

HIDDEN COSTS OF FILE TRANSFER: THE STATUS QUO IS SURPRISINGLY COSTLY

June 2016

→ **Derek E. Brink**, CISSP, Vice President and Research Fellow
Information Security and IT GRC



Report Highlights

p2

Files are the foundation for countless enterprise initiatives. It's no surprise that all organizations are moving files, using a wide variety of mechanisms.

p5

The productivity risk — i.e., the median cost of errors, problems, and exceptions in file movements — is just over \$50 for every file transferred using mechanisms that are mistakenly thought to be “free.”

p6

The security and compliance risk — i.e., the median cost of data breaches and audit deficiencies — is twice as high for every file transferred using “free” mechanisms, as opposed to with an MFT solution.

p7

Organizations using an enterprise-class MFT solution realize a median return of more than 500 times on their investment —i.e., an investment of about a nickel per transfer yields a reduction in risk of nearly \$30.

Every file sent “for free” — as an *email attachment*, using a consumer-oriented *file-sharing app*, with a low-level *FTP server*, or with *custom programs and scripts* — actually has an 80% chance of costing your organization money. Just how much “free” can actually cost may surprise you. Aberdeen Group’s analysis shows that organizations using an enterprise-class **managed file transfer (MFT)** solution significantly reduce the productivity risks from dealing with persistent errors, exceptions, and problems in transmission, as well as the security and compliance risks related to the movement of sensitive information.

2

Unstructured data — which may take the form of documents, presentations, spreadsheets, email and text messages, notes, images, audio, video, and so on (collectively, these are also referred to as files, or content) — supports countless enterprise initiatives for collaboration between individuals, integration of business processes and workflows, innovation in products and services, growth in revenue and earnings, and efficiency of operations.

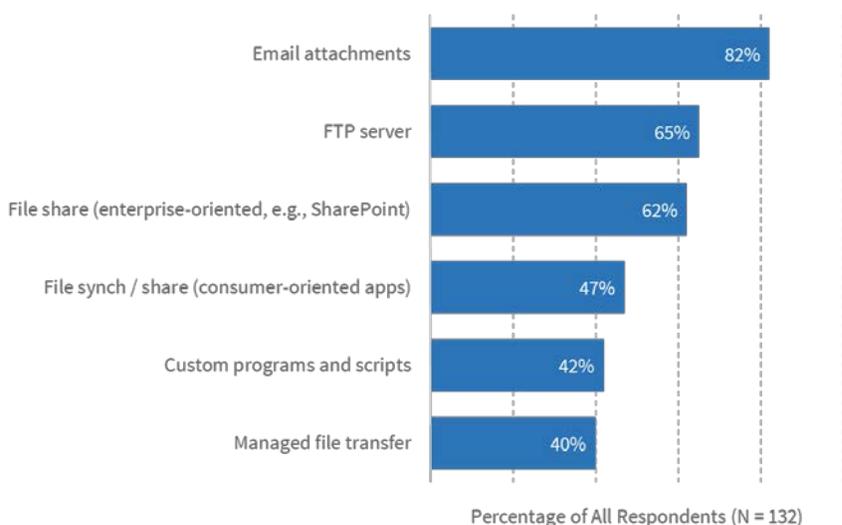
Business Context: Every Organization is Moving Files

Unstructured data — which we can also refer to as **files**, or **content** — plays a fundamental role in carrying out the mission of most modern organizations. Files are the foundation for countless enterprise initiatives, including:

- Collaboration between individuals
- Integration of business processes and workflows
- Innovation in products and services
- Growth in revenue and earnings
- Efficiency of operations

For this reason, it’s not really a surprise that literally every organization in Aberdeen’s benchmark research moves files, using a wide variety of file transfer mechanisms (Figure 1).

Figure 1: “Free” Solutions for Moving Files Are Clearly Popular — But Are They Really Free?



Source: Aberdeen Group, December 2015

3

If It’s Free, It’s for Me – But Many Costs of Moving Files Are Hidden

As seen in Figure 1, “free” solutions for moving files are clearly popular: *email attachments*; *FTP servers*; enterprise-oriented *file sharing* solutions (such as Microsoft SharePoint, which is bundled with the tools that so many organizations use to create content in the first place); consumer-oriented apps for *file sync*; and *custom programs and scripts* top the list. But are these solutions really free? What are the hidden costs of moving files?

