BEST PRACTICES IN CONTROLLING AND TRACKING FINANCIAL INFORMATION ELECTRONICALLY

A report prepared by CFO Research,
commissioned by RR Donnelley

CFO research

RR DONNELLEY
VENUE

Contents

About this Report

In the spring of 2014, CFO Research conducted a survey exploring U.S. finance executives' understanding of the use and misuse of electronic financial information at their companies, and how they can help their businesses improve policies and procedures to better protect the electronic flow of financial information. We were particularly interested in "best practices" in information security, especially with respect to collaboration mechanisms.

We gathered a total of 153 responses from senior finance executives at U.S. companies with annual revenues of $100 million or more, representing a range of industries.

Title

Chief financial officer	35%
Controller	19%
VP of finance	11%
Director of finance	9%
EVP or SVP of finance	5%
CEO, president, or managing director	5%
Treasurer	5%
Other finance title	4%
Other	7%

Revenue

$100 million – $250 million	22%
$250 million – $500 million	18%
$500 million – $1 billion	16%
$1 billion – $2 billion	12%
$2 billion – $5 billion	12%
More than $5 billion	20%

Industry

Auto/Industrial/Manufacturing	18%
Financial services/Real estate/Insurance	14%
Wholesale/Retail trade	12%
Public sector/Nonprofit	9%
Health care	9%
Chemicals/Energy/Utilities	7%
Food/Beverages/Consumer packaged goods	6%
Business/Professional services	6%
Construction	5%
Transportation/Warehousing	4%
Telecommunications	3%
Media/Entertainment/Travel/Leisure	3%
Hardware/Software/Networking	2%
Aerospace/Defense	1%
Pharmaceuticals/Biotechnology/ Life sciences	1%

Note: Percentages may not total 100%, due to rounding.

Do You Know Where Your Financial Information Is?

Are your employees—or for that matter, your CFO—thinking as much as they need to about the use and misuse of their company's financial information in the Digital Age? That was the underlying theme of a survey conducted by CFO Research and sponsored by RR Donnelley. Gathering 153 responses from finance executives working at large U.S. companies, we looked into how aware finance executives are of the risks their employees are taking with the company's electronic financial data, and we examined "best practices" for finance executives in data governance and technology use.

The fact is, the security of a company's financial information is no longer just the concern of the IT function, or even of the CFO. In an electronic world in which practically every employee has the technology to access and share information electronically, security becomes everybody's business.

With an increasingly mobile workforce, employees expect to be able to share information whenever and wherever they need to, and computers—large and small—offer that. Most employers issue office-based workers desktops or laptops for business-related use. Field workers nowadays often are provided with mobile phones, tablets, or phablets, any of which may connect to the internet or to company networks. On the consumer side, mobile phones are commonplace; over 90% of American adults have one, and over half of those phones are smartphones, meaning that most of us, everywhere we go, carry around a tiny computer in our pocket. And whether or not the mobile device we carry was issued by our employer, at some point and to some degree, some form of work is being accessed or conducted electronically with that device.

Even if a hard copy is printed and distributed eventually, documents are almost invariably created on a computing device, which means that they are likely also stored electronically and potentially distributed via email. Information is created, stored, and shared electronically every single day in companies all over the world.

Yet many employees, including CFOs, aren't especially concerned about the ramifications of the use and misuse of all this electronic information. Employees—and the employers governing their work—can be so focused on the end result, whether it's meeting goals or increasing revenues, that productivity takes precedence over information security. All too often, employees and management alike resort to workarounds or other unauthorized practices simply to do their jobs. In fact, writing in our survey, one chief executive turns a glaring spotlight on the problem: "Better leadership in finance and IT [is needed]. These departments are supposed to serve the business. We use workarounds like Dropbox, Google drives, pen drives, and so on because IT too often simply doesn't work right."

As this executive officer notes, both tone and direction need to come from the top, if employees are to be expected to take information security seriously. Only 15% of the finance executives in our survey think that their companies' policies for controlling financial information are very well understood throughout the company, and 41% of the respondents characterize employee understanding of policies as less than adequate. As the steward of a company's most sensitive financial information, the CFO needs to remain aware of the risk of *misuse* of that information, as well as the potential for its use.

Today's CFO needs to remain aware of the *misuse* of sensitive financial information, as well as the potential for its use.

More Information Leads to More Risk

The growth in electronic transmission and storage of data may be exposing companies to more vulnerability than they recognize. The survey revealed that nearly all executives—92%—say that the electronic flow of financial information has increased over the past three years. However, only half (50%) believe that the risk of a data breach for financial information is any higher than it was before. (See Figure 1.) This finding is reflected in the view of a CFO from the transportation and warehousing industry in the survey, who writes, "[I] don't think the risk has changed that much over the last few years."

