarget.com/news/930493/Security-and-Sarbanes-Oxley

The HIPAA Security Rule focuses on safeguarding electronic protected health information (EPHI), and applies to covered healthcare providers, health plans, healthcare clearinghouses, and Medicare prescription drug card sponsors.[16] HIPAA is the "number one file transfer priority for those in the healthcare space."[17]

Figure 2.3: HIPAA Components



Source: National Institute of Science and Technology[18]

HITECH focuses on promoting the adoption and meaningful use of health information technology, such as electronic health records. The Omnibus Rule was put in place to implement the HITECH Act, and requires that "all entities that handle healthcare data … adhere to strict security and privacy requirements."[19]

[16] Scholl, M., et al. "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule." National Institute of Standards and Technology (NIST), October 2008. http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

[17] Allen, K. "Transferring Healthcare Files in the US? Here are the Terms You Should Know." Ipswitch File Transfer, May 15, 2015. http://www.ipswitchft.com/blog/healthcare_file_transfer_terms/

[18] "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule," Op. cit.

[19] [1] "WatchDox Secures Healthcare Data for Providers, Insurers and Their Partners." WatchDox, September 23, 2013. https://www.watchdox.com/en/press-releases/watchdox-secures-healthcare-data-for-providers-insurers-and-their-partners-2/; [2] "Transferring Healthcare Files in the US? Here are the Terms You Should Know," Op. cit.

FINANCIAL SERVICES

According to Bill Ho of Biscom, financial services organizations use a variety of methods of sharing information, ranging from email to FTP servers, USB drives, and electronic data interchange solutions, among others. Sharing files through file synchronization is considered a relatively new method of sharing information. As Ho notes, "While this is not an entirely novel concept, the advent of smartphones and tablets has brought on a new wave of interest as the increase in personal mobility and upsurge in working remotely has sharpened demand for access to information anywhere and anytime."[20]

The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to protect their customers' information against security threats. This includes ensuring "the security and confidentiality of customer records and information" and protecting "against unauthorized access to or use of such records or information."[21]

"PEOPLE ARE RETHINKING CLOUD-BASED SOLUTIONS IN SOME SCENARIOS. YES, YOU CAN STORE IN [THE CLOUD], AND YOU CAN FEEL THAT IT'S SAFE BECAUSE THEY HAVE A BIGGER FOOTPRINT AND A BIGGER ABILITY TO DO THE BEST-IN-CLASS SECURITY SOLUTIONS, BUT THEN THEY'RE ALSO THE BIGGEST TARGET."

- ASSOCIATE DIRECTOR, HEALTHCARE INDUSTRY

HIGHER EDUCATION

Institutions of higher education face an array of EFSS demands and challenges, such as a highly mobile user base, high user turnover (as students and faculty arrive and depart each school year), and the expansion of online courses and degree programs. Moreover, the cooperative nature of many educational and research programs often necessitates both internal and external file sharing. Brian Verkamp, IT director for one of the largest colleges within the University of Cincinnati, explains how his team sought to help safeguard collaboration with authors outside of the university without complicating the process for faculty members:

> We've all heard horror stories about sensitive data such as a manuscript stored in the cloud that gets stolen and published elsewhere. We didn't want that happening…[w]e needed a product that would allow us to use our secure local cloud storage but provide features like other public cloud solutions, such as web access and device sync.[22]

Educational institutions must also comply with a range of security regulations, as they typically maintain and transmit a great deal of information about their students in addition to academic records. In particular, they must abide by both HIPAA and GLBA, as well as the Family Educational Rights and Privacy Act (FERPA).

[20] "Enterprise File Synching For Sharing Financial Information," Op. cit.

