Symantec 2010
Information Management Health Check

Global Results

July 2010
CONTENTS

Executive Summary ................................................................. 3
Methodology ........................................................................ 4
Finding 1: .............................................................................. 5
Finding 2: .............................................................................. 6
Finding 3: .............................................................................. 8
Symantec Recommendations ................................................. 9
Appendix ................................................................................. 11
EXECUTIVE SUMMARY

Information is the lifeblood of any enterprise, but too much information can create information overload. It can drive up storage costs, expand backup windows, complicate eDiscovery and increase litigation risks.

Symantec’s 2010 Information Management Health Check surveyed 1,680 enterprises in 26 countries and found that the vast majority of companies realize they need a formal information retention plan to address these issues. Yet despite this awareness, most have not implemented such a plan.

This report explores the issues caused by this information management plan gap and presents simple steps that companies can take to gain control of their information.
METHODOLOGY

Applied Research fielded the survey by telephone in June of 2010. The survey respondents came from a wide variety of industries and at each company we spoke to senior IT and legal executives.

Geographically, the study reached 1,680 respondents in 26 countries. The confidence level is 95 percent +/- 2 percent.
FINDING 1:  
**Gap exists between information management goals and practice**

The survey’s first finding is that an information management gap exists between what enterprises realize they should do and what they actually do. Most enterprises (87 percent) said they realize a proper information retention strategy will allow them to delete unnecessary information.

That’s a very important goal in terms of reducing costs, litigation risk and eDiscovery complexity.

However, less than half (46 percent) actually have a formal information plan. Many are exploring implementing such a plan, but are stuck trying to create the perfect plan. Our next two findings show why this is a costly mistake.

There are also differences in how IT and legal respondents cited issues for lack of an information retention plan. Forty-one percent of IT administrators don’t see a need for a plan, 30 percent said no one is chartered with that responsibility and 29 percent cited cost. Legal cited the top issues as cost (58 percent), lack of expertise to build a plan (48 percent) and no one chartered with the responsibility (40 percent).

---

**Pie Chart:**

- **Yes**: 87%
- **No**: 13%

**Question:** Do you believe that a proper information retention strategy/policy should allow you to delete unnecessary information?
FINDING 2:  
Gap is driving common information management mistakes

Our second finding is that this information management gap is driving many common mistakes.

First, enterprises are over-retaining information. In lieu of an information retention plan, companies are keeping everything “just in case.”

For example, three quarters of backups have infinite retention or are on legal hold. That is a huge number. Think of this: Some estimates are that there is roughly 50 petabytes of backup tape stock in enterprise backup libraries. That means nearly 38 petabytes of backup tape is dedicated to retaining enterprise information forever in a format that is extremely difficult to access and manage. To put that in perspective, 38 petabytes of backup tape would stretch to the moon and back 13 times with enough left over to circle the globe 7 times. That is a lot of tape.

Furthermore, enterprises told us they know a quarter of the information isn’t even needed and shouldn’t be retained.

Enterprises also report that one in six files is archived indefinitely.

Second, enterprises are performing legal holds incorrectly. Most (70 percent) are using their backup systems to perform legal holds – something backup systems were not designed to do effectively. Worse yet, 25 percent preserve the entire backup set indefinitely.

What this drives is an environment in which nearly half (45 percent) of backup storage comes from legal holds alone.

In addition, enterprises cited that, on average, 40 percent of information placed on legal hold is not specifically relevant for that litigation. Using archiving and backup together provides immediate access to the most pertinent information while allowing enterprises to backup less.

Third, enterprises are employing improper practices in the area of backup and recovery as well as archiving. For example, 51 percent prohibit employees from creating their own archives on their local machines and drives. And while most companies prohibit end users from
creating their own archives, 65 percent admit that end users routinely do so anyway.

Finally, nearly half of the enterprises use their backup software for archiving files and documents, something it was neither designed for nor is especially good at doing.
FINDING 3:
Gap is driving serious enterprise consequences

The survey’s final finding is that the information management gap is driving serious enterprise problems.

Applied Research analyzed the 1,680 responses for Symantec and divided them into 5 tiers based on their information management practices. The differences between the top tier enterprises and the bottom tier were stunning.