Despite the fact that publicly disclosed data breaches and website or software vulnerabilities are splattered across the headlines regularly today, finance executives appear to be more complacent about security risks than is warranted. A little more than half of the respondents (53%) say that their company's vulnerability to a data breach is no more nor less than that of its peers, perhaps indicating either a lower priority placed on information security or a staunch refusal to acknowledge the realities of information security risks.

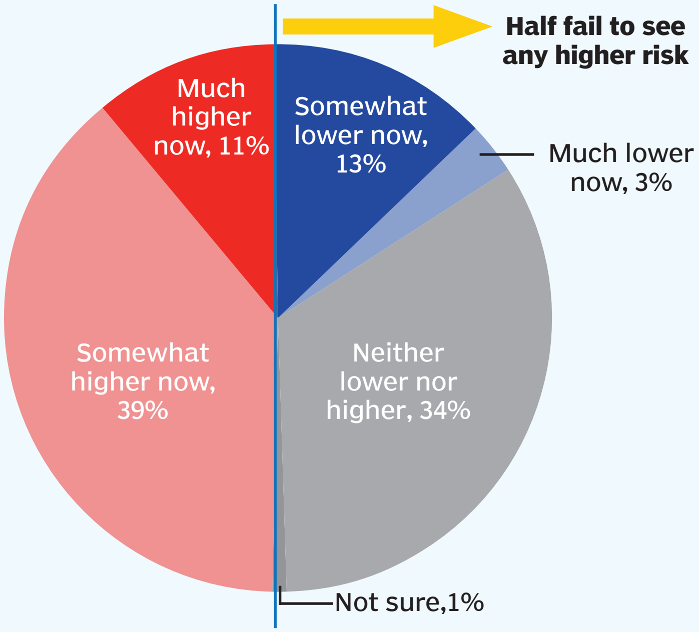
The lack of recognition of the threat may help explain the spotty record in oversight that our survey reveals; many companies could do a much better job of instituting policies around the use and handling of electronic data. When asked about company policies for controlling the electronic exchange of financial information, only one-third (33%) of respondents say they have developed a formal, enterprise-wide plan, indicating that they consider the issue serious enough to put concerted effort behind it. The remainder say they either have no plan at all or only a general directive in place. A quarter of respondents report that their companies have not developed or communicated any policies for controlling financial information electronically. Business executives at these companies should indeed be wondering about the whereabouts and uses of company-owned information.

Lack of a formal policy, combined with the belief that the potential for data breach is no more nor less than it was three years ago (despite the

Only one-third of respondents say they have a formal, enterprise-wide plan for controlling the electronic exchange of financial information.

FIGURE 1. Risky Business: Only half of the finance executives surveyed recognize a threat from the rising tide of electronic information.

Compared to three years ago, how much higher or lower would you say the risk is of a data breach for financial information at your company?



increase in the flow of electronic information), may be an indication that companies are not taking the issue of information security seriously enough. For example, among the respondents without a formal policy for data security, two-thirds (66%) say they are no more nor less vulnerable than their peers, suggesting that the majority of companies without an electronic use policy fail to correlate the lack of a policy with greater risk.

In contrast, among the "best practice" companies—those with formal policies in place—45% of finance executives believe that they are less vulnerable than their peers. (See Table 1.) This could be a result of the efforts undertaken by "best practice" companies to not only develop a formal, written policy, but also to communicate that policy throughout the company and put an information security program in place that regularly assesses risks and vulnerabilities.

So, for example, seven out of ten (69%) respondents from "best practice" companies use a risk model to evaluate security risks for financial data. While risk modeling, in general, is known to aid in risk identification, only 45% have adopted the practice at companies that have issued a general directive about information security, but lack a detailed plan. And the number plummets to 15% at companies where no specific policies for controlling electronic data have been developed. Given that finance executives typically are seen as risk-averse, it's curious as to why they haven't taken up all the tools available for managing some of the most sensitive data a company holds—financial data.

Just having a plan in place, however, is not an end in itself. A treasurer from a financial services company writes in the survey, "We have a fairly robust set of controls in place. The one thing we need to do more of is training and updating employees so that we can be more confident that the rules are being followed." In fact, 80% of survey respondents say that their companies need to improve their communication of security policies, with 28% saying that they need to make substantial improvements.

For a CFO, fostering a security-conscious culture can start with putting information security on the agenda. According to our survey, finance executives at companies with a formal electronic use policy are the most likely to meet with an information security executive to discuss security issues for financial data, with half of them (49%) reporting that they meet regularly. This number drops to only 25% at the other companies. A plurality (43%) of the respondents from companies without any plan whatsoever admit that their top finance executive rarely or never formally discusses data security with someone else.