[21] Scarfone, K., et al. "Guide to Storage Encryption Technologies for End User Devices." NIST, November 2007. http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800111.pdf

[22] "Customer Success: University of Cincinnati." Novell. http://www.novell.com/success/stories/university-of-cincinnati.html

HIPAA and Higher Education

In general, an institution of higher education must comply with HIPAA as a "covered entity" if it provides health care services and engages in one or more of the electronic transactions covered by HIPAA, such as health care claim status, enrollment and disenrollment in a health plan, or first report of injury.[23] Furthermore, regardless of whether or not they provide health care services, many educational institutions are affected by HIPAA because they offer health plan benefits to employees. Institutions must also consider HIPAA rules if they perform research that involves access to protected health information.[24]

GLBA and Higher Education

The Federal Trade Commission (FTC) has made it clear that it considers educational institutions to be "financial institutions" subject to its jurisdiction under GLBA. Because colleges and universities collect and maintain information about their students and others with whom they interact – for the purpose of processing student loans, for example – they must comply with GLBA's safeguarding rules as if they were conventional financial institutions.[25]

FERPA

According to a Congressional Research Service (CRS) report, FERPA, enacted in 1974, guarantees parental access to student education records, while limiting the disclosure of those records to third parties. No substantive legislative changes have been made to FERPA since 2001. However, in 2011 the U.S. Department of Education issued regulations that allow educational agencies and institutions to disclose PII to third parties for purposes of conducting audits or evaluations of federal or state supported education programs.[26] Privacy advocates have raised concerns over these changes, noting that they may pose increased risks to student privacy.[27]

---

[23] Sitko, T. et al. "Life with HIPAA: A Primer for Higher Education." Educause Center for Applied Research, Research Bulletin, 2003:7, April 1, 2003. p. 4-5. http://net.educause.edu/ir/library/pdf/ERB0307.pdf

[24] Ibid, p. 9-10.

[25] [1] "FTC'S Gramm-Leach-Bliley Act Safeguards Rule: Guidelines for Compliance." National Association of College and University Attorneys. NACUALERTS, 1:4, May 16, 2003. http://www.nacua.org/nacualert/docs/GLB_Note_051603i.html

[2] "Privacy Practices and Policies: Gramm-Leach-Bliley Act (GLBA)." The University of Akron. http://www.uakron.edu/ogc/legal-policies-and-procedures/privacy-practices-and-policies/gramm-leach-bliley-act-glba.dot

[26] Feder, Jody. "The Family Educational Rights and Privacy Act (FERPA): A Legal Overview." CRS Report for Congress, November 19, 2013. p. 2. http://www.higheredcompliance.org/resources/publications/CRS_FERPAOverview_2013_11_19.pdf

[27] Ibid. p. 9.

RISK MITIGATION

Highly regulated enterprises value security, and are seeking file sharing and management solutions that will help them comply with regulatory requirements. **In implementing EFSS solutions, regulated enterprises are also interested in mitigating the risks associated with employees using the public cloud to share files.** Public cloud file sharing solutions pose significant challenges for enterprises. Besides security lapses, other challenges include vendor lock-in, illicit access by employees and outsiders, exposed files, co-mingled files, service outages, and vendor viability.[28]

> "THE UNAUTHORIZED ADOPTION OF PERSONAL CLOUD SERVICES RAISES SECURITY CONCERNS AND REPRESENTS A MAJOR DRIVER FOR INVESTMENTS IN EFSS."
>
> - MONICA BASSO, GARTNER

While regulated industries are "beginning to look into the cloud," they **tend to be far more focused on on-site deployment of synchronization and sharing services.**[29] As noted by the Director of Infrastructure for a large regional network of healthcare facilities, these organizations are seeking to build private cloud solutions, or on-site solutions that "can reach over the internet as well."[30] **All respondents from highly-regulated industries who were interviewed for this report state that they are looking for on-site based EFSS solutions,** noting the sensitive nature of their documents, as well as security concerns in general. While some companies in these industries may be interested in the public cloud, they are unlikely to make a switch until security issues are properly addressed.[31] The Chief Information Officer of a private network of nonprofit healthcare centers summarizes his organization's approach succinctly, saying they like to **"keep data on our own servers … we don't trust anybody."**[32]

These findings are echoed by a survey of 334 North American IT professionals conducted by the Enterprise Strategy Group (ESG). Although the survey included IT professionals in large, midmarket, and small organizations, in a variety of industries, it found that 97 percent of **organizations currently using public cloud-based file sharing solutions are interested in on-premises file sharing services.**[33] Nearly 70 percent say they are "extremely interested" in on-site alternatives. Respondents cite "security, the ability to leverage current investments, and concerns about third-party access to sensitive corporate data" as reasons for interest.

