State of File Collaboration Security

File Insecurity: The Final Data Leakage Frontier

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for FinalCode, Inc.

September 2015

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Table of Contents

Executive Summary

Data dissemination and file collaboration are natural parts of most business and operational workflows, thus security must be an integral part of the workflow to protect information.

The diversity of devices and mechanisms to share files has grown exponentially over the past decade, particularly with increased adoption of bring your own device (BYOD), enterprise mobility, cloud-based applications, and next-generation content manager systems. At the same time, the growth of sophisticated attacks and malware have increased the probability of network, application, and system breaches as well as the risk of ensuing unauthorized data access. Lastly, the heightened awareness of data breaches in government and business sectors continues to drive additional legislative and commercial data privacy compliance requirements with regard to safeguarding confidential and regulated data. These factors have placed greater demands on IT and information security professionals to re-examine their organization's data leakage/loss programs.

Unfortunately, the protection of sensitive, confidential, and regulated data within files being shared both internally and externally remains a significant source of exposure within many organizations. This lack of capability for controlling unstructured data as it moves through its lifecycle will not only yield more data privacy breaches, but will impact the adoption of advanced enterprise and cloud content management systems.

This ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) research report, *State of File Collaboration Security*, offers insights into file data leakage risks and incidents, security process and control maturity, perceived cloud-based file platform threats, and anticipated investments that attempt to preempt file access and usage exposures. Sponsored by FinalCode, the research serves to provide IT professionals an understanding of where their organization sits on the file security spectrum, how staff may need to re-examine their policy and controls considering file collaboration risks, and new file collaboration risks, and how organizations should move to close file data leakage gaps.

The report reveals that all responding organizations expressed significant concern for risk of data leakage due to inappropriate sharing or unauthorized access to files containing sensitive, confidential, or regulated information. Correspondingly, more than 80% of survey participants experienced file data leakage incidents in their organization and 50% expressed frequent incidents. While the majority of IT organizations have enhanced technical controls and auditing, only 16% of the respondents felt highly confident in their file security investments, indicating an underlying insecurity in monitoring and enforcement capabilities.

Fortunately, the vast majority of respondents across IT, security, and line of business roles indicated that their organizations plan to invest in stronger security controls. The research also focused on security risks with regards to file collaboration. Survey respondents indicated that inappropriate file sharing with others inside the organization, inappropriate file sharing with those outside the organization, and unauthorized file access through malware and hackers were the most likely causes of data leakage in their organization.

Many organizations are assessing their enterprise content manager (ECM) systems and are exploring cloud-based enterprise file sharing and synchronization (EFSS) platforms. However, despite the need and heightened interest in the EFSS platforms, more than 90% of respondents stated the lack of protection of files leaving cloud-based platforms or device containers as the highest risk to adopting cloud-based file storage and collaboration services.

While policy development and legal enforcement were cited as the most mature nontechnical control options, organizations are increasing their investments in user awareness training programs and plan to purchase additional security technology to manage, monitor, and enforce policy and training initiatives. The research found that email gateway/proxy technologies were the top mature technical controls, but that file encryption and usage control software and enterprise mobility management were among the top upcoming technical control investments. Eighty-two percent of the respondents have funded projects to investigate file encryption and usage control software with the intent of purchasing in the next year.

The research polling and analysis were completed by EMA in September 2015. The survey targeted information security decision-makers in midmarket and enterprise organizations across multiple industries in North America. Respondents were comprised of 153 senior IT, information security, and line of business professionals that are responsible for information technology purchase decisions in their organization (see disclosure section).

Managing Data Loss/Leakage

Data security has become a huge focus for businesses and individuals alike. According to digital security company Gemalto and its *2014 Breach Level Index*[1] report, 2014 saw over one billion records[2] stolen from organizations from every vertical, including financial, education, fast food, retail, health care, government, and high tech. No vertical seemed to be immune to the assault.

Knowledge is power and its value is gained through the accumulation of information. Because of these factors, information thieves, both external and internal, are highly motivated to persist in their attacks using as diverse methodologies as they can muster or afford. Records are stolen from hacks against vulnerable networks, systems, and software via malware and malicious-link embedded phishing campaigns and malicious sites, credential scraping from compromised websites and databases, and even compromises through third-party suppliers.

Aside from the onslaught of hackers out to steal information, organizations are leaking data due to insiders. The problem is not just malicious insiders who seek to take or destroy information for their own gain or out of some twisted sense of justice, but insiders who innocently, but inappropriately, share information during their daily work duties. This is especially common in collaborating work groups as only the most meticulous personnel tend to understand the data management requirements, and of those personnel only the most disciplined strictly obey those requirements.

Our *State of File Collaboration Security* report found that twenty percent of respondents believed that data leakage from internal, inappropriately shared files was the largest threat to their business. Secondly, 11% of respondents perceived that their largest threat came from information being shared inappropriately outside the company. Files stolen by hackers came in third at 10%. This perception is highly interesting because the world at large has some level of quantification concerning how many data records are leaked via breaches, but there is little quantification around how much data is inappropriately shared, either accidentally or intentionally. With all of the media attention around stolen records, for internally shared records to be at the top of people's minds means this is likely a widespread issue.

[1] http://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf
[2] 1,023,108,267

File Data Leakage: Concerns, Control, Confidence, and Investment

Research from this project identified that all organizations are concerned about data loss or leakage due to unauthorized and/or inappropriate sharing of sensitive files. In detail, 75% of organizations were highly to very highly concerned about data loss or leakage, while 25% were moderately concerned. Due to this concern, organizations are seeking solutions to their data leakage and data breach problems. Many technologies are under consideration, but data protection using encryption coupled with persistent rights management was highly favored.