- Top tier enterprises are more likely to have a formal information retention plan (71 percent) than the bottom tier enterprises (27 percent)
- Top tier enterprises are less likely to use their backup software for archiving (26 percent) than the bottom tier enterprises (49 percent)
- Top tier enterprises have very little backup storage that they felt was not necessary and shouldn’t be backed up
- Top tier enterprises also used much less (20 percent) of their backup storage for legal holds than the bottom tier enterprises (60 percent)

These differences have dramatic consequences.

First, high storage costs. Studies show that storage costs continue to skyrocket as over retention has created an environment where it is now 1,500 times more expensive to review data than it is to store it. And it is not just the raw cost of tape stock and hard disks, but the higher costs of managing such massive stores.

Second, backup windows are bursting at the seams. It is becoming increasingly common to hear of weekend backups taking more than a single weekend. Recovery times are even worse. The time it takes to restore such massive backups will bring any disaster recovery program to its knees.

Finally, with the massive amounts of information stored on difficult-to-access backup tapes, eDiscovery has become a lengthy, inefficient and costly exercise.
SYMANTEC RECOMMENDATIONS

Enterprises know they need to do better – that they need a plan. But creating the “optimal” plan is difficult. As a result, many enterprises do nothing and suffer serious consequences as a result. Symantec recommends a simple 5-step action plan to solve the information management problem:

Step 1: Create a formal information retention plan
Without a formal plan it is difficult to know when – and what – to delete. This is what drives over-retention. Get started with a formal plan as soon as possible. You can always improve on the plan as you progress.

Step 2: Stop using backup for archiving and legal holds
Backup is intended for disaster recovery. All you need is a few weeks of backup (30-60 days at the outside). Files should be deleted or archived after that. So, enterprises should:

- Reduce backup retentions to 60 days or less
- Implement a full-featured archive system

Step 3: Deploy deduplication
Step 1 will go a long way towards decreasing your storage footprint, but it is not enough. Implementing deduplication will further reduce the amount of storage needed in all areas of the company. Enterprises should:

- Deploy deduplication close to information sources, where possible, to reduce storage everywhere. This reduces the amount of storage that must travel across the network
- Centralize the management of deduplication to reduce complexity

Step 4: Delete according to your information retention plan
Most enterprises believe that a proper information retention strategy should allow them to delete unnecessary information. They are right. By using backup only for disaster recovery you can delete older backup sets within months instead of years.
Step 5: Use an archive system for discovery
In general, discovery means identifying relevant material, placing it under hold so it cannot be deleted and then efficiently reviewing the information to extract the value.

- Use a full-featured archive system to make discovery as efficient as possible.

- No need to make additional physical copies “for compliance reasons.” No more legal holds in backup.

- Search for and find information much more quickly – and with more granularity. This will reduce the time and cost it takes to evaluate litigation risk.

- Enforce information retention policies (what can and cannot be deleted and when) automatically. Courts are generally more supportive of automated, policy-driven deletion than of ad-hoc, manual deletion.
APPENDIX
All graphs included
Demographics: All respondents

How many employees are in your company worldwide?

- 500 - 2,500: 26%
- 2,500 - 10,000: 37%
- 10,000 - 50,000: 22%
- 50,000 - 200,000: 11%
- 200,000 - 1,000,000: 4%
- More than 1,000,000: 0%

In which industry do you work?

- Financial: 10%
- Manufacturing: 10%
- Technology: 9%
- Telecommunications: 8%
- Healthcare: 7%
- Automotive: 7%
- Consumer: 7%
- Insurance: 7%
- Retail: 6%
- Education: 4%
- Energy: 4%
- Media: 3%
- Online: 3%
- Public sector: 3%
- Transportation: 3%
- Real estate: 2%
- Other (please specify): 2%
- Hospitality: 1%
IT Department: General Section

What is your job title?

- IT: CIO/CTO: 17%
- IT: VP/SVP: 12%
- IT: Director: 9%
- IT: Manager: 20%
- IT: Staff: 32%
- Other (Please indicate): 2%

What is your level of knowledge in terms of day-to-day operations in each of the following areas?