In addition to **the cost of the file transfer mechanism(s)** themselves, the total cost of moving files also includes:

- **The cost of user productivity** (e.g., time and effort by both senders and receivers to deal with errors, exceptions, and problems with file transfers)
- **The cost of security** (e.g., data breaches – whether malicious, inadvertent, or well-intentioned – that compromise sensitive information)
- **The cost of non-compliance** (e.g., audit deficiencies or other compliance issues that need to be resolved)
- **The cost of responders** (e.g., IT staff, Help Desk personnel, administrative support, or other resources needed when something goes wrong)

To gain more insight into this important question, Aberdeen seized the opportunity to leverage findings from its benchmark studies and other industry sources to quantify these hidden costs of file transfer in a simple Monte Carlo model. As the basis for comparison, Aberdeen analyzed the following two groups:

- **MFT Non-Users** (N = 53) — This subset of survey respondents currently uses any combination of email

→ Related research: [No Content Left Behind: When to Extend File Sync / Share with Enterprise Content Management](#)

4

Most file transfers take place as planned, but a material few — a median of 5.6% for organizations relying on “free” solutions for moving files — are problematic. Perhaps the files are too large, or the network connections are unreliable, or the transmissions were inadvertently misdirected or delayed. For whatever reason, senders and receivers must spend time trying to figure out what happened, asking responders for help, and seek a workaround so they can stop thinking about transferring files and get back to their primary tasks.

attachments, FTP servers, file sync / file share, or custom programs and scripts, but does *not* use an enterprise-class **managed file transfer (MFT)** solution.

- **MFT Users** (N = 36) — This subset of survey respondents currently uses an enterprise-class managed file transfer solution. In addition, they may also use some combination of email attachments, FTP servers, file sync / file share, and custom programs and scripts. In other words, there were no “pure” MFT users in Aberdeen’s benchmark study. For this reason, readers should keep in mind that the MFT Users group also carries some of the same costs as the MFT Non-Users group, as it was not possible to make a clean separation. However, this also means that the cost advantages for MFT solutions (described below) are *even higher* than those shown by this analysis.

Productivity Risks: The Cost of Errors, Problems, and Exceptions

Unfortunately, moving files is not perfect— that is, some fraction of an organization’s total annual volume of file transfers is going to have some kind of error, problem, or exception. For the respondents in Aberdeen’s benchmark study, the MFT Non-Users had more than twice as many issues to deal with as the MFT Users: a median of **5.6%** of all file transfer volume for the former, as compared to **2.7%** for the latter.

Resolving these problems takes time. In Aberdeen’s simple analysis, problems with file movements were modeled as affecting three parties: the *sender*, the *receiver*, and a *responder*. The time to resolve such issues was the same for both groups, a median of **11.4 business hours**. For senders and receivers, Aberdeen modeled only a portion of this time as unproductive,

5

but included the entire hourly cost of one full-time equivalent responder.

These figures from survey data are in line with common experience — most file transfers take place as planned, but a few are problematic. Perhaps the files are too large, or the network connections are unreliable, or the transmissions were inadvertently misdirected or delayed. For whatever reason, senders and receivers are spending time trying to figure out what happened, asking responders for help, and trying to find and implement a workaround so they can stop thinking about transferring files and get back to their primary tasks.

A big benefit of using a Monte Carlo model is that it uses ranges and distributions for each variable in the analysis, as opposed to fixed, average values — and the results of its calculations are likewise expressed in ranges and distributions. This maps perfectly to the proper definition of **risk**, which includes both the *likelihood* of something occurring, and the magnitude of the *business impact* if it does in fact occur. Thus, we can say that there is an 80% likelihood that every file transferred with mechanisms that are thought to be “free” will actually cost your organization money. For the MFT Non-Users, the median cost of each file movement is **just over \$50 per transfer** — as compared to *just over \$21* for the MFT Users. Given the “long tail” nature of probabilities and risk, we can also say that there’s a 10% chance that the cost for MFT Non-Users could be greater than \$300.

Said another way, Aberdeen’s analysis shows that **the use of an enterprise-class managed file transfer solution reduces productivity risk by about 60%** (and arguably even higher, as discussed on page four). In addition, Aberdeen’s model does *not* include the cost of business that is lost, deferred, or eroded as a consequence of unreliable and inefficient movement of files. In that sense, it represents a conservative, understated assessment

The productivity risk — i.e., the median cost of errors, problems, and exceptions in file movements — is just over \$50 for every file transferred using mechanisms that are mistakenly thought to be “free.” The likelihood of every file transferred costing your organization money is about 80%.

6

The security and compliance risk — i.e., the median cost of data breaches and audit deficiencies — is twice as high for every file transferred using “free” mechanisms, as opposed to those moved with an enterprise-class managed file transfer solution.

of the actual risk of using the so-called “free” file transfer mechanisms.

