2021

Data Governance Trends:

Predictions, pitfalls and technologies for the future of digital work

EGNYTE

Table of Contents

Introduction 3

Major Trends 4

Data Deluge 5

- Content: Here, There, and Everywhere
- A Range of Repositories in a Remote-Work World
- Top Concerns About Content Sprawl

Risk Report 8

- Customer Content Meets Security
- Ransomware in the Crosshairs

CIO Wishlist 11

Barriers Remain

The Role of AI Going Forward

Methodology 14

Introduction

Remote work isn't going away anytime soon, nor is the long list of apps and tools employees rely on to store data and collaborate on projects. These shifts have been a lifesaver for employees navigating the pandemic, but there's also been a ripple effect for businesses trying to get a handle on their disparate collections of content.

Unstructured data is growing at unprecedented and exponential levels. This represents one of the biggest challenges facing IT leaders today, as content such as emails and files are constantly shared across businesses and with third-parties. Moreover, the content often contains sensitive information, such as personally identifiable information (PII).

To make matters worse, this data is housed in multiple locations, including private data centers, the cloud, corporate devices, and personal devices—some of which is outside IT's purview. All this falls against the backdrop of regular reports of high-profile ransomware cases, leaving IT executives scrambling to secure their data, even though they don't all agree on the best path forward.

In July 2021, Egnyte partnered with Wakefield Research to understand:

- How content is being stored and shared in hybrid work environments.
- The top data security threats associated with the current work paradigms.
- The strategies companies have adopted—or plan to adopt—to combat these issues.

We surveyed 400 C-level IT leaders across industries, with a focus on understanding the challenges in securing and governing the single largest source of enterprise data risk: unstructured content. (Content includes all the information stored in files like Excel, Word and PowerPoint documents, as well as images, video and more.) The results of Egnyte's second annual Data Governance Trend Report were enlightening, and several major trends emerged:

Results: Major Trends

1. **Remote work will remain a reality.**
In 2020, IT leaders said the shift to remote work accelerated content sprawl and created new levels of risk. In 2021, they said remote work will continue for the foreseeable future.

2. **Content is everywhere.**
Companies use an average of 14 informal content repositories, including email, messaging apps and unauthorized cloud storage.

3. **Ransomware is in the spotlight.**
Ransomware has become a top data security concern for IT leaders, with 25% citing it as the second biggest security priority for business leadership.

4. **Businesses are split on the impacts of ransomware.**
Concerns about being locked out of company data is nearly matched by worries over data being publicly exposed.

5. **Mid-sized businesses are at a disadvantage.**
While the vast majority of respondents plan to invest in new security solutions, small to mid-size businesses are less likely to already have tools in place. They're also less likely to have the resources to implement those capabilities going forward.

6. **The path forward with AI is unclear.**
Many IT leaders plan to implement AI as part of their security portfolio, but they don't agree on how best to apply it or whether their businesses are fully committed to AI.

Data Deluge

It should come as no surprise at this point, but data continues to grow exponentially. In 2020, 64.2 zettabytes of data were created, captured, copied and consumed globally, and that figure is projected to experience a 23% compound annual growth rate through 2025. Only a small fraction is saved or retained, but it's still a staggering figure, with an installed base of 6.7 zettabytes of storage capacity last year.

Egnyte's 2021 Data Governance Trends report highlights a specific problem that arises from all this data being created: content sprawl.

Content: Here, There, and Everywhere

This flood of content being generated and stored creates significant challenges for IT teams trying to keep company and user data secure. This survey reflects the scope of the problem. More than half the IT leaders surveyed (52%) say their companies have at least 10 file storage repositories.

Average Number of File Storage Repositories in use

Response	%
1 file storage service	**0**
2 file storage services	**4**
3-4 file storage services	**10**
5-9 file storage services	**35**
10-20 file storage services	**31**
More than 20 file storage services	**21**

The degree of content sprawl often comes down to time and scale. One-fifth (21%) of all respondents say they have more than 20 file storage repositories, but that figure is even higher for companies with more than 1,000 employees (44%), $1 million or more in annual revenue (40%), and those that have been around for more than 20 years (27%).