The concern over unauthorized and/or inappropriate sharing of sensitive files seems to be tightly coupled with the fact that many respondents felt their organization has insufficient auditing and technical controls to validate the security of their data. According to the research, only 16% of the respondents were highly confident that these auditing and technical controls were in place and effective. On the other hand, 84% of respondents were between moderately confident and not at all confident that the controls and auditing were in place, illustrating a general lack in confidence.

Participants were also asked how their organizations were dealing with the gap in controls. All of the respondents said their organizations were pursuing additional policies and procedures to reduce data leakage/loss. However, just increasing policy is an insufficient strategy. Though it will improve the situation, it is only a small incremental improvement since policy changes by themselves cannot measure change; enforcement and reporting are necessary to sufficiently maintain controls to validate data. As the old saying goes, "If we cannot measure something, we cannot improve it." Fortunately, all of the demographics in the research said their second highest initiative to address this problem is a technology investment. Just over 90% of enterprise participants and 84% of midmarket respondents indicated their organizations were going to make a technology investment to manage data leakage. When analyzed by respondent role in the organization and grouped by IT, information security, and line of business function, between 87% and 90% of organizations were planning to invest in a data security technology.

Concerns

There was a significant level of concern about file security from respondents across all survey demographics and industries that sensitive, regulated, or confidential data held in files is being accidentally, inappropriately, or maliciously leaked.

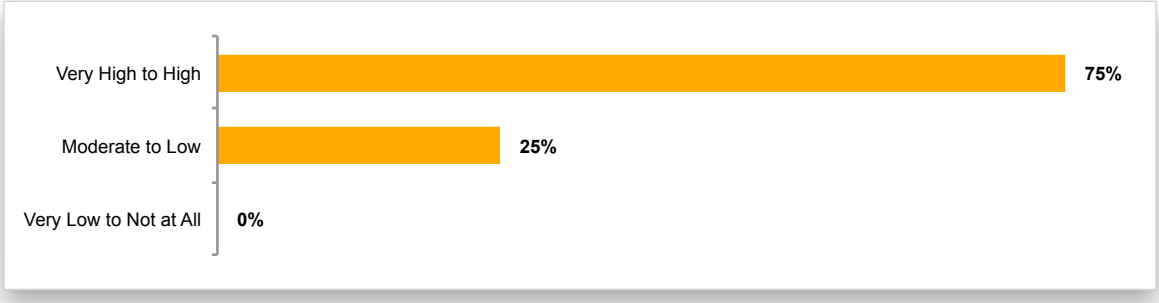

Figure 1. Level of Concern: Risk of Data Leakage Due to Inappropriate Sharing or Unauthorized Access

Controls Confidence

The majority of respondents were only moderately confident in their organization's technical controls or ability to audit sensitive data leakage from sharing or collaboration. Only 16% had high confidence. This means that 84% had between a moderate to total lack of confidence in file security monitoring, reporting, and policy enforcement capabilities.

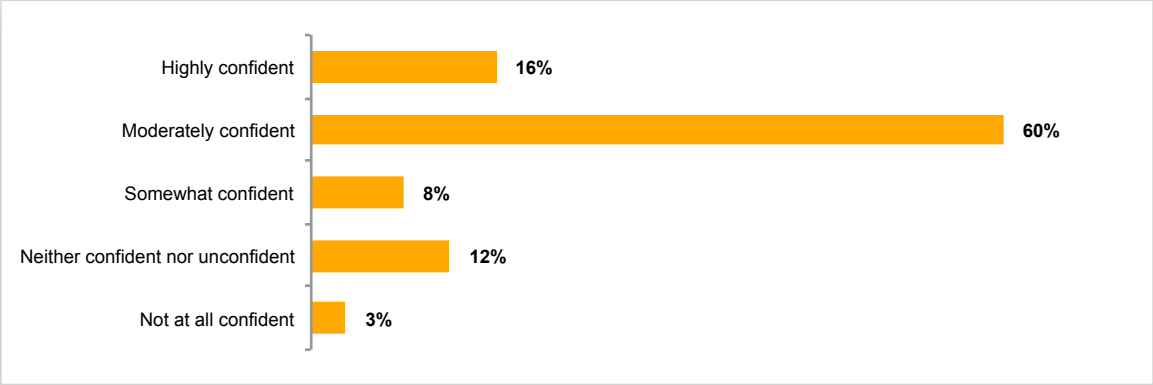

Figure 2. Level of Confidence in Organization's File Security, Technical Controls, and Auditing

Methods

While medium and large enterprises have invested in both policy development and process documentation (essentially best practices), they also planned to invest in technology and security awareness training to manage file security risks.

Figure 3. Methods Organizations Are Using to Improve Security and Reduce File Sharing Services Risk

File Security: Incidents, Occurrences, and Impacts

Eighty-three percent of respondents indicated their organizations experienced data leakage/loss from inappropriately shared data or unauthorized access to data and 50% of the respondents were aware of these incidents happening frequently. This is a pretty staggering number and also relates directly to the overall level of concern respondents had with this issue.

Fifty-four percent of respondents believed some form of inappropriate sharing was the most likely source of data leakage/loss while only 19% felt that leakage/loss from some sort of hacking attack was most likely. Only 18% felt that data from lost or stolen media, including electronic and/or paper documents, and devices was a likely source of leakage/loss. Lastly, only about 9% of respondents felt that an insider was their most likely threat for data leakage.