---

[28] "Accellion vs. Box: 5 Key reasons Enterprise IT Selects Accellion." Accellion.

[29] [1] Director of Infrastructure for a large regional healthcare network. Phone correspondence.; [2] Vice President, Data Management and Programming, global pharmaceutical company. Phone correspondence.

[30] Director of Infrastructure for a large regional healthcare network, Op. cit.

[31] Vice President, Data Management and Programming, global pharmaceutical company, Op. cit.

[32] Director of Infrastructure for a large regional healthcare network. Phone correspondence.

[33] "Video Blog: The Demand for Hybrid Online File Sharing Solutions" Terri McClure, Senior Analyst, Enterprise Solutions Group, March 25, 2014. http://www.esg-global.com/blogs/video-blog-the-demand-for-hybrid-online-file-sharing-solutions/

OTHER FACTORS

The following figure summarizes comments by respondents to Hanover Research inquiries when asked about key factors that their companies looked for when purchasing EFSS solutions. Responses illustrate that security, including privacy, confidentiality, and encryption, plays a major role in the decision-making process. Another aspect of the purchasing process – rarely mentioned in secondary literature, but of universal interest to decision-makers – is pricing.

Figure 2.4: Commonly Mentioned Factors in Assessment of EFSS Solutions

Font sizes correspond to frequency.
Source: Wordle, Hanover Research

Besides security and pricing, ease of use is considered another primary driver for EFSS adoption in highly regulated industries such as financial services.[34] Workers appreciate solutions that are simple to use, and lack a complicated delivery process because synchronization is automatic. Solutions that reduce the number of mouse clicks and are easy to understand by users are not only preferred by users, this preference helps to drive consistent utilization of the designated tools.[35]

Respondents also note the desire to leverage not only current software and solutions, (for example, collaboration tools like Microsoft SharePoint or corporate address books like Active Directory or eDirectory), but also existing vendors. As the Director of Infrastructure for a large regional healthcare network states, "Certainly we want to leverage existing vendors whenever possible when they have a solution. We have to answer, 'why go outside when they have it?'"[36]

[34] "Enterprise File Synching For Sharing Financial Information," Op. cit.

[35] Ibid.

[36] Vice President, Data Management and Programming, global pharmaceutical company, Op. cit.

TRENDS

MOBILITY

While Gartner's Magic Quadrant rates mobility as a key factor in its evaluation of EFSS solutions, it appears that for highly regulated industries mobility – while important – is not the primary consideration. Several respondents to Hanover's inquiries note that their companies are beginning to look at the mobile-centric EFSS solutions, but that security concerns remain a significant counterweight. According to one respondent, mobility is not a core requirement at present because first the organization must ensure that "the right data is at the right place with the right security." [37] He adds that the mobility features of EFSS are currently seen as a "nice to have, but it's working without." [38]

> "AS IT DEPARTMENTS FINALLY ACCEDE TO USER DEMANDS THAT THEY SUPPORT ANY AND ALL DEVICES, ONE SOLUTION TO STAYING IN CONTROL OF CORPORATE DATA IS EFSS."
>
> - DREW ROSS, ENTERPRISE STORAGE FORUM

By expanding file sharing solutions to reach different mobile platforms, organizations run the risks associated with bring-your-own-device (BYOD) environments. According to a Forrester survey, the top concerns for BYOD all relate to security: 65 percent cite mobile device security as a top challenge facing BYOD deployment, 59 percent cite data breach security, 55 percent consider mobile data security as the top challenge, and 50 percent believe mobile application security is the top barrier.[39]

Based on IBM's X-Force 2011 report, mobile malware and vulnerabilities were expected to grow at least 15 percent year-on-year. [40] And a survey of 1,600 information security workers found that BYOD causes "significant security concerns." [41] Loss of company or client data, unauthorized access to company data and systems, and fear of malware infections are the top security concerns related to BYOD.

---

[37] Director of Infrastructure for a large regional healthcare network, Op. cit.