Security and Compliance Risks: The Cost of Sensitive Data

Some files are more valuable than others and need to be protected — whether this decision is driven by the organization’s own policies or by the complex matrix of compliance requirements imposed by governments and industries. But in spite of these protections, security incidents and non-compliance issues still happen. Some are *malicious* (e.g., from external attackers or insider threats), but Aberdeen’s research consistently shows that the majority are actually either *inadvertent* (e.g., the result of simple human error) or *intentional* (e.g., not malicious, just users ignoring policies or controls in their efforts to carry out their jobs). For the respondents in Aberdeen’s benchmark study, the MFT Non-Users had more than twice as many security-related incidents to deal with as the MFT Users: a median of **6.2** incidents in the last 12 months for the former, as compared to a median of **3** incidents for the latter.

Once these incidents are detected, they take time to contain and remediate. The time to resolve security incidents was the same for both groups, a median of **16.2 business hours**. For simplicity, Aberdeen modeled the entire cost of one full-time equivalent responder— although for many security incidents, containment and remediation could easily involve several people.

In addition, Aberdeen’s analysis included estimates for the cost of a data breach based on its previous Monte Carlo models derived from the Verizon 2015 Data Breach Investigation Report ([DBIR](#)). For example, for a breach of between 10,000 and 100,000 records, the DBIR estimates a total business impact of about \$179,000, with a range of \$144,000 to \$223,000.

In Aberdeen’s study, the number of compliance issues was the same for both groups (a median of **5.1** issues in the last 12 months), as was the time to fully resolve them (a median of about **60 days**). In this case, Aberdeen modeled only a portion of the cost of one full-time equivalent responder, to account for the reality of waiting for changes in business processes and human behaviors over a period of several weeks.

In the dimension of security and compliance, the median cost of each file movement for MFT Non-Users is **about \$1.10 per transfer** — as compared to half that amount (*about 55 cents*) for the MFT Users. Said another way, Aberdeen’s analysis shows that the use of an enterprise-class managed file transfer solution reduces security and compliance risk by about 50% (and arguably even higher, as discussed on page four).

Putting It Together: The Hidden Costs and Risks of File Transfer

The hidden costs of file transfer are summarized in Table 1, which reflects the median cost per transfer estimated by Aberdeen’s Monte Carlo model. By inspection, we can see that organizations using an enterprise-class MFT solution:

- ➔ Reduce their median productivity risk by nearly 60%
- ➔ Reduce their median security and compliance risk by 50%
- ➔ Realize **a median return of more than 500 times on their investment in MFT** (i.e., an investment of about a nickel per transfer yields a reduction in risk of nearly \$30)

This last point is important: The reduction in hidden costs and risks from an investment in an enterprise-class managed file transfer solution are significant, but nothing comes for free — which is why the cost of the MFT solution itself is also incorporated into the analysis for the MFT Users group.

Organizations using an enterprise-class managed file transfer solution realize a median return of more than 500 times on their investment — i.e., an investment of about a nickel per transfer yields a reduction in risk of nearly \$30.

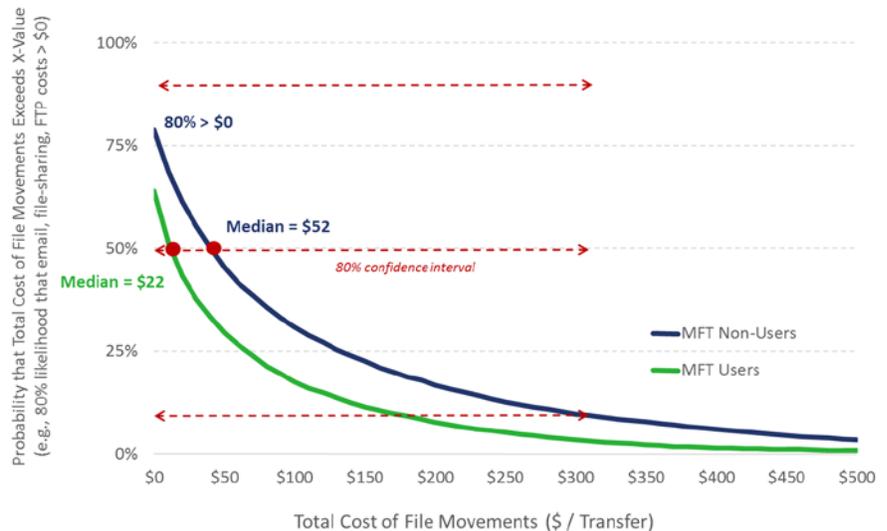
Table 1: An Investment in MFT Greatly Reduces Hidden Costs