One the other hand, respondents were asked about the greatest impact from leakage/loss events. In this case, 42% of respondents believed that inappropriate sharing and unauthorized access was the largest impact to the organization. This goes against what we tend to hear in the media, but is probably closer to reality. It is not exciting and therefore not reported in the news. Eleven percent felt that data stolen by insiders has the largest impact while 25% felt that information from lost or stolen media, electronic and/or paper, and devices is most impactful. Twenty-five percent of respondents perceived that the largest impact is from information lost to hackers.

The comparison of these two measurements creates a noteworthy picture. Though there is some variance between likelihood and impact, respondents still perceived that inappropriate sharing and unauthorized access of data exceeds the impact from hacking.

Incidents

Eight-three percent of participants were aware of data leakage incidents occurring in their organization and 50% cited that they happened frequently. When combined with the perceived lack of technical controls and auditing capacity, the risk of file data leakage appears more significant and is likely underestimated.

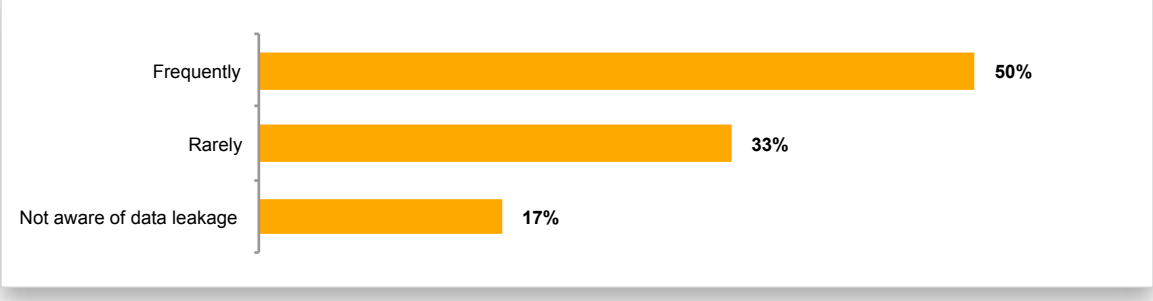

Figure 4. Frequency of Data Leakage from Shared Content or Unauthorized Access

Occurrence

Respondents cited internal file sharing exposures as being twice as common as the other data leakage types. External file sharing issues were ranked second as most likely to occur. Combining hacker and malware activity as external attacks, which results in a 19% response, indicates a need for a layered defense approach such as user, access, and device activity monitoring.

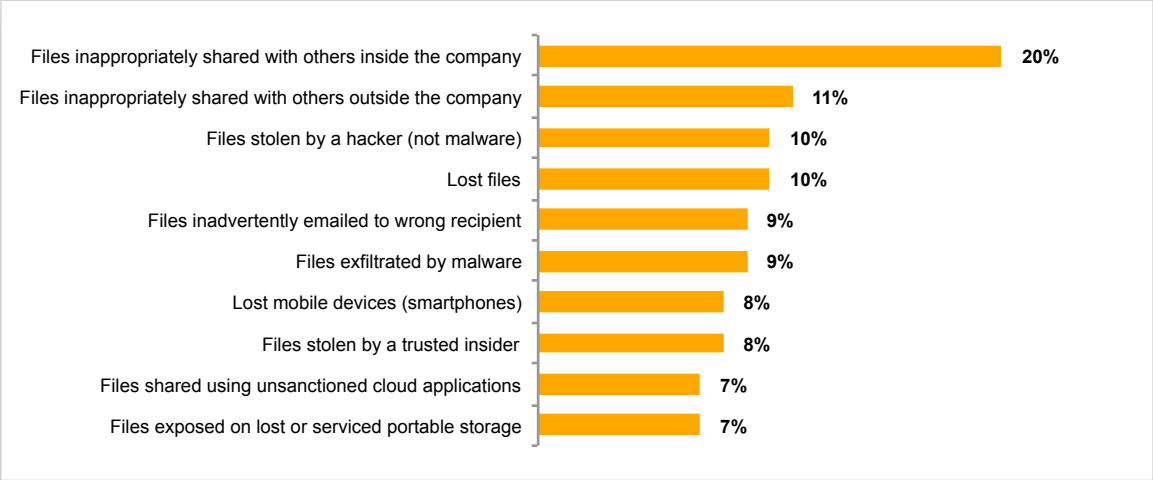

Figure 5. Which Do You Believe Is the Most Likely Occurrence of Data Leakage Within Your Company?

Impact

Though respondents indicated higher risk exposure for internally shared files, externally shared file risks were cited as most impactful. Despite maturity in endpoint security, data leakage from malware was a close second in impact, followed by insider threat risks.