While more and more information is flowing electronically, and new technologies—some developed specifically for business use, and others adopted for business use in spite of the fact that they aren't developed with security in mind—are brought to market every day, executives interested in keeping their business's information private should put more effort behind understanding risks and the habits and technologies that contribute to them.

Given that finance executives typically are seen as risk-averse, it's curious as to why they haven't taken up all the tools available for managing some of the most sensitive data a company holds—financial data.

TABLE 1. Armor Up: A formal information security plan can help companies feel less vulnerable.

	We are LESS VULNERABLE THAN OTHERS to breaches of financial information
My company has a **formal, enterprise-wide plan** in place for controlling financial information electronically.	45%
Company management has issued a **general directive** regarding the control of financial information electronically.	40%
My company **has not developed or communicated specific policies** for controlling financial information electronically.	17%

Habits Established by Personal Use of Communication Technologies Creep into the Workplace

Mobile technologies are one such risk. Mobile technologies offer myriad user- and business-focused benefits but also raise information security concerns. The four major operating systems (iOS, Android, Windows Phone, Blackberry) ship to consumers with varying levels of security built in, and none of them with security standards at the level of desktops or even laptops. Each new version of a smartphone, too, will have different security features. On top of that, carriers have varying levels of security around data transmission.

Most consumers—who are also employees—have their own personal phone, one not issued by their employer. This means that the company has very little governance over what goes on with that phone. Which apps have been added? Did the user change technical controls or security settings that affect what can be installed or downloaded? How much sharing does the user/owner allow on social media sites which he or she regularly accesses from the mobile device? The organization can certainly put some technical controls in place to limit access to specific company systems, data, and information, but there are always workarounds, and if they're there, employees will find and use them.

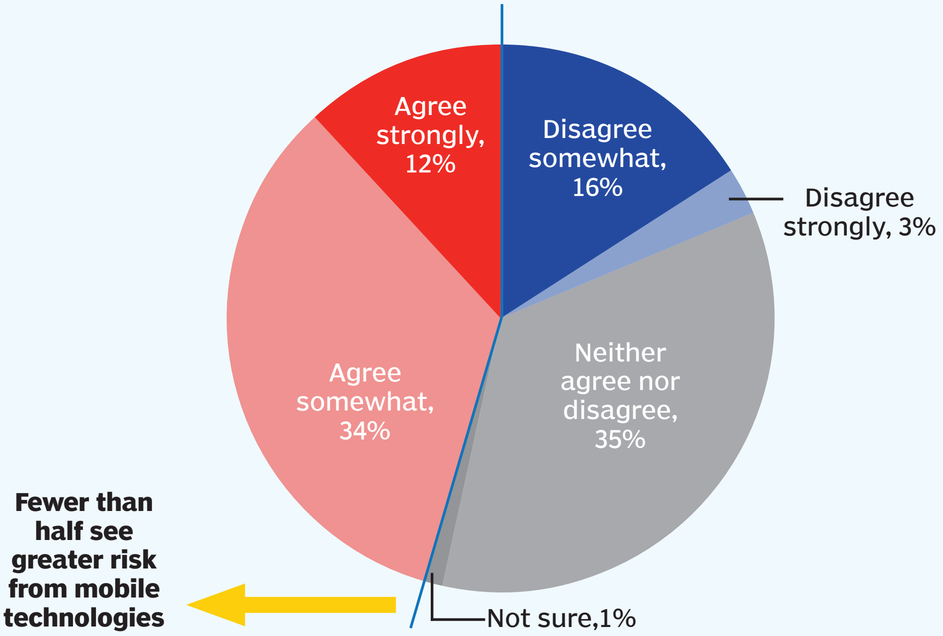
Finance executives are aware of this conundrum, yet only 46% of finance executives agree that the use of mobile technologies has weakened the company's control around financial information. (See Figure 2.) Security-conscious finance executives would do well to evaluate technologies that can improve mobile data security, such as encryption, endpoint protection, access controls, and containerization.

Email provides another example of a frequently overlooked security risk. Almost all (94%) of the survey respondents believe that their companies' employees use email to access and exchange

There are always workarounds, and if they're there, employees will find and use them.

FIGURE 2. Where You Go, I Go: Finance executives recognize the growing use of mobile technologies in the workplace, but many overlook the increased risk to information security.

The growing use of mobile technologies at my company has weakened the controls we have in place for financial information.



financial information electronically. Email alone is an insecure method of sharing information, to begin with. Emails are often accessed and sent via personally-owned devices, and when employees can access company-owned data, then send that information via email from their phones, the risks become immense.

Yet, finance executives do not appear to have thoroughly considered the problem (even when emails are sent from company laptops and desktops), as evidenced by the overwhelming use of email containing financial information. In response to an open-text question on the subject, one respondent writes, “Files sent via email are secure.” Buyer beware. The use of encryption can certainly strengthen email security, but encryption can be cracked, and email in and of itself is not a secure method of transmission.