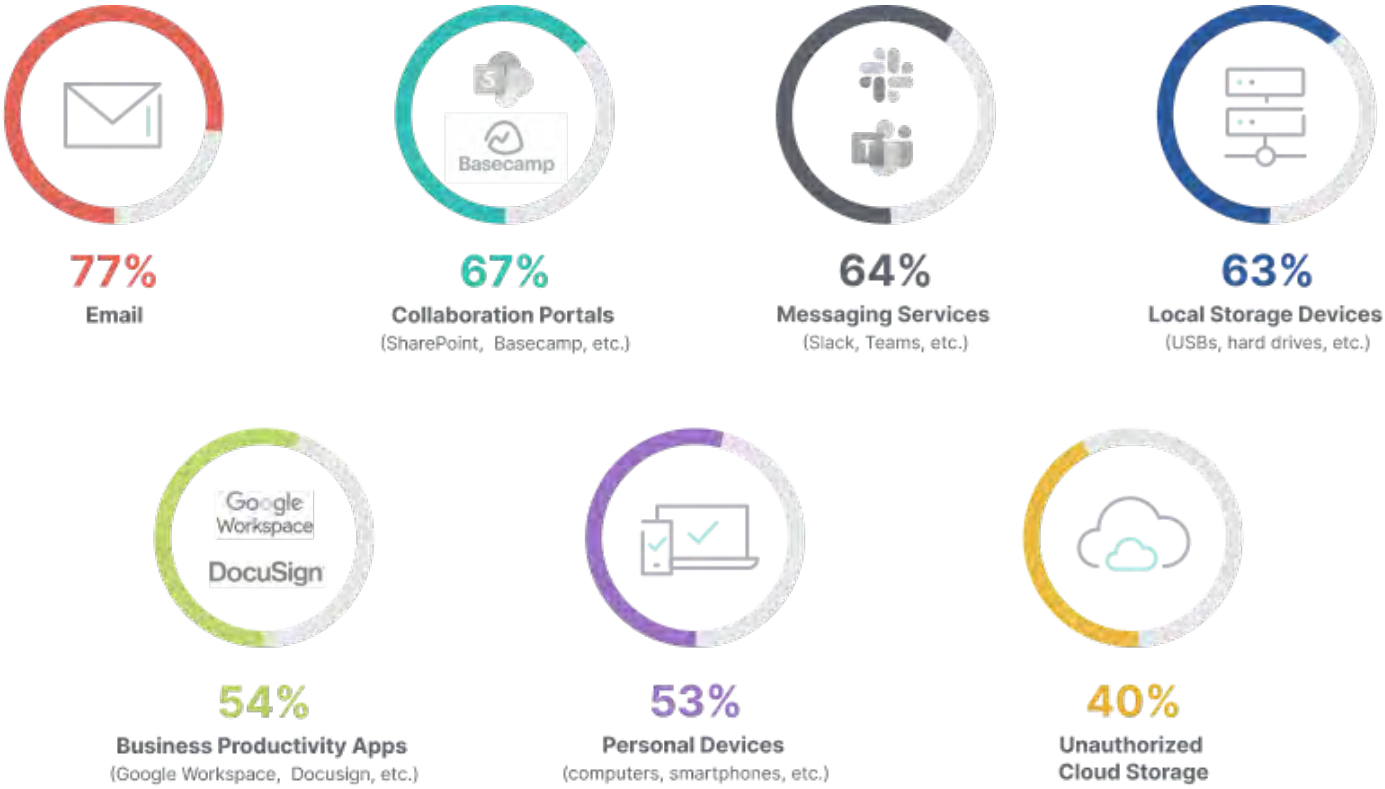
Interestingly, the IT leaders that say their business is completely prepared for a ransomware attack are more likely to have 20-plus repositories (36%). While that could be attributed to hubris, it might also be a sign that those organizations have the resources and governance in place to better secure their content, regardless of where their users put it.