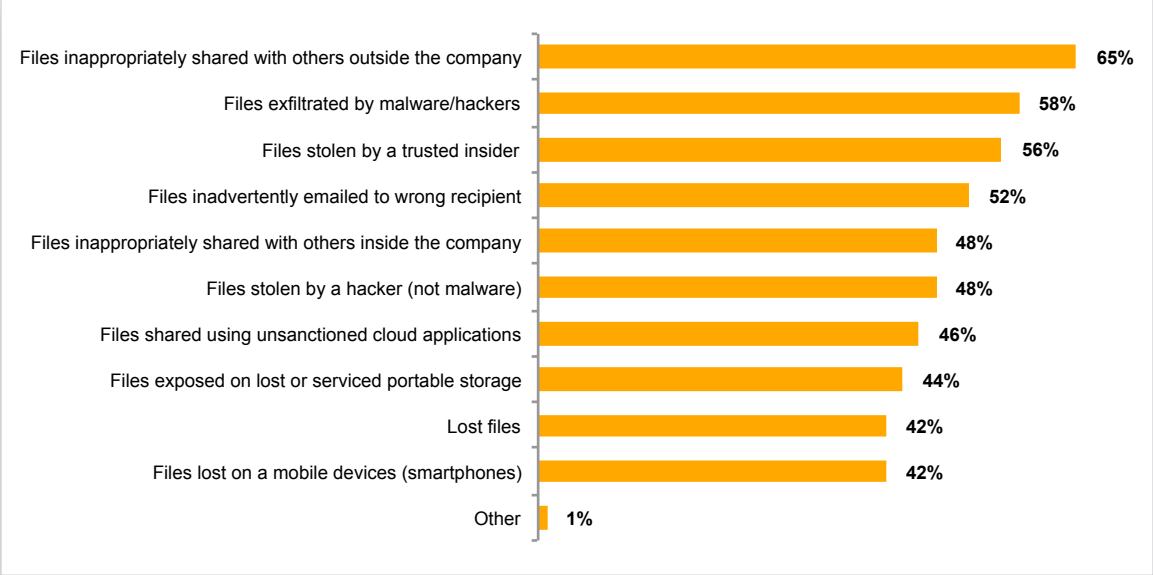

Figure 6. Most Impactful Data Leakage in Organization

File Security Adoption

A 2013 research project by SkyHigh Networks[3] which used data from over three million users determined that, on average, personnel had company data in 545 cloud services while the highest ranking organization had its data in 1769 cloud services. With the proliferation of data sharing applications and cloud services on top of the existing use of email for collaboration, the risk of data leakage and exposure is climbing almost exponentially.

Our research participants were asked about their perception of the top risks in relation to adopting cloud-based file storage/collaboration services. In response, 91% said that their top concern was the lack of ability to protect the files leaving the cloud service repository—essentially, the ability for a recipient to take a file out of the "cloud folder" and put it in a location that is outside of the cloud service provider's controls. This is encouraging as it shows concern for the company data and recognition of the lack of persistent file protection. The second largest concern was the use of the actual platforms. Eighty-eight percent recognized that just by using collaboration services/platforms, the organization's risk increased. The third concern was the lack of means to secure the files using other collaborative mechanisms. Through sharing, a privacy issue is created. The sharing service did not have fine/granular enough control over the data.

When evaluated together, the collection of data points is even more telling than the singular points. This shows us that, as stated earlier, sharing is intrinsic to many organizations and, to get their jobs done, personnel are willing to accept or at least tolerate risk in order to share information despite the possibilities of leakage and other exposures to the business.

Eighty-seven percent of the participants that identified themselves as holding information security positions said their organizations already had a project underway to invest in stronger file security tools and technology. Respondents holding IT positions were only one point behind that. However, the line of business respondents were less in-the-know and were 10 points behind security personnel.

This indicates that executive management accepts that file sharing is taking place that it is a necessary part of operations, and therefore it must not only be facilitated, but secured. This means that executive management must direct IT and security organizations to meet the business need for sharing and simultaneously reduce the risk of that sharing.

[3] Infographic: Cloud Adoption and Risk 2013

Control Maturity

Of the file security controls implemented by respondents, email proxy/gateway solutions were cited as the most mature and active form of technical control, with policy and legal enforcement rated as the most utilized nontechnical control. Enterprise Content Management (ECM) adoption were also similarly popular as being used to protect access to internal files. Companies are also commonly employing encryption and usage control technologies.

Figure 7. Top Five Controls Organizations Are Using to Secure Files in Their Organization

Popular Approaches

Email gateway/proxy technologies are far more actively deployed than data loss prevention (DLP) technologies. Email proxies have an impact on spam, antimalware, and other threats. DLP offers a means to create a data classification policy based on content inspection, but with any automated filtering technology, it can be resource intensive and is prone to false positives and exceptions.

Both enterprise mobility management and enterprise content management represent additional layers of access control. With the adoption of bring your own device enterprise initiatives, EMM is very much a purchase consideration while ECM solutions may begin to fall short of new/expanded inter-organizational data classification, access, sharing, and collaboration requirements.