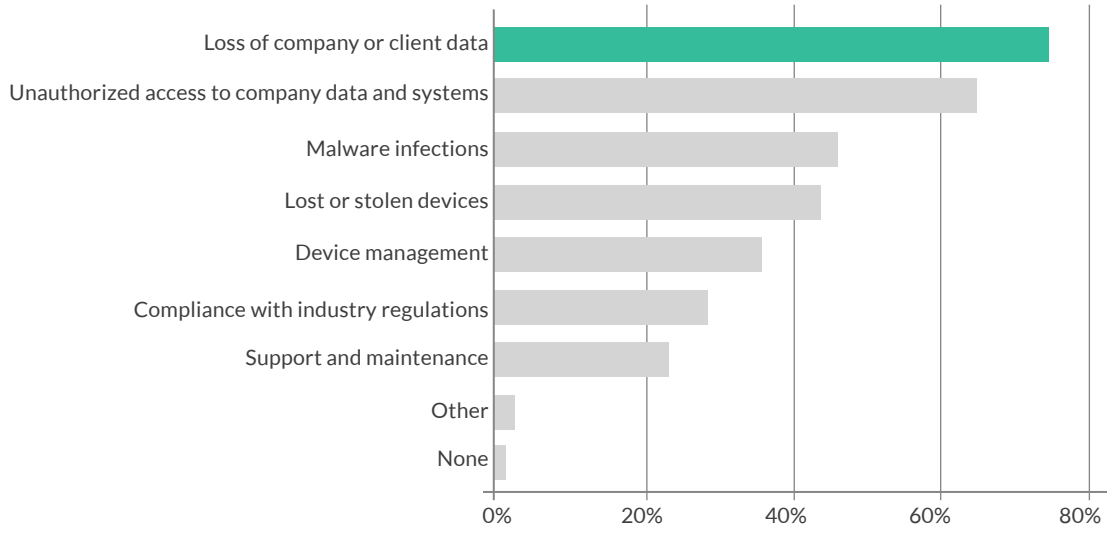
[38] Ibid.

[39] "Bring your own device." EY, September 2013. http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf

[40] Williams, J. "Mobile malware is on the rise, warns IBM report." Computer Weekly, September 30, 2011. http://www.computerweekly.com/news/2240105733/Mobile-malware-is-on-the-rise-warns-IBM-report

[41] "BYOD & Mobile Security." Lumension. http://blog.lumension.com/docs/BYOD-and-Mobile-Security-Report-2013.pdf

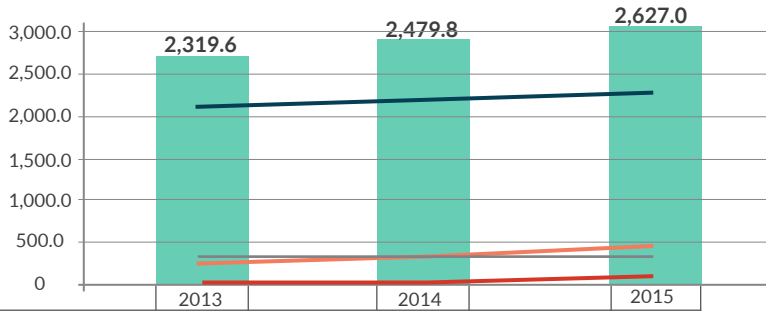
Figure 2.5: Main Security Concerns Related to BYOD



Source: Lumension[42]

While Hanover's inquiry respondents tend to downplay the importance of mobility as a factor in their purchasing decision, Monica Basso, of Gartner, notes that **"the proliferation of consumer mobility, media tablets and bring your own device programs in the enterprise is increasing adoption" of EFSS solutions.**[43] Global shipments of devices, including personal computers (desktops and laptops), tablets, ultramobiles, and mobile phones, are expected to reach about 2.5 billion units in 2014, an increase of nearly 7 percent over 2013 shipments. By 2015, shipments are expected to increase to over 2.6 billion units.

Figure 2.6: Worldwide Device Shipments (in millions of units)



	2013		2014		2015
Total	2,319.6		2,479.8		2,627.0
PCS	296.1		276.7		263.0
Tablets	195.4		270.7		349.1
Mobile Phones	1,807.0		1,895.1		1,952.9
Other Ultramobiles (hybrid and clamshell)	21.1		37.2		62.0

Source: Gartner[44]

[42] Ibid.