- Disaster Recovery: 64%
- Backup and recovery: 65%
- Information retention: 65%
- Archiving: 67%
- eDiscovery: 77%
IT Department: Data Center Section

Roughly how many "data centers" does your organization have?

In terabytes, what is the total storage capacity of all of your organization's data centers combined worldwide?
What is your estimated growth of storage over the next 12 months?

40% Median

Roughly what percent of your data-center backup goes to each of the following storage types?
(Mean shown)

- Tape: 27%
- Disk (other than VTL): 23%
- VTL (virtual tape, i.e., disk that acts like tape): 19%
- Removable optical media: 15%
- Flash/raid: 13%
- Other (please specify): 3%
**IT Department: Backup Section**

### Roughly what percent of your data-center archiving goes to each of the following storage types? (Means shown)

<table>
<thead>
<tr>
<th>Storage Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tape</td>
<td>20%</td>
</tr>
<tr>
<td>Disk (other than VTL)</td>
<td>22%</td>
</tr>
<tr>
<td>VTL (virtual tape, i.e., disk that acts like tape)</td>
<td>10%</td>
</tr>
<tr>
<td>Removable optical media</td>
<td>15%</td>
</tr>
<tr>
<td>Flashram</td>
<td>12%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>4%</td>
</tr>
</tbody>
</table>

### Why do you have the backup retention periods that you have today? (Select all that apply.)

- Compliance with company policies: 64%
- Compliance with government regulations: 50%
- Recovery point objectives: 53%
- Compliance with industry regulations: 52%
- Business unit requirements: 48%
- Litigation risk: 41%
- Cost issues: 14%
- That is how we have always done it: 15%
- I just wanted to cover all my bases: 10%
- We don’t have backup retention periods defined: 3%
What percentage of your backups has infinite retention?

- 30%

Are you routinely performing legal holds in your backup environment?

- Yes: 70%
- No: 30%
**What percentage of your backup storage is dedicated to each of the following?**
(Medians shown)

- Legal holds: 45%
- Infinite retention for other reasons: 30%

---

**For which storage locations do you deploy deduplication in your backup?**

- Data center: 63%
- Remote offices: 18%
- We don’t use it: 35%
- Desktop/laptop: 6%
IT Department: Archiving Section

Which of the following features are needed for an archiving system to be complete?

1. Required, not necessary
2. Optional, but nice to have
3. Required

- 72% 
- 62% 
- 54% 
- 54%

- 5% 
- 8% 
- 6% 
- 7%

- 23% 
- 30% 
- 30% 
- 39%

What do you use for archiving information in your organization?

1. We don't archive this kind of information
2. We archive manually
3. We use software designed specifically for archiving
4. We use our backup software

- Email: 24%, 32%, 20%, 10%
- SharePoint: 45%, 10%, 15%
- Files and Documents: 43%, 41%
- Database or Application data: 45%, 41%
- Instant Messenger (IM): 35%, 32%
- SMS Test and PHI on BlackBerry devices: 41%
- Social Media (Twitter, Facebook, etc.): 35%, 23%
Why are you using backup for your archiving needs? (SharePoint)

- It is good enough: 39%
- I can use existing staff/resources: 28%
- Using my backup solution doesn't require new training: 20%
- Cost issues: 21%
- Other (Please specify): 2%

Why are you using backup for your archiving needs? (Files and documents)

- It is good enough: 38%
- I can use existing staff/resources: 25%
- Using my backup solution doesn't require new training: 24%
- Cost issues: 12%
- Other (Please specify): 1%
Why are you using backup for your archiving needs?
(SMS text)

- It is good enough: 32%
- Using my backup solution doesn’t require new training: 26%
- I can use existing staff/resources: 26%
- Cost issues: 14%
- Other (Please specify): 2%

Why are you using backup for your archiving needs?
(Social media)

- It is good enough: 36%
- I can use existing staff/resources: 39%
- Using my backup solution doesn’t require new training: 21%
- Cost issues: 31%
- Other (Please specify): 2%
What is your policy around end users creating their own archives?