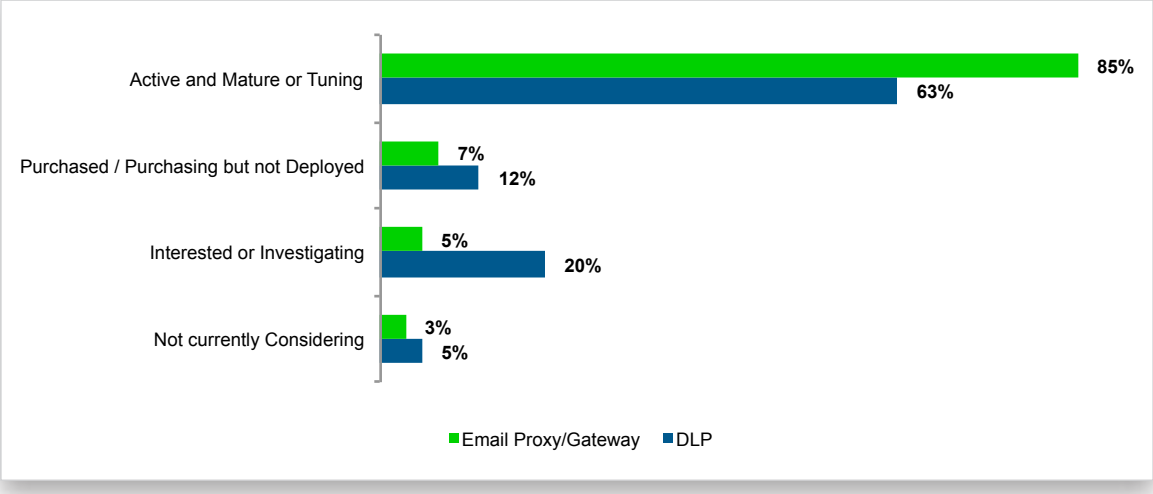

Figure 8. Comparing Organizations' Control Adoption: Email Gateway/Proxy to DPS

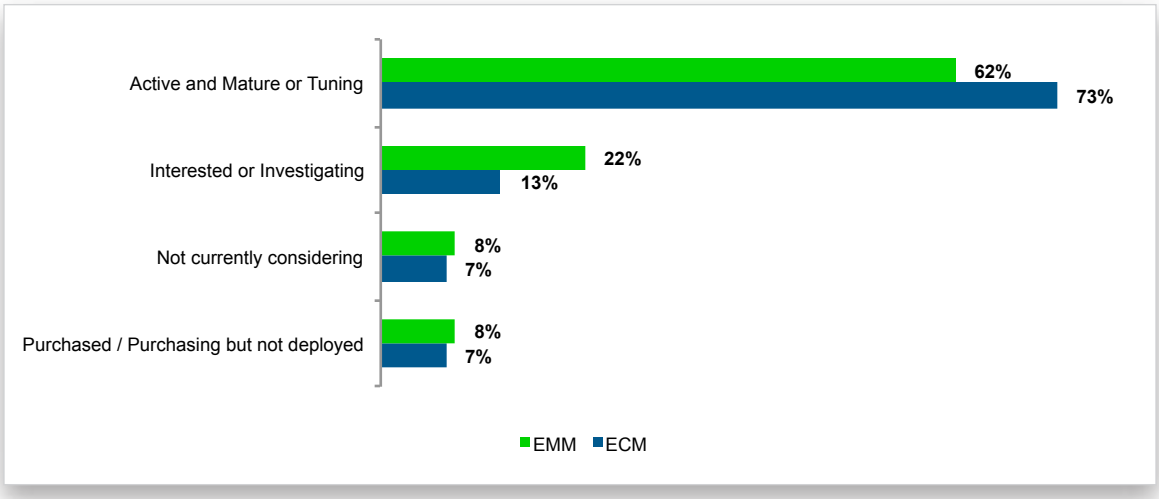

Figure 9. Comparing Organizations' Control Adoption: EMM to ECM

Planned Purchases

"File encryption and usage control software" tied with "portable storage devices" for the most common project organizations have underway to facilitate file sharing. One aspect to further investigate is the overlap in respondents who indicated both. Using portable media without encryption is at least as risky, if not more so, than using electronic transfer means due to the possibility of data leakage/loss from lost media. There is hopefully a high correlation between the two answers to protect the portable media.

Figure 10. Top Five Technologies Being Investigated or Purchased in the Next 3-6 Months

Cloud File Sharing

Top Perceived Risks

The survey findings show material concerns with regard to securing file data in cloud storage, sharing, and collaboration platforms. The most significant issue identified was how to secure data leaving a cloud sharing repository and how to secure it once it leaves a container.

The risk due to lack of controlled access to unauthorized cloud file sharing and collaboration tools are also a top concern.

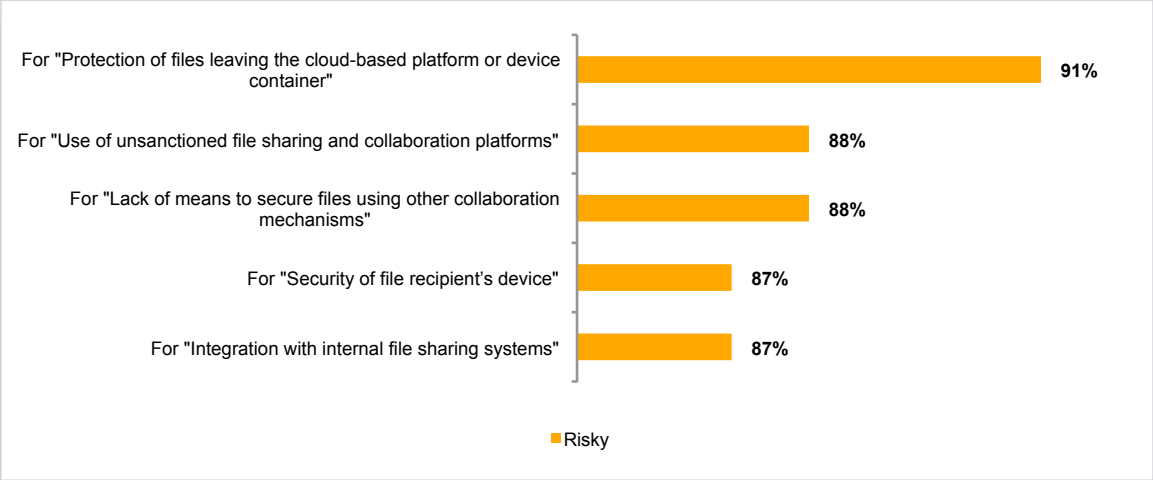

Figure 11. Top Five Perceived File Security Risks Facing Cloud-based File Storage/Collaboration

Stronger Controls

Seventy-nine percent of respondents cited their organizations as either having or investing projects to improve security around cloud-based sharing platforms. IT and security respondents that are closer to the solutions revealed a significantly higher number of projects currently in the investigation stage.