[43] Robb, D. "Ten Things You Need to Know about Enterprise File Sync and Share." Enterprise Storage Forum, May 21, 2013. http://www.enterprisestorageforum.com/storage-management/ten-things-you-need-to-know-about-enterprise-file-sync-and-share.html

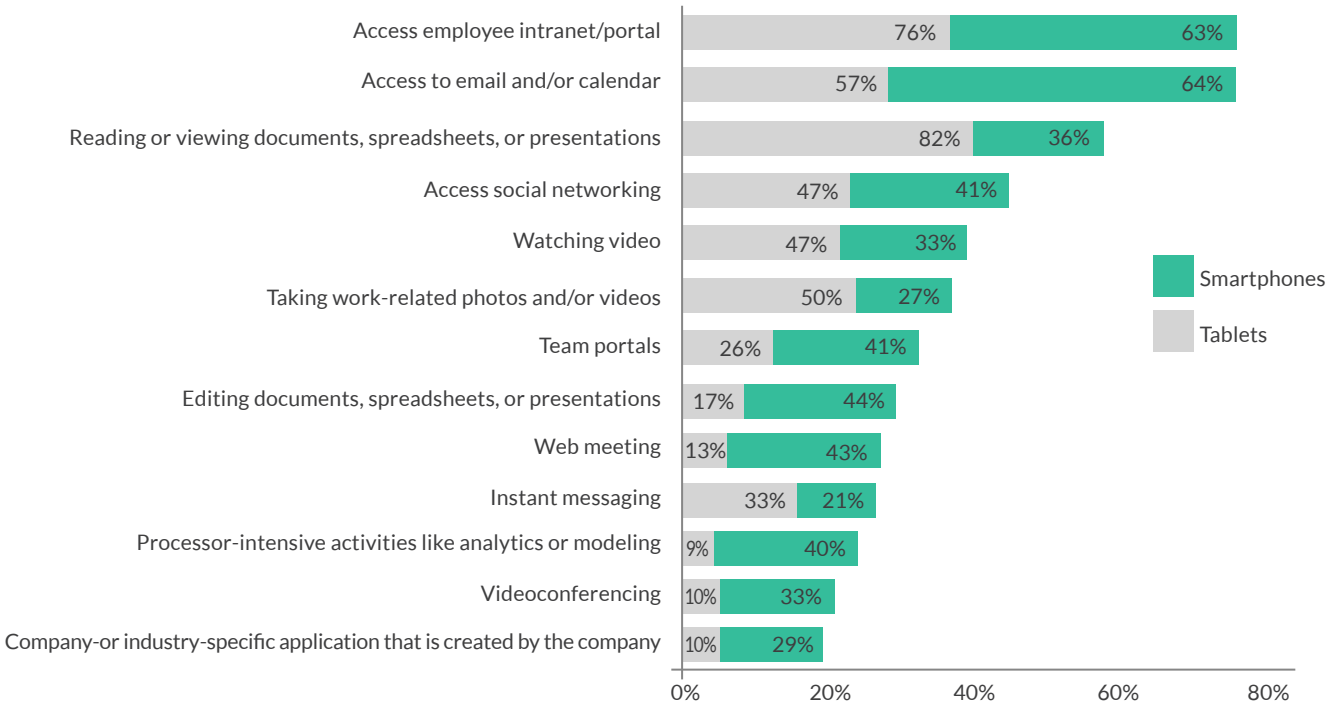
[44] "Gartner Says Worldwide Traditional PC, Tablet, Ultramobile and Mobile Phone Shipments Are On Pace to Grow 6.9 Percent in 2014." Gartner, March 27, 2014. http://www.gartner.com/newsroom/id/2692318

As Forrester notes,

> Corporate mobility momentum will continue as an increasing number of employees purchase and use their personal smartphones for work-related activities, and a growing number of enterprises support [BYOD] programs to cost efficiently mobilize their workforce.[45]

According to a study conducted by Forrester in February 2012, 82 percent of employees use smartphones to access and read documents, spreadsheets, or presentations. About 44 percent of employees use tablets to edit documents.