Interestingly, companies with a formal policy for the use of electronic information are just as likely to use email for accessing and exchanging financial information as companies with a general directive or no policy in place. Because email is such a common business communication tool, finance executives may not have fully considered the possible misuse or inappropriate/unauthorized access that can easily occur.

Finance Executives Must Be Able to Make Informed Tradeoffs Among Risk, Convenience, and Cost

That’s not to say that all data is created equal; for many daily business activities, less secure methods for storing, transmitting, or sharing information—even email—are perfectly reasonable. Understanding the different levels of risk inherent in different kinds of activities, and the different consequences of a data breach, is key to adapting the proper tools and controls for each situation.

Finance executives say their companies have made use of various types of file storage and collaboration technologies for different purposes. While specifics vary from company to company, the types of tools in use fall into a few main categories: shared internal drives/intranets, shared external drives/extranets, private clouds, and public clouds. Shared internal drives and private clouds are provided through infrastructure—hardware, storage, and networks—that is dedicated to a single client or company, and that can only be accessed by that client. In contrast, shared external drives and public clouds provide infrastructure that is used by more than one company or client.

When it comes to sensitive information, it appears that companies prefer the perceived security and control of internal electronic storage and collaboration tools. Three-quarters (75%) of the survey respondents say their companies have used a shared internal drive or private cloud regularly or occasionally, for both sensitive financial and other business purposes. But nearly half (46%) of the respondents say their companies have never used an external shared drive or public cloud at all, for either financial or other business purposes. (See Figure 3, next page.) (A very few respondents write that they only use “controlled paper distribution” as a means for accessing and exchanging financial information.)

General cloud- or server-based capabilities are best suited for serving ongoing needs, or in instances when sharing or storing electronic documents may not pose a high risk to the organization and the conveniences of cloud are the biggest boon to the business. For business activities requiring collaboration among a company’s employees, internal drives and private clouds are relatively inexpensive and manageable.

However, these general-use capabilities are not the most effective tools for sharing electronic information outside of the company, which is required for activities such as debt financing and M&A. Rights management and security become issues when access to internal resources is provided to external parties. For these kinds of activities, a company may set up single-use data rooms—either physical or electronic spaces where information relevant to the intended use is collected, stored, viewed, and controlled.

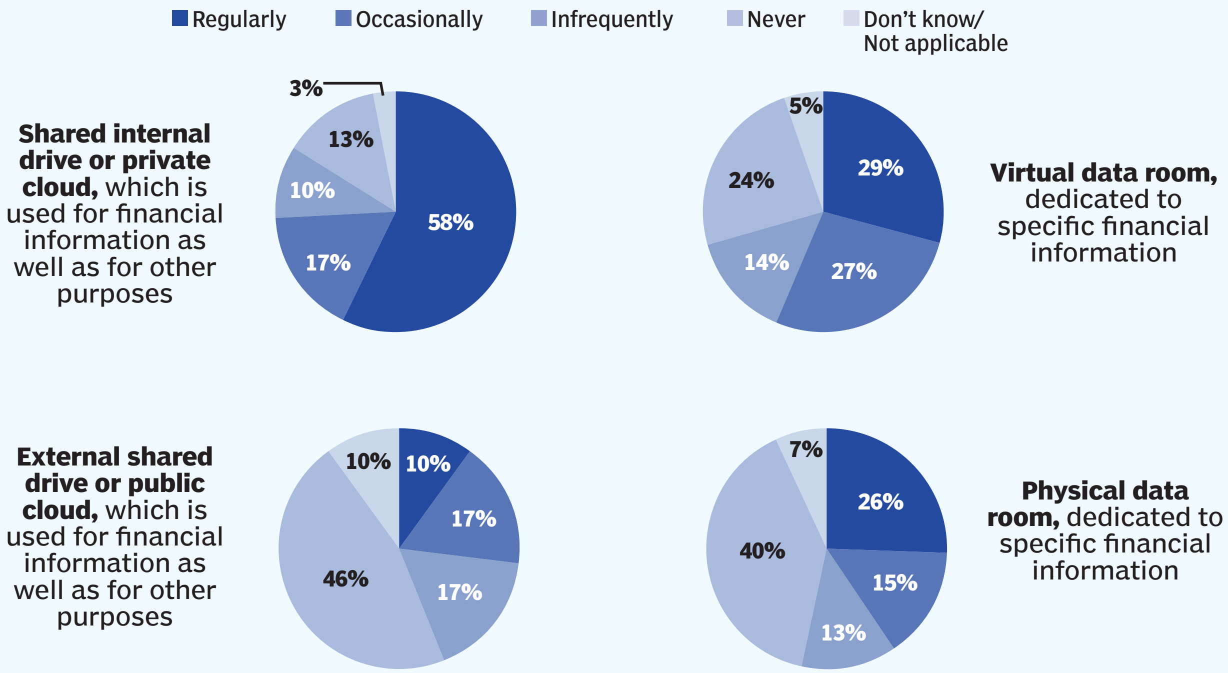
Finance executives typically use data rooms, virtual or physical, for specific purposes—mainly financial reporting and M&A activity—which

Almost all (94%) of the survey respondents believe that their companies’ employees use email to access and exchange financial information electronically.