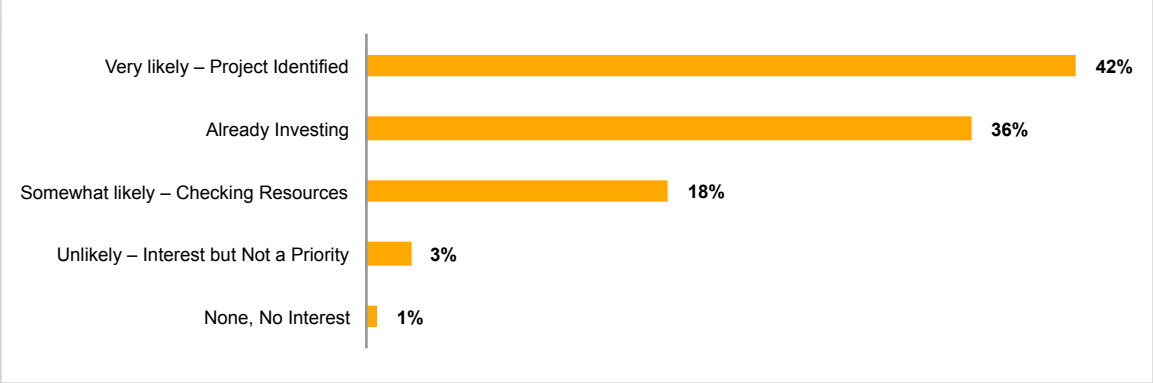

Figure 12. Likelihood to Implement Stronger Security Capabilities to Support Cloud ECM/Collaboration

File Protection: IRM Control Concerns and Adoption

EMA asked respondents to identify their top five concerns with using file encryption.

1. **Key Management, 86%** – In most cases, this concern is based upon a previous personal experience respondents had managing keyrings and other similar structures both as a sender and a receiver of shared data.
2. **Encryption Strength, 85%** – This is more of a perceived issue than a real issue. Though there have been issues with encryption implementations, such as recent issues with SSL flaws like Heartbleed, Poodle, and FREAK, most individuals felt that in the wake of all of the data breaches they wanted to be sure that the encryption would be effective, but they had no real-world examples of how it had failed other than the SSL issues, which are not relevant to data at rest.
3. **Impact to Data Recipients, 83%** – Organizations are concerned with usability and the impact encryption and usage control will have on productivity and workflow. This concern is not only for internal users, but also those outside the organization such as contractors, partners, and customers.
4. **Impact to Operational Workflows, 81%** – This concern is based on legacy implementations and the necessity to encrypt files outside of the email or other sharing mediums, which can be inconvenient and may impact productivity.
5. **Interoperability with Existing Applications and Infrastructure, 81%** – This concern can stem from a number of scenarios, including experience with public key infrastructure (PKI) systems and encryption technology that did not integrate with either email clients or application databases, causing various business operations impacts.

The general perception in the user community is that file encryption/protection is secure, but there is fear of business impact and introducing a high degree of user friction. This perception is not historically unfounded, as it is based upon experience with previous Information Resource Management (IRM) solutions that could be highly impactful to the user workflow and productivity as well as to external recipients.

IRM Inhibitors

Research investigated respondents' concerns with encryption and entitlement controls to better understand why they may not use purchase, deploy, or use them. Key management had the highest concern among respondents, but was closely followed by all other categories.

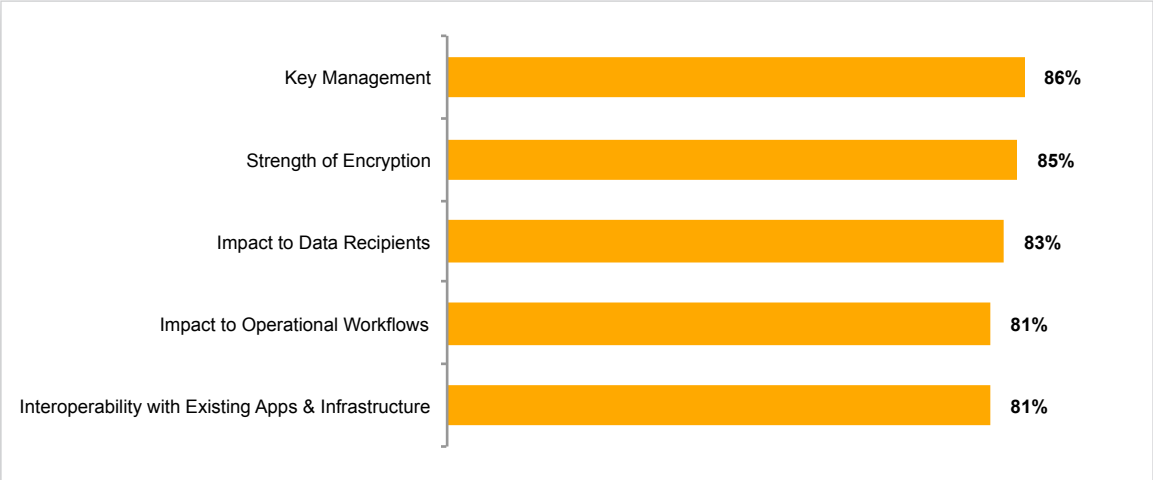

Figure 13. Concerns with Implementing Encryption and Entitlement Controls

IRM Adoption

Information resource management or eDRM (digital rights management) has been around for quite some time. Many integrated eDRM solutions—which encompass data discovery, classification, and policy management—have been found to be complex and thus more challenging to use and support. Research data suggests that specialized encryption and entitlement solutions are less complex, apply to broader use cases, and may more easily accommodate users outside the organization.