A Range of Repositories in a Remote-Work World

With the vast majority of IT leaders (88%) expecting some form of remote work to continue through 2022, the use of multiple content repositories is likely to remain a problem in the short-term. A closer look at the repositories in use is reflective of the continued remote work environment. It also highlights the fact that content is finding its way into more untraditional data stores.

Employees today rely on a multitude of tools and techniques to remain productive, and many of those tools have become de facto storage repositories for all sorts of content. This includes email (77%), collaboration tools (67%), messaging services (64%), and productivity apps (54%). Perhaps most alarming, from a security perspective, is the number of respondents who cite the use of personal devices (54%) and unauthorized cloud storage (40%) for file storage at their companies. The likelihood of these being repositories is almost universally higher for businesses that are older, larger, and have more revenue.

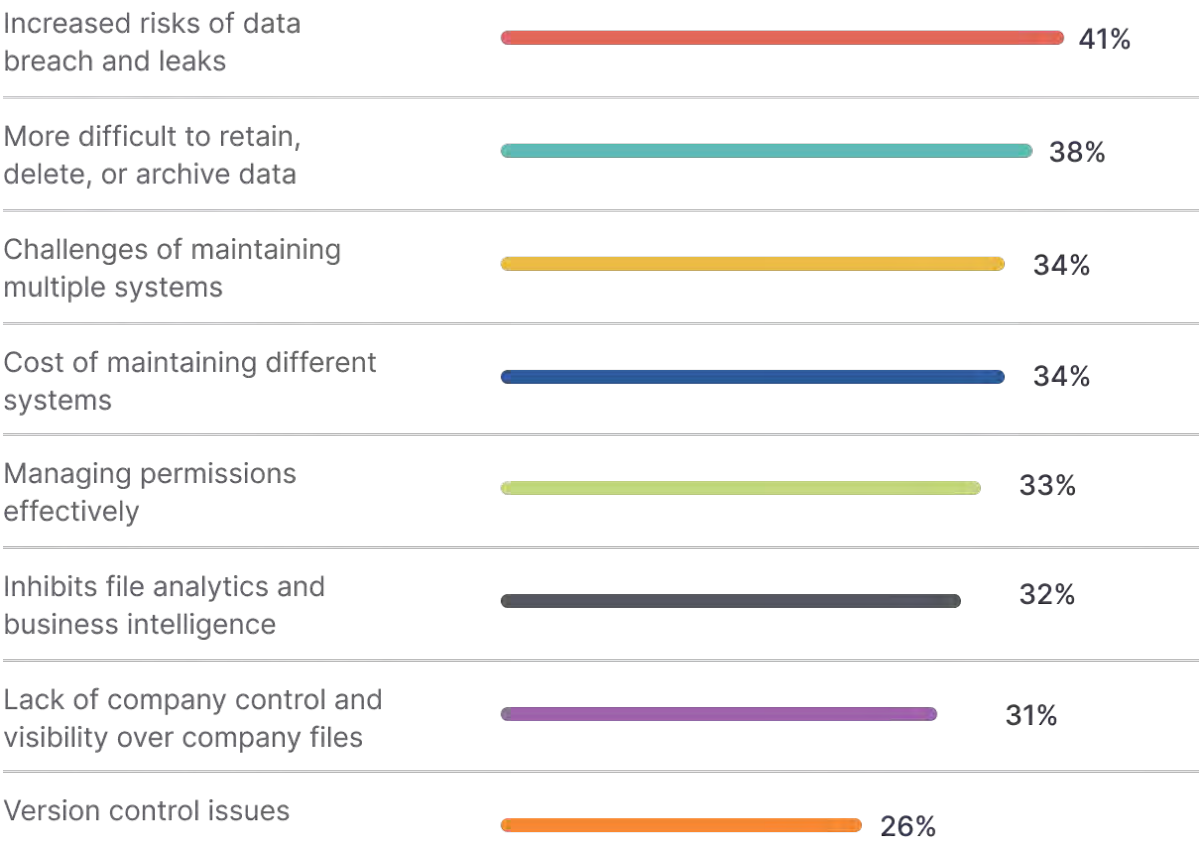
Informal Repositories: Top locations where files are stored and shared



Top Concerns About Content Sprawl

BYOD and shadow IT are potential attack vectors for hackers due to the lack of internal controls and visibility. Those types of security threats are a big part of why 41% of IT leaders say their top concern with content sprawl is the increased risk of data breaches and leaks.