FIGURE 3. Keeping It In-House: To store and share financial files, companies favor internal and electronic solutions over external or physical ones.

Within the past three years, how frequently has your company employed any of the following means to house and share sensitive financial information?

We use the following for sensitive financial information...



require delimited time periods and more rigorous controls. Data rooms essentially are point solutions that offer greater security, control, and tracking capabilities necessary for highly sensitive information.

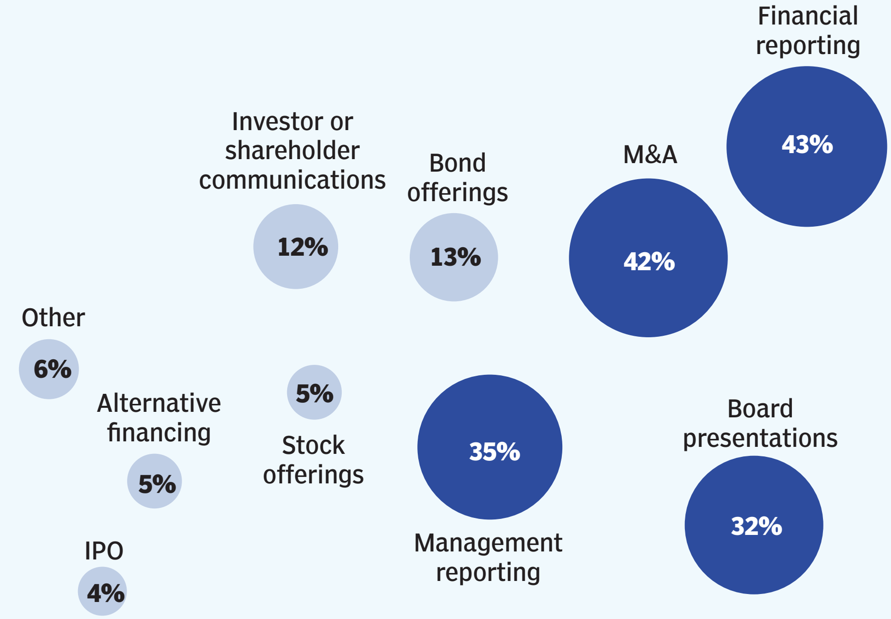
Virtual data rooms (VDRs) are a relatively new technology, as far as document storage and sharing goes, but our survey shows that they have become the point solution of choice in recent years. Companies have been sharing sensitive information with business partners, potential investors, and other third parties since the dawn of corporate society (or the creation of the legal profession, at least). The Great Merger Movement occurred between the years 1895-1905, but at that time, paper documents were passed between parties, one at a time, behind closed doors. As corporations became more complex and as companies wanted to expand the pool of potential bidders, physical data rooms were created to allow interested third parties controlled and monitored access to company-confidential documents related to an impending merger or sale.

With the internet age, a more affordable, less time-consuming, and less paper-intensive way to store and share documents relevant to the due diligence process became available. VDRs have seen an uptick in use in recent years, and appear to have grown more attractive to finance executives than physical data rooms. As seen in Figure 3, 40% of respondents report never having used a physical data room within the past three years, but only 24% say the same for VDRs. In fact, 56% of respondents say their companies have used VDRs either regularly or occasionally for storing and sharing financial information over the last three years, with another 14% saying they have used a virtual data room at least once.

The highest percentages of respondents say they use data rooms primarily for financial reporting (43%) and M&A activity (42%). But a substantial number of respondents say that their companies have internal uses for data rooms,

FIGURE 4. Room to Grow: Finance executives report using data rooms to store and share documents for a range of activities, not just what's "expected."

For which activities does your company typically use either a physical or a virtual data room?



Finance executives recognize the value of VDRs over cloud-based services for handling highly sensitive data.

as well; management reporting (35%) and board presentations (32%) seem to be other cases for which finance executives see a need for the benefits of data rooms. (See Figure 4.).

The main benefits of VDRs versus cloud-based services, according to respondents, are better control over the information stored there (52%), increased security (50%), better usage tracking capabilities (information rights management) (47%), and greater ability to customize to end-user needs (35%). (See Figure 5, next page.) These characteristics are valued more in situations involving highly sensitive financial data, rather than "everyday" uses, and justify the higher cost required to establish and maintain a VDR.