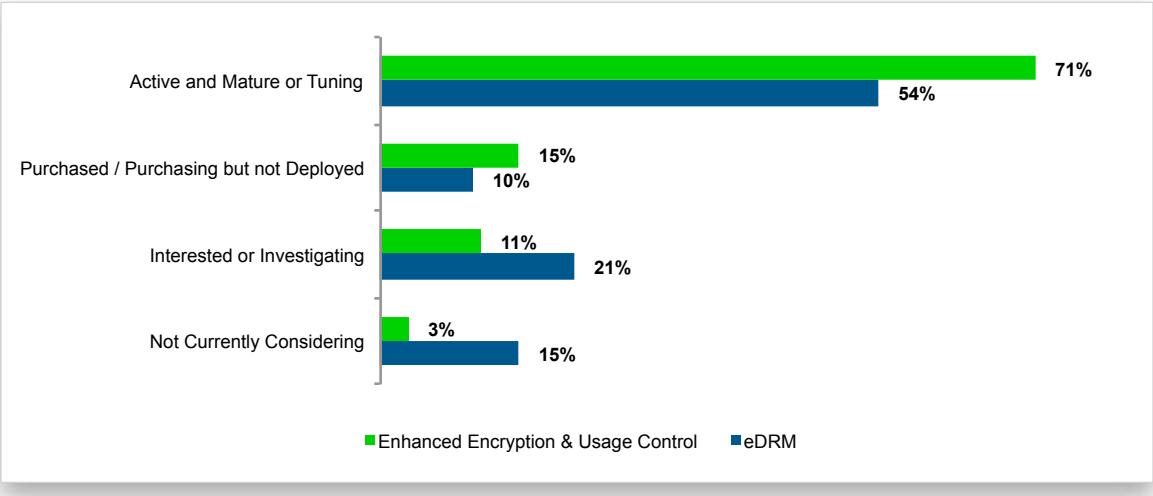

Figure 14. Comparing Organizations' Control Adoption: Enhanced File Protection

File Security: Policy and Enablement

As mentioned earlier, all of the participants indicated that their organizations were reviewing and, as necessary, adopting further data protection policies. However, 79% of the respondents also recognized that they needed additional technical controls to manage, monitor, and enforce those policies and were investing in projects to address these needs.

Respondents recognized the gap between policy and enforcement capabilities, and 70% of them were "confident" to "highly confident" that the personnel in their organization would leverage stronger security controls to protect shared data if they had it. A general premise of the responses gathered from additional conversations was "if it [the security control] was very low friction." As with all solutions in this area, though people want to protect data, they also want to be more productive. This means that solutions that impact productivity are not well received and are generally a no-starter for implementation and/or adoption.

Policy and Legal Enforcement

Every organization and role said they have policy documentation and used legal enforcement to protect data. Policies and legal controls set the bar for how data should be classified and handled. However, organizations need more active defenses to manage file access risks.

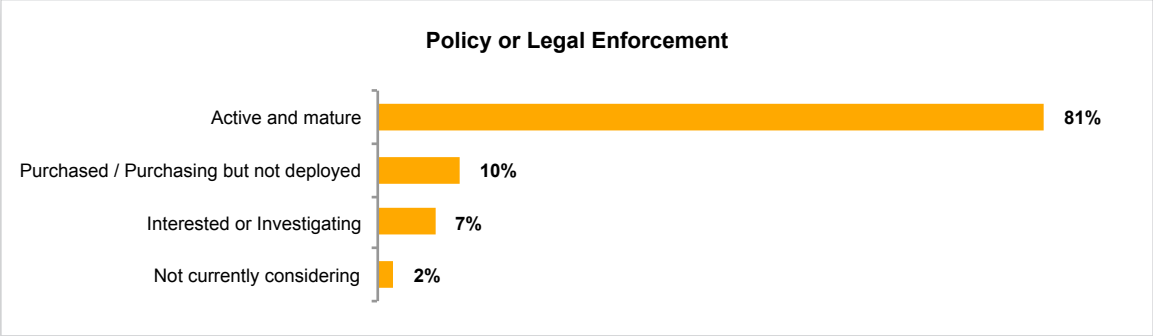

Figure 15. Extent Technical Controls Are Currently Applied to Protect Shared Files/Data

Enablement

Organizations must establish file usage and protection policies to be adopted by end users. Even in conjunction with advanced, automated data classification and filtering and monitoring tools, companies can still rely on levels of user enforcement if protection policies are clear and the impact to usability and workflow remains nominal.

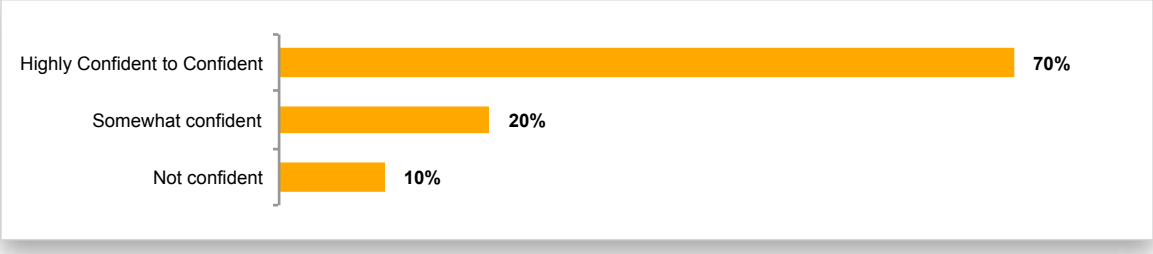

Figure 16. Confidence that Personnel Would Invoke Stronger Security Controls on Shared Data If Empowered

EMA Perspective

Today's solutions for encrypting and protecting unstructured data have evolved significantly over solutions of the past. Workflow integration and access control persistence have given these solutions capabilities that combine the access control and tracking strengths of enterprise content management (ECM) solutions with the content management and data protection of digital rights management (DRM) solutions. This is probably why next-generation file encryption and usage control tools ranked higher than both of these solutions in the technologies being considered for investment.