- We don't have a policy: 20%
- We have a policy that allows it: 29%
- We have a policy that partially restricts it: 28%
- We have a policy that prohibits it: 23%
IT Department: eDiscovery Section

How do you implement a legal hold on email? (Mark all that apply.)

- We have an automated archiving system that handles this: 35%
- Preserve an entire backup set: 21%
- Image the entire mailbox, directory, database, etc.: 22%
- We have enterprise search and collection tools: 11%
- We ask the end user not to delete items: 6%
- We ask the end user to copy files to new location: 4%

How do you implement a legal hold on SharePoint? (Mark all that apply.)

- We have an automated archiving system that handles this: 54%
- Preserve an entire backup set: 23%
- We have enterprise search and collection tools: 15%
- Image the entire mailbox, directory, database, etc.: 14%
- We ask the end user not to delete items: 8%
- We ask the end user to copy files to new location: 5%
How do you implement a legal hold on files and documents?
(Mark all that apply.)

- We have an automated archiving system that handles this: 34%
- Preserve an entire backup set: 25%
- We have enterprise search and collection tools: 16%
- Image the entire mailbox, directory, database, etc.: 13%
- We ask the end user not to delete items: 8%
- We ask the end user to copy files to new location: 5%

How do you implement a legal hold on social media?
(Mark all that apply.)

- We have an automated archiving system that handles this: 23%
- Preserve an entire backup set: 18%
- We ask the end user not to delete items: 17%
- Image the entire mailbox, directory, database, etc.: 16%
- We ask the end user to copy files to new location: 14%
- We have enterprise search and collection tools: 13%
Do you believe that a proper information retention strategy/policy should allow you to delete unnecessary information?

- Yes: 87%
- No: 13%

How many days does it take you to give your lawyers information they need to make an early case assessment?

- 7 days
What are the goals you are trying to achieve in your information management (backup/archiving) strategy?

Imagine the following medium to low risk scenario: You receive a request to produce all email and electronic information from five of your organization's executives. Which of the following would you be likely to search? (Mark all that apply.)
IT Department: Disaster Recovery Section

What is the state of your data center's disaster recovery plan (actions taken during an event)?

- Informal/Undocumented: 5%
- Need work: 11%
- Average: 18%
- Pretty good: 38%
- Excellent: 26%

How confident are you in your organization's DR plan?

- 84%
How is your recovery site provisioned?

- Another site/facility owned by our company: 39%
- Shared IT infrastructure at a service provider: 33%
- Dedicated IT infrastructure at a service provider: 24%
- We don't have a separate recovery site: 6%

Which of the following best describes how you protect your non-virtualized critical applications and data against a site outage? (Select all that apply.)

- Backups written directly to disk or tape storage at a secondary site: 46%
- Replication of the live data to a secondary site with clustering failover: 19%
- Replication of backups written to disk-based storage: 19%
- Replication of the live data to a secondary site without clustering failover: 11%
- Backup to tapes sent to off-site storage/on site: 27%
- Replication of backups written to VTL: 24%
### Which of the following best describes how you protect your virtualized critical applications and data against a site outage? (Select all that apply.)

<table>
<thead>
<tr>
<th>Description</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backups written directly to disk or tape storage at a secondary site</td>
<td>40%</td>
</tr>
<tr>
<td>Replication of live data to a secondary site with clustering failover</td>
<td>37%</td>
</tr>
<tr>
<td>Replication of live data to a secondary site with virtual technology failover or manual failover</td>
<td>55%</td>
</tr>
<tr>
<td>Replication of backups written to disk-based storage</td>
<td>34%</td>
</tr>
<tr>
<td>Backup to tape with tapes sent to off-site/DR site</td>
<td>24%</td>
</tr>
<tr>
<td>Replication of backups written to VTL</td>
<td>23%</td>
</tr>
</tbody>
</table>

### What is your involvement with each of the following data protection technologies as they pertain to disaster recovery?