Where cloud seems to have the edge over VDRs, respondents cite lower cost (45%), higher capacity (31%), ease of use (28%), and access across geographies (26%)—the types of benefits that carry more weight when conducting routine business. (See Figure 6, next page.)

With so many data breaches in the news recently, companies might also evaluate other situations—such as the development of new product lines, patents or formulas, or growth plans—where a VDR might be more beneficial than less secure and less easily controlled or monitored environments. Intellectual property, like patents or formulas, is becoming more and more desirable to corporate poachers, for example. Wise executives will evaluate the internal risks (misuse by employees or privileged users) and external risks (theft by hackers/attackers, unauthorized use by potential competitors). With a better understanding of the range of risks in hand, companies can then design protections around the most sensitive company data to prevent, to the highest degree possible, misuse.

FIGURE 5. Good, Better, Best: Finance executives recognize differences in high-value benefits between VDRs and cloud-based collaboration services.

Do either VDRs (dedicated virtual data rooms) or cloud-based collaboration services (such as Dropbox.com or Google Drive) provide clear advantages for sharing and storing financial information?

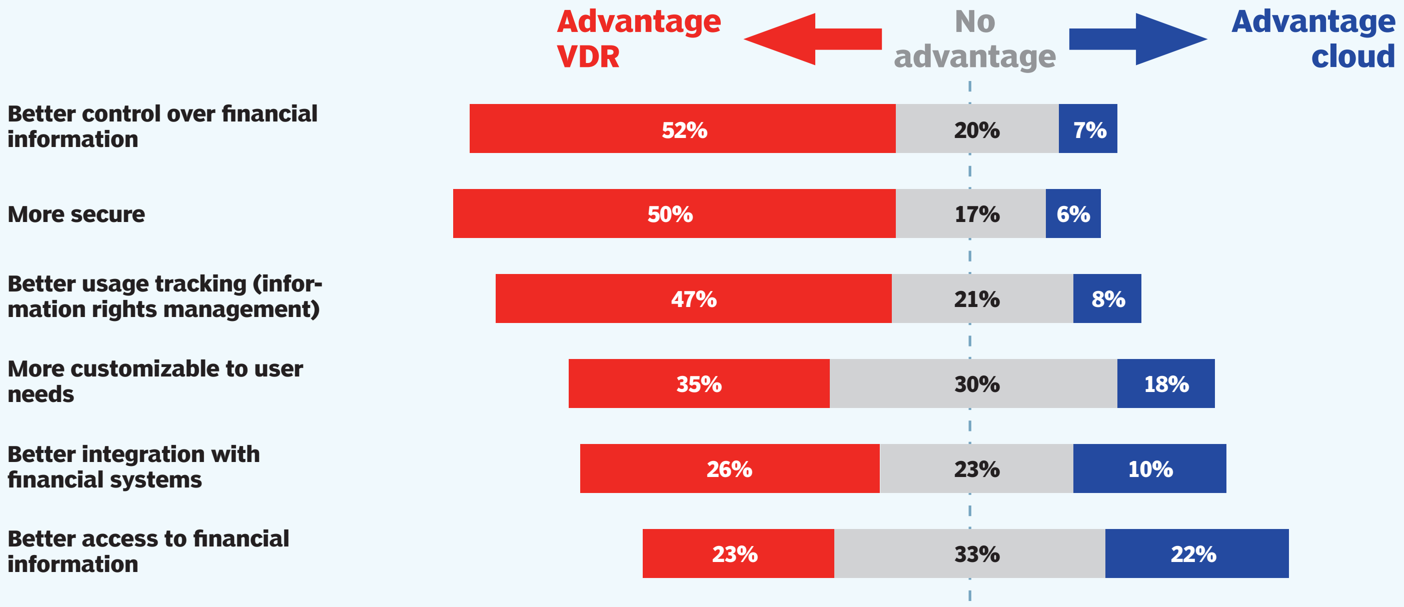
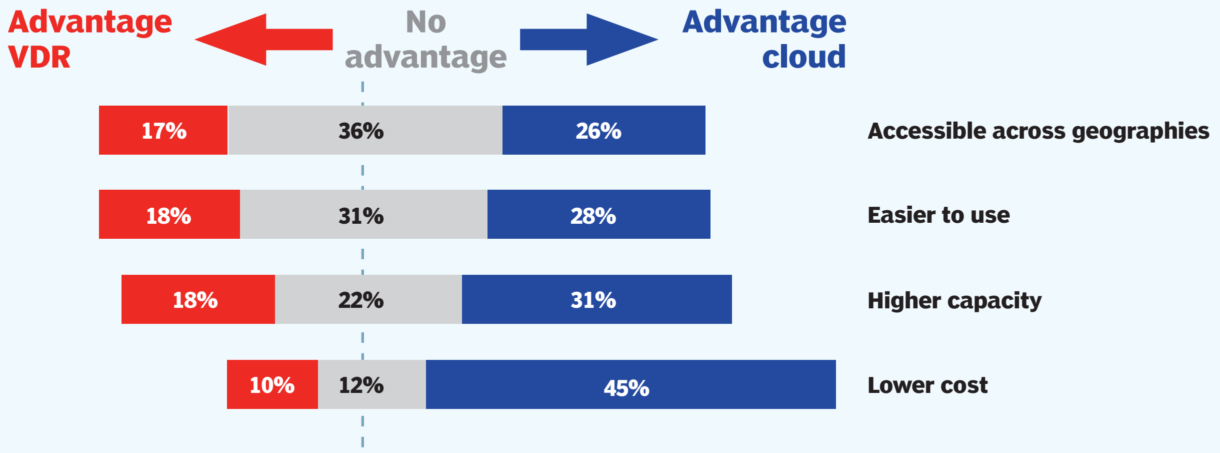