The real improvements in next-generation data security tools are not the encryption capabilities, but the usability, key management and business workflow integrations that make access virtually seamless for both the senders and the recipients. A significant consideration for the adoption of these tools will be the degree of transparent operation within an organization, the ease of deployment and scalability, and the extent to which users outside an organization can be on-boarded and productive. Additionally, the ability to support access control and protect content as the files are shared across enterprises and cloud services is crucial. The latter will be a key differentiator among not only previous and next generation tools but also between the next generation tools vying for market share.

File owners have the flexibility to add recipients' access, modify usage entitlements, and even revoke access for recipients that are removed from a project or found to be errantly added. This on-demand capability removes access in real time to not only reduce the exposure window, but address multiple compliance requirements. This is especially important when the recipient may not be inclined to comply with the disposal request or feels that he/she has an opportunity to gain from the error.

As data leakage incidents, information theft, and public breach notifications increase, the importance of file and shared data protection will continue to increase. Organizations both public and private, large and small that require data sharing and collaboration as part of their workflows and business models will make identifying and investing in enhanced file security platforms a top priority.

Disclosure

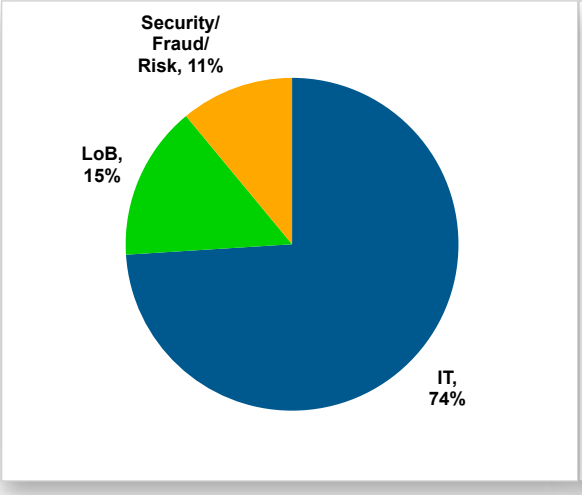

Figure 17. Respondent Roles

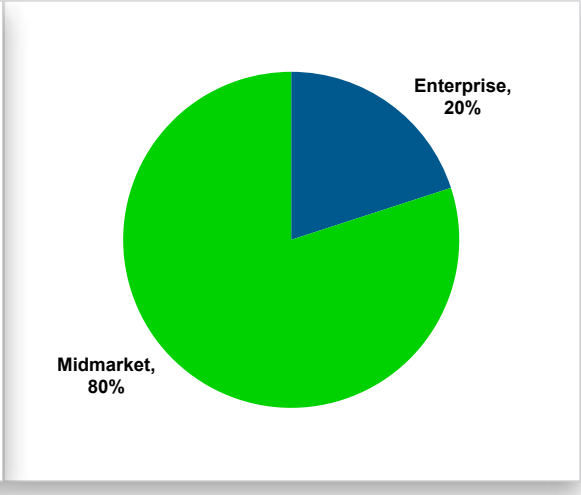

Figure 18. Respondents' Organization Size

The research survey and analysis were completed by EMA in September 2015 on behalf of the sponsor, FinalCode, Inc. The survey tapped information security decision-makers in midtier enterprises (companies with 500 to 2500 employees) and large enterprises (companies with greater than 2500 employees) across multiple industries in North America. Respondents comprised 153 senior IT, information security, and line of business professionals that are responsible for information technology purchase decisions in their organization. Since IT and security are in the unenviable position of being held responsible as data custodians, their responses are of particular value. The majority of respondents represented IT, and 35% of the respondents represented senior leadership—IT directors, VPs, CIOs, or CTOs. This particular demographic within IT is also an important group as they are most often responsible for data protection within their organization.

About EMA

Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on LinkedIn, Twitter, and Facebook.

Research Sponsor: FinalCode

FinalCode offers organizations the ultimate means to secure sensitive files wherever they go within and outside the corporate network. Available as a SaaS or virtual appliance offering, FinalCode delivers enterprise-grade file security that works with popular applications, file storage, devices, cloud, and content management systems and across all communication channels: trusted, untrusted, private, or public. The solution allows for user-defined and corporate policy-enforced file security with an extensive array of granular controls and the ability to remotely delete files. The company's patented CryptoEase™ technology streamlines file security and encryption processes without requiring the user to remember passwords, and by dramatically reducing key management overhead, makes implementation of FinalCode rapid and scalable. Headquartered in San Jose, California, FinalCode offers its solutions through its global network of authorized partners. Learn more at http://www.finalcode.com.

Attribution

Use of this report and the respective data and graphics, in whole or in part, must be unaltered and must reference the sources as "© 2015 EMA- State of Secure File Collaboration Report, September 2015 Sponsored by FinalCode."

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3249.092515