Other top concerns point to the complexity that comes with wrangling so many repositories.



2021 vs. 2020

Increased risk of data breaches and leaks was the top concern in 2020 too. But with the number of IT leaders citing it going up slightly (41% v.s. 40%), clearly this is an issue that hasn't gotten any better a year later.

Risk Report

CIOs and other IT leaders have good reason to be concerned about content sprawl. They estimate nearly half (49%) of their company files contain sensitive information, such as PII or credit card numbers, with 21% saying at least three-quarters of their files contain sensitive information. Additionally, 65% suspect files and documents with sensitive information are saved locally to employees' personal devices.

This represents a significant risk to companies. That data may be subject to regulatory restrictions, such as General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). It's also a prime target for hackers who can then hold the content for ransom.

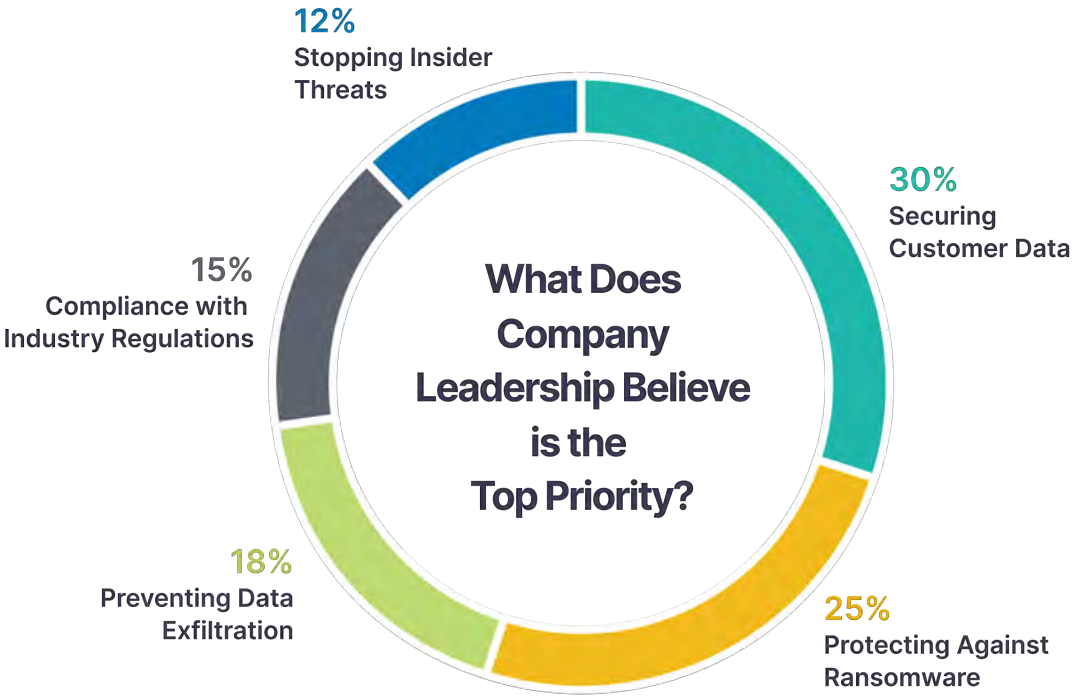
Customer Content Meets Security

The unstructured nature of content makes it particularly difficult to secure. The problem is compounded when the data is stored in multiple locations. Ironically, more than a third (35%) of respondents say emails are the most difficult data source to secure, even though 77% report employees using email to share files. Email is particularly challenging because it's a gateway for ransomware and other attacks, data leakage and insider threats.

Which Data Source is Most Difficult to Secure?