Median \$ / Transfer	MFT Users	MFT Non-Users	Business Value of MFT	
Productivity Risk	\$21.55	\$50.50	\$28.95	57%
Security and Compliance Risk	\$0.55	\$1.10	\$0.55	50%
Cost of MFT Solution	\$0.05	-	(\$0.05)	> 500X return
Total Cost of Moving Files	\$22.15	\$51.60	\$29.45	57%

Source: Aberdeen Group, December 2015

Expressing the results of this analysis in terms of risk, as risk is properly defined, is a bit more complex than the simplicity of using the medians. But advising business decision-makers about risk is the security professional’s *raison d’être*, so it’s important to give it a try. In Figure 2, the risks of moving files discussed above are described as a curve, with likelihood on the y-axis.

Figure 2: Use of Enterprise-Class MFT Reduces the Risks of Moving Files by Nearly 60%, Compared to “Free” Alternatives



9

Source: Aberdeen Group, December 2015

For example, from Figure 2, we can now more easily visualize the following statements about the risk of “free” file transfer mechanisms, most of which have already been made:

- ➔ There’s an 80% likelihood that “free” mechanisms will actually cost more than \$0 (said another way, there’s really only a 20% probability that “free” is really free).
- ➔ The median total cost per transfer is about \$52 — meaning that out of thousands of independent scenarios, 50% of the time it will be higher than this figure, and 50% of the time it will be lower.
- ➔ There’s a 10% likelihood that “free” mechanisms will actually cost more than \$300 per transfer – e.g., a scenario in which there is a significant breach of sensitive data, with substantial time for containment and remediation.
- ➔ We could also turn the problem around: suppose that management’s appetite for risk for file movements is less than \$20 per transfer — from Figure 2, the likelihood of this result is about one in three.

The most important point is that we now have much better insight into the costs and risks of file transfer mechanisms that are mistakenly thought to be “free.” In addition, we have the means to describe how an investment in an enterprise-class managed file transfer solution will quantifiably reduce that risk, in language and non-technical terms that business decision-makers — the people who actually own the risk — already understand.

10

Customer Case-in-Point for Enterprise Managed File Transfer: North Carolina State Employees’ Credit Union

From its humble beginnings in 1937 — just 17 members, and \$437 in deposits — the **North Carolina State Employees’ Credit Union (NCSECU)** today serves more than 2 million state and public school employees and their families throughout all 100 counties of North Carolina, with more than 250 local branches, 1,100 ATMs, and 15 million online transactions per month. As a not-for-profit cooperative, NCSECU places a heavy focus on safe investments, low expenses, and high value for its member-owners.

Robert Skinner, an Information Systems (IS) Manager at NCSECU, described the still-expanding role of an enterprise-class managed file transfer (MFT) solution in this business context:

- ➔ **For IT infrastructure.** The initial use case for MFT was to move data internally, from one server to another. “In this case, MFT was implemented for best practice,” said Skinner. “For data managed by different groups, the MFT solution provides us with a necessary audit trail.”
- ➔ **For NCSECU employees.** One example of an expanded use case for MFT is the movement of personally identifiable information (PII), such as payroll files, between NCSECU and its third-party partners. “Our previous methods — email attachments — were not automated, and required a lot of human involvement,” Skinner explained. “MFT provides us not only with cost-saving automation and an audit trail, but also with end-to-end data security, which helps to maintain compliance with regulatory requirements for protecting this type of sensitive information.”

11

→ **For NCSECU customers and partners.** One of the most recent use cases for MFT is automating and streamlining the mortgage closing process, by electronically transferring closing documents between NCSECU and the various parties involved (e.g., buyers, sellers, attorneys and closing agents, title companies, real estate agents). “Previously, we relied on overnight delivery services to move the required documents. With MFT, we’ve significantly reduced our monthly costs,” said Skinner. “In addition, we’ve significantly reduced the cycle time for these steps — what used to take an overnight delivery each way, with at least one day in between for processing, is commonly taken care of on the same day.”

Based on their positive experience using the Ipswitch *WS_FTP* product, NCSECU evaluated and selected Ipswitch *MOVEit DMZ* and *MOVEit Central* (now known as *MOVEit Transfer* and *MOVEit Automation*, respectively) as their standard managed file transfer platform, citing capabilities such as a familiar user experience, a task-based approach, and a highly customizable solution that is easily tailored for their diverse and ever-changing requirements. “File transfer has become an under-the-covers, transparent NCSECU capability,” said Skinner. “It was never easy before, but now it’s easy. MFT is not viewed as just a taxi service for our data — it’s viewed as a vital part of our IT infrastructure.”