Figure 2.7: Smartphone and Tablet Use by Employees



Source: Gartner [46]

According to CompTIA's 3rd Annual Trends in Enterprise Mobility study, about 50 percent of large firms have a partial or full BYOD device deployment, compared to nearly 60 percent of both medium-sized and small firms.[47] Organizations that have implemented EFSS solutions that are supported by various mobile platforms focus on the "big three" operating systems: iOS, Android, and Windows.[48] Respondents note that they find no need to support other mobile platforms.

---

[45] "The Expanding Role Of Mobility In The Workplace." Forrester, February 2012. https://www.cisco.com/web/solutions/trends/unified_workspace/docs/Expanding_Role_of_Mobility_in_the_Workplace.pdf

[46] Ibid.

[47] "Bring your own device." EY, September 2013. http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf

[48] Williams, J. "Mobile malware is on the rise, warns IBM report." Computer Weekly, September 30, 2011. http://www.computerweekly.com/news/2240105733/Mobile-malware-is-on-the-rise-warns-IBM-report

INTEGRATION

According to most respondents, the ability to integrate EFSS solutions with current enterprise software and programs is also relatively unimportant, when compared with security requirements. Several respondents state that their companies have disparate file sharing software and solutions for different departments and groups of users. For example, a Vice-President in the IT department of a large pharmaceutical company notes that his company has "thousands of tools to share documents," including document management systems, SharePoint, and both internal and external file sharing systems, such as SSTP.[49]

However, according to an associate director of a healthcare organization, **there is a big push towards the integration of different applications and solutions,** "to make them talk to each other, and reduce the manual transfer, verification and re-verification of data."[50]

[49] Vice President, Data Management and Programming, global pharmaceutical company, Op. cit.

[50] Anonymous respondent. Phone correspondence.

APPENDIX A: PARTICIPANT INTERVIEWS

This report is presented as a synthesis of quantitative market research, analyst commentaries, and original primary-source interviews conducted by Hanover Research with knowledgeable IT leaders within highly regulated enterprises.

Figure A.1 provides a summary or "snapshot" of the industry sources who shared their insights and perspectives, who (in order to promote open dialogue during interviews) Hanover Research agreed not to identify by name or company affiliation.

Figure A.1: Participating Industry Sources

Participant Titles:

- *Chief Information Officer*
- *Director of Infrastructure*
- *Vice President, Data Management and Programming*
- *Director, Data Management and Reporting*
- *Associate Director, Clinical Programming*
- *Executive VP of IT*
- *Database Analyst III*

Industries Represented:

- *Healthcare*
- *Financial Services*
- *Higher Education*

Average Number of Employees at Participant Firms: *18,516*

Average Annual Revenues of Participant Firms: *$14.2 billion*

APPENDIX B: ABOUT THIS REPORT

REPORT SPONSORS

Novell, Inc. - At Novell, we design and build software that makes people more productive and work environments more secure and easier to manage. We support thousands of organizations around the world with products that enable your work force in the office and on the go. These solutions include endpoint management, collaboration, and file and networking solutions. Learn more at **www.novell.com**

Attachmate Corporation - For 30 years, Attachmate has been helping organizations to extend, manage, and secure their essential business information. Today, our products run on 19 million desktops and mobile devices worldwide. Built to integrate existing systems and emerging technologies, they make it possible for you to put your IT assets to work in new and meaningful ways. Learn more at **www.attachmate.com**

ABOUT HANOVER RESEARCH

Hanover Research is a global information services firm providing knowledge support to both non-profit and for-profit organizations. Through our unique, fixed-fee model we deliver customized, timely, and authoritative research and advice enabling our clients to make informed decisions, identify and seize opportunities, and heighten their effectiveness.

Within the for-profit space, B2B and B2C executives apply Hanover Research's market trends, competitive intelligence assessments, and data insights to guide product development, size market opportunities, and gauge brand perception. These insights inform corporate strategy – enabling companies to work smarter to drive revenue and ensure customer satisfaction.

To learn more about Hanover Research's services and our unique model, contact **202.559.0050** or e-mail **info@hanoverresearch.com**

HANOVER RESEARCH

4401 Wilson Boulevard
4th Floor
Arlington, VA 22203
P. 202-559-0050
E. info@hanoverresearch.com
www.hanoverresearch.com

FOLLOW US FOR ONGOING INSIGHTS

@Hanover4Biz **www.linkedin.com/company/hanover-research**