1. Email
2. Cloud File Storage
3. Personal Devices (computers, smartphones, etc.)
4. Structured Databases
5. On-premises file storage
6. Productivity apps
7. Company devices (computers, smartphones, etc.)

Content sprawl has wide-ranging implications for organizational priorities around data security, privacy, and compliance. Thirty percent of IT leaders cite securing customer data as their top priority—an effort that can be severely hampered when that data is spread across such a wide attack surface. Customer data is front of mind for many organizations with new data privacy laws being enacted and ransomware on the rise.



Ransomware in the Crosshairs

Ransomware is also a major issue for IT executives, as a quarter of respondents say it's a top priority for company leadership. Companies with annual revenue over $100 million are more likely to rank ransomware as their top concern (37%) than companies with less than $100 million (21%).

It's no wonder ransomware is getting so much attention, as the average ransomware payment has climbed 82% since 2020, to $570,000. And while payouts make headlines, IT leaders are surprisingly split on the impacts of these extortion attempts. The majority (54%) say their biggest worry is having their files encrypted, making them inaccessible and disrupting operations. However, 46% say they're more concerned about data being improperly accessed and made public.

Which of the following consequences of a ransomware attack worries you more?

46%
Your company's data being improperly accessed and made public

54%
Your files getting encrypted, making them inaccessible and disrupting business operations

Forty-four percent of IT leaders at smaller companies say they are completely or mostly prepared for a ransomware attack, versus 69% of larger enterprises, while companies that have or plan to invest in security solutions in the next 12 months are far more likely to say they're prepared for an attack (93% vs. 65%). This split in preparedness is precisely why smaller companies are sometimes the target of ransomware. And if they partner with larger organizations, they can be at even greater risk because hackers will use them as a backdoor to steal enterprise data and secure more lucrative paydays.

2021 vs. 2020

Sensitive files are only becoming more common: 84% of IT leaders report at least one in four files contain sensitive information—a 16-point jump from last year (68%). And while these figures were roughly the same across most demographics in 2020, a significant gap emerged in 2021. Smaller companies—in terms of both the number of employees and revenue—are far more likely to have sensitive data in at least a quarter of their files.

CIO Wishlist

With the depth and breadth of the challenge of securing unstructured data expanding, it's no surprise 80% of IT executives are likely to invest in new cloud security solutions, including cloud access security broker (CASB) and data loss prevention (DLP) software, in the next 12 months.

However, they're not all starting from the same place in terms of preparedness. While small to mid-sized businesses are just as vulnerable as their larger counterparts, they're less likely to already have the necessary security tools at their disposal.

Has your company specifically purchased any of the following cloud security solutions?

Response	Average	Under 1K employees	Over 1K employees	<$100M in revenue	>$100M in revenue
DLP	**55%**	**41%**	**78%**	**42%**	**73%**
Data access governance	**47%**	**41%**	**56%**	**36%**	**62%**
CASB	**43%**	**41%**	**48%**	**39%**	**50%**

In terms of investments, there's a wide gulf between mid-sized businesses and large enterprises, especially around DLP and data access governance. These types of solutions have traditionally been reserved for highly regulated industries, but they're quickly gaining broader traction. Businesses of all sizes need tools to protect sensitive data amid expanding regulations and growing concerns over distributed employees and data repositories, insider threats, and ransomware—and mid-sized businesses are clearly playing catch up.

Barriers Remain

Most organizations have invested in some tools, but some IT leaders say they face barriers to adoption, including cost (34%), lack of time to research (31%) and lack of in-house skills (28%). Small to mid-sized businesses are especially challenged in areas where a lack of resources don't always show up in the bottom line, such as a lack of free time and in-house skills.