Case-in-Point: Lessons Learned

Asked about lessons learned or words of wisdom for others who may be currently investigating MFT solutions, the IS Manager at the North Carolina State Employees’ Credit Union noted that users have business problems that need to be solved, and IT needs to provide them with a supported solution that goes beyond the commonly used free or do-it-yourself alternatives.

“We didn’t anticipate that our use of MFT would grow as big as it did, as quickly as it did,” he said. “In hindsight, the one thing we might have done differently is to invest more up-front on back-end resources, and to design the platform for faster growth.”

12

Summary and Key Takeaways

- **Files** (unstructured data) are the foundation for countless enterprise initiatives. It’s no surprise that all organizations are moving files, using a wide variety of mechanisms.
- “Free” solutions for moving files are the most widely deployed: *email attachments*, *FTP servers*, enterprise-oriented *file sharing solutions*, *consumer-oriented apps* for file sync, and *custom programs and scripts*. But are these solutions really free?
- In addition to the **cost of the file transfer mechanism(s)** themselves, the total cost of moving files also includes the **cost of user productivity**, the **cost of security**, the **cost of non-compliance**, and the **cost of responders**.
- To gain more insight into this important question, Aberdeen leveraged findings from its benchmark studies and other industry sources to quantify these hidden costs of file transfer in a simple Monte Carlo model. As the basis for comparison, Aberdeen analyzed two groups: **MFT Users** (N = 36), and **MFT Non-Users** (N = 53).
- For the respondents in Aberdeen’s benchmark study, the MFT Non-Users had more than twice as many **errors, problems, and exceptions** to deal with as the MFT Users: a median of **5.6%** of all file transfer volume for the former, as compared to **2.7%** for the latter. The time to resolve such issues was the same for both groups, a median of **11.4 business hours**.
- The **productivity risk** — i.e., the median cost of errors, problems, and exceptions in file movements — works out

13

to be **just over \$50** for every file transferred using mechanisms that are mistakenly thought to be “free.”

- For the respondents in Aberdeen’s benchmark study, the MFT Non-Users had more than twice as many **security-related incidents** to deal with as the MFT Users: a median of **6.2** incidents in the last 12 months for the former, as compared to a median of **3** incidents for the latter. The time to resolve security incidents was the same for both groups – a median of **16.2 business hours**.
- In Aberdeen’s study, the number of compliance issues was the same for both groups (a median of **5.1** issues in the last 12 months), as was the time to fully resolve them (a median of about **60 days**).
- In the combined dimension of security and compliance, the median cost of each file movement for MFT Non-Users is **about \$1.10 per transfer** — as compared to half that amount (*about 55 cents*) for the MFT Users.
- Organizations using an **enterprise-class managed file transfer solution** conservatively **reduce the total risk of file transfers by about 60%**. In addition, they realize a median **return of more than 500 times on their investment** in MFT — i.e., an investment of about a nickel per transfer yields a reduction in risk of nearly \$30.
- This type of analysis provides valuable insights into the costs and risks of file transfer mechanisms that are mistakenly thought to be “free.” In addition, it provides the means to describe how an investment in an enterprise-class managed file transfer solution will quantifiably reduce that risk, in language and non-technical terms that business decision-makers — the people who actually own the risk — already understand.

For more information on this or other research topics, please visit www.aberdeen.com.

Related Research

[*Quantifying the Risk of DDoS Attacks for Network Service Providers*](#); December 2015

[*No Content Left Behind: When to Extend File Sync / Share with Enterprise Content Management*](#);
November 2015

[*How Managing Privileged Access Reduces the Risk of a Data Breach*](#); September 2015

[*Flash Forward: Putting Managed File Transfer in Perspective*](#); February 2015

[*The Last Mile in IT Security: Changing User Behaviors*](#); November 2014

Author: Derek E. Brink, CISSP, Vice President and Research Fellow, Information Security and IT GRC
(Derek.Brink@aberdeen.com)

About Aberdeen Group

Since 1988, Aberdeen Group has published research that helps businesses worldwide to improve their performance. Our analysts derive fact-based, vendor-neutral insights from a proprietary analytical framework, which identifies Best-in-Class organizations from primary research conducted with industry practitioners. The resulting research content is used by hundreds of thousands of business professionals to drive smarter decision-making and improve business strategies. Aberdeen Group is headquartered in Waltham, Massachusetts, USA.

This document is the result of primary research performed by Aberdeen Group and represents the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen Group and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Aberdeen Group.