FIGURE 6. Match Game: The perceived benefits of cloud-based collaboration services are typically more suited for transactional or routine types of activities.

Do either VDRs (dedicated virtual data rooms) or cloud-based collaboration services (such as Dropbox.com or Google Drive) provide clear advantages for sharing and storing financial information?



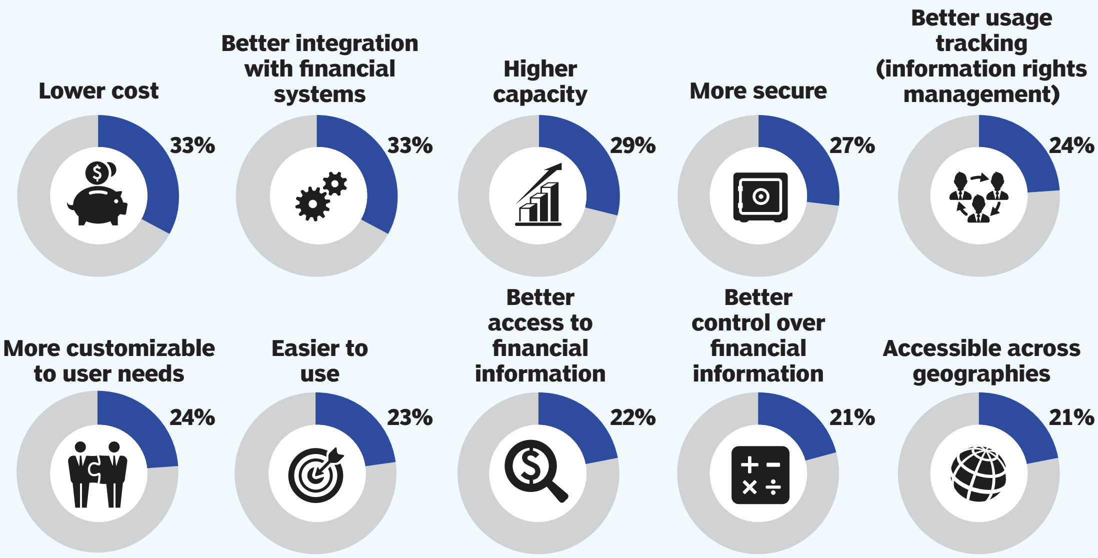
In Managing Information Risk, What You Don’t Know Can’t Help You

Despite some of the clear, business-benefitting features of VDRs, unusually large proportions of respondents don’t know enough about them to be able to judge their advantages or disadvantages. A full one-third of respondents don’t have enough information on the costs of VDRs versus cloud-based services, for instance, to make a determination in favor of one over the other. In each of the other categories listed, respondents answer “I’m not sure” between 21% and 33% of the time, which is a remarkably high number of finance executives to be in the dark. (See Figure 7.)

With companies’ growing reliance on technology to manage their information workflow, finance executives today need to develop at least a high-level understanding of the benefits their company’s investments provide; at the bare minimum, they should have a grasp on the cost differences. A strong case can be made that finance executives would do well to learn more about both the advantages and the appropriate uses of the options for information management they have available, in order to base their companies’ technology use on an informed understanding of the tradeoffs required among risk, cost, and convenience.

FIGURE 7. In the Dark: The survey reveals that large numbers of finance executives simply don’t know enough about the options to make effective decisions on use of collaboration technologies.

Percentage of respondents who answered “not sure” when asked whether VDRs or cloud-based collaboration services provide a clear advantage



Conclusion: Controlled, Secure Access to Sensitive Data Is Everyone's Business

The amount of electronic information companies create, store, and use for internal and external collaboration is increasing at a rapid pace. While finance executives are aware of this trend, they are not necessarily aware of all the ways to best protect and maintain control over their most sensitive information.