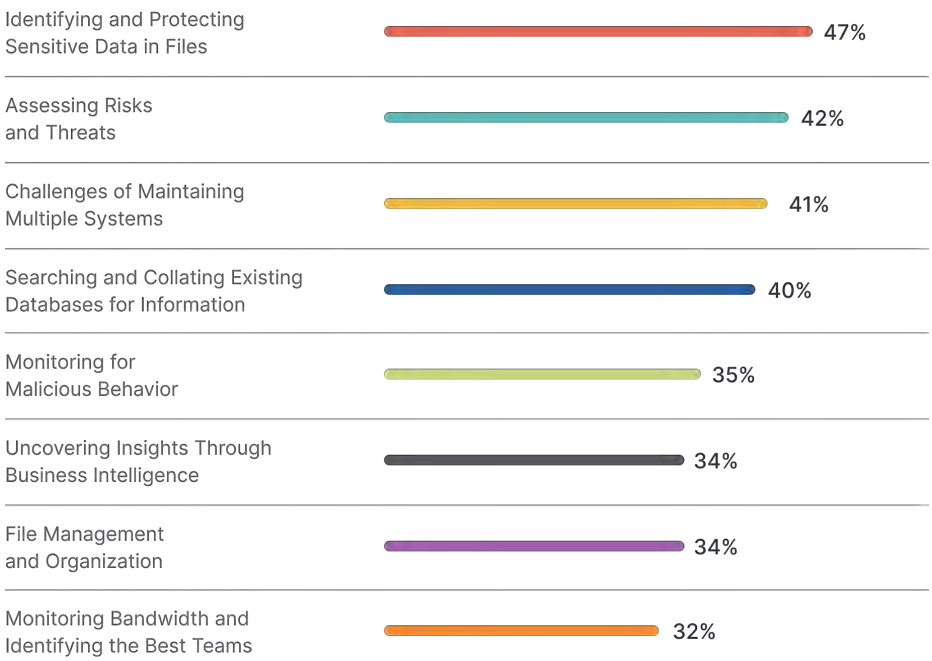
Biggest Barriers to Investing in New Cloud Security Tools:

SMB 100-1000 Employees	Response	Large Company 1000+ Employees
27%	**Too Expensive**	38%
37%	**Haven't Had the Time to Research**	27%
35%	**Don't Have the Right People to Administer Them**	24%
24%	**Too Complex for Our Business**	26%
29%	**I Personally Don't Have the Expertise to Administer Them**	19%
22%	**I'm Not Sure What They Do**	22%
8%	**Don't Need Them**	11%

The Role of AI Going Forward

The focus on securing sensitive data has prompted C-level tech executives to seek new technologies to buttress their efforts. Among AI applications currently in use or planned as investments in the next 12 months, identifying and protecting sensitive data files was the most frequently cited by IT leaders (47%). This has become one of the more common services offered by cloud providers, as these types of tools can scan files for PII and other sensitive information. Other, more complex applications also top the wishlist, including risk and threat assessments (42%), and monitoring for malicious behavior (40%).

What Does Company Leadership Believe is the Top Priority?



Collectively, nearly all respondents (99%) say their companies plan to use AI applications within the next year. But how that plays out in reality remains to be seen. Seventy percent of IT leaders say leadership isn't ready to fully commit to AI, despite having talked it up.

2021 vs. 2020

In 2020, 24% of IT leaders agreed that identifying and protecting sensitive data in files was a top use for AI tools. In 2021, a full 47% say they have already implemented or plan to implement an AI-based solution for sensitive data discovery in the next 12 months.

Methodology

The Egnyte Survey was conducted by Wakefield Research (www.wakefieldresearch.com) among 400 U.S. C-Levels with Technology/IT Titles at companies of 100+ employees, between July 15 and July 26, 2021, using an email invitation and an online survey. Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. For the interviews conducted in this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 4.9 percentage points from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

Egnyte provides the only unified cloud content governance solution for collaboration, data security, compliance, and threat prevention for multicloud businesses. More than 17,000 organizations trust Egnyte to reduce risks and IT complexity, prevent ransomware and IP theft, and boost employee productivity on any app, any cloud, anywhere. Investors include GV (formerly Google Ventures), Kleiner Perkins, Caufield & Byers and Goldman Sachs. For more information, visit **www.egnyte.com.**

Contact us

+1-650-968-40181350
W. Middlefield Rd.
Mountain View, CA 94043, USA
www.egnyte.com