While some might argue that it is the job of the information security professional to secure electronic data, the reality is that information security is the entire company's responsibility. As such, senior executives must stay on top of the best tools that employees can use for storing and sharing company information, and the best practices for ensuring their proper use. They must ensure that their companies can adequately answer the key questions relating to data security:

- Are adequate controls in place? Do all employees understand them and follow them?
- Who can access financial data? How can they access it? Where do they access it from?
- Where is financial data being stored, and in how many places? How is it being transmitted? How secure are the transmission modes?
- Who needs to use financial data, and for what purposes? How widely is financial data being shared, and with whom?
- What kinds of technologies are being used to share data? What capabilities do end users have for storing, printing, and transmitting financial data?

Information technology, in general, is improving and evolving all the time, and organizations should be regularly investigating features, benefits, capabilities, and return on investment to keep up to speed. But they also need to be able to accurately gauge the financial risk and cost of a data breach should particular types of information be lost inadvertently or stolen intentionally.

Companies need to make information security part of the working culture.

Companies need to make information security part of the working culture, creating formal policies that specify acceptable use of electronic information and the ramifications of misuse, and providing company-wide training on the policy to ensure that it is very well understood. As summarized nicely by one respondent when asked about the most important actions a company can take to improve the security of its financial information, "[We have to provide] better communication and education of the need to secure financial information, and who might want to inappropriately gain access to the information, and how they might gain access in a manner that the employees would not suspect."

When it comes to sharing and collaborating externally, especially in the case of M&A activity, financial statements, or proprietary company intelligence, it becomes even more imperative to monitor who is accessing what and when. In such situations, a data breach can most definitely impact the bottom line, and therefore it is incumbent upon the chief finance executive to ensure that the proper access controls and technologies are in place.

Awareness of appropriate uses of sensitive information is just as important as the systems used to store and control it, and the processes start at the top. Finance executives, assisted by IT and security teams, can lead the charge by learning more about best practices in controlling and tracking electronic information.

Sponsor's Perspective

Document management solutions are becoming increasingly popular, but as the Heartbleed security bug not so gently reminded us last quarter, convenience can come at a trade-off to information security. While the bug hit some well-known document management and cloud storage providers, threatening the security of their users' sensitive information, RR Donnelley's Venue® virtual data room remained completely unaffected.

To the chagrin of IT managers everywhere, many employees are using the same file sync-and-share platforms at home and work. Consumer file synchronization and sharing tools are cause for serious concerns around data breaches and loss of control over sensitive business documents. The prevalence of mobile computing and the BYOD trend only compound these security risks.

RR Donnelley understands the need for secure document management platforms at the business level, which is why our Venue virtual data platform offers unparalleled security and is the data room of choice for the deal-making community. The platform's built-in security includes dynamic watermarking, instant reports of exactly who's accessing which files, encryption of all data communication, code access security and communication protocols like SSL, protective software to inhibit print screen operations, and the ability to revoke rights to a document even after it has been downloaded to the user's desktop.

As a $10.5 billion corporation, serving 98% of the Fortune 500, RR Donnelley manages billions of documents and other digital assets for clients around the world. With a deep background in financial services and deal management, we know what it takes to protect highly-confidential information. Our Venue data rooms provide industry-leading AT101/SOC2 Type II compliance under three AICPA Trust Principles: Data Security, Data Confidentiality and Data Availability. Other vendors and consumer heritage platforms may audit only their data center and only against the data security trust principle, or in the case of an SSAE16, against no trust principles.

With Venue, security is our number one priority.

To the chagrin of IT managers everywhere, many employees are using the same file sync-and-share platforms at home and work.

RR DONNELLEY
VENUE

Venue.RRD.com
www.rrdonnelley.com
888.773.8379

Best Practices in Controlling and Tracking Financial Information Electronically is published by CFO Publishing LLC, 51 Sleeper Street, Boston, MA 02210. Please direct inquiries to Linda Klockner at 617-790-3248 or lindaklockner@cfo.com.

CFO Research and RR Donnelley developed the hypotheses for this research jointly. RR Donnelley funded the research and publication of our findings. At CFO Research, David W. Owens directed the research, and Katherine Teitler and David W. Owens wrote the report.

RR Donnelley is the sponsor of this report. All information contained in this publication is for informational purposes only and should not be construed as legal, accounting, tax, or other professional advice of any kind, on any subject matter. RR Donnelley expressly disclaims all liability in respect to actions taken or not taken based on any or all the content herein.

CFO Research is the sponsored research group within CFO Publishing LLC, which includes *CFO* magazine, CFO Conferences, and CFO.com.

September 2014