- 1 - No plans
- 2 - Discussing
- 3 - Implementing
- 4 - In place

<table>
<thead>
<tr>
<th>Technology</th>
<th>1 - No plans</th>
<th>2 - Discussing</th>
<th>3 - Implementing</th>
<th>4 - In place</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous data protection with replication</td>
<td>40%</td>
<td>41%</td>
<td>36%</td>
<td>35%</td>
</tr>
<tr>
<td>Application-based replication</td>
<td>26%</td>
<td>26%</td>
<td>22%</td>
<td>24%</td>
</tr>
<tr>
<td>Host-based replication</td>
<td>22%</td>
<td>21%</td>
<td>21%</td>
<td>24%</td>
</tr>
<tr>
<td>Array-based replication</td>
<td>19%</td>
<td>19%</td>
<td>19%</td>
<td>19%</td>
</tr>
<tr>
<td>Snapshits</td>
<td>13%</td>
<td>10%</td>
<td>20%</td>
<td>22%</td>
</tr>
</tbody>
</table>
IT Department: Declared Disaster Section

How many times have you had to declare a disaster and perform recovery operations at your recovery site in the past five years?

Median: 1
What was the cause(s) of these disaster declaration(s)?
(Mark all that apply.)

- Network failure: 45%
- Power failure: 44%
- Computer hardware failure: 42%
- Computer software failure: 34%
- User/operator error: 27%
- Malicious employee behavior: 19%
- Flood: 17%
- Hurricane: 15%
- Winter storm: 15%
- Fire: 15%
- Data breach or loss: 12%
- Earthquake: 9%
- Terrorism or war: 6%
- Tornado: 8%
- Chemical spill: 7%

In general, how well did your plan work?

- Significantly poorly: 3%
- Somewhat poorly: 7%
- Neutral: 20%
- Somewhat well: 45%
- Significantly well: 25%
IT Department: Information Retention Section

How would you rate your preparedness to responding to a legal, compliance or regulatory request for electronically stored information?

- Extremely unsure: 2%
- Somewhat unsure: 9%
- Neutral: 19%
- Somewhat confident: 42%
- Extremely confident: 28%

How many times in the past year has your company had to respond to a legal, compliance or regulatory request for electronically stored information?

Median: 2
What percentage of the time do you leverage your backup infrastructure to comply with these types of requests?

- 40%

When asked to respond to a legal, compliance or regulatory request for electronically stored information, what percentage of the time do you do each of the following?

- 22% Completely fail to fulfill the request
- 34% Partially fail to fulfill the request
- 28% Successfully fulfill the request, but more slowly than the requester would like
- 40% Successfully fulfill the request in a timeframe that is acceptable to the requester
In those cases where you were asked to respond to a legal, compliance or regulatory request for electronically stored information and were either late, partially, or completely unsuccessful, which of the following consequences did you experience?

- Hampered our decision-making ability: 33%
- Damage to Enterprise reputation or embarrassment: 23%
- Compromised legal position: 18%
- Fines: 16%
- Raised our profile as a potential litigation target: 9%
- Sanctions by courts: 3%

What percentage of your deletions are made without considering your retention policies?
(Medians shown)

- Primary storage: 20%
- Backup storage: 10%
- Archives storage: 10%
**IT Department: Drivers Section**

Please rate the following drivers in terms of their importance in setting policies about how long to retain versus when to delete electronic files.

- **Regulatory requirements about how long to keep electronic files**: 47% extremely important, 44% somewhat important, 40% neutral, 32% somewhat unimportant, 4% extremely unimportant.
- **Risk from potential litigation**: 24% extremely important, 16% somewhat important, 14% neutral, 6% somewhat unimportant, 4% extremely unimportant.
- **Preservation for business purposes**: 30% extremely important, 32% somewhat important, 35% neutral, 4% somewhat unimportant, 6% extremely unimportant.
- **Cost**: 30% extremely important, 32% somewhat important, 39% neutral, 4% somewhat unimportant, 4% extremely unimportant.
How many different classes of retention does your company have at this time?

Median: 5

How closely do your backup retention policies follow your information retention policies?

- The two are completely independent of each other: 10%
- There is a slight correlation between the two: 7%
- Neutral: 35%
- They are highly correlated: 40%
- They are completely in lockstep: 21%
Does your formal policy specify how long you are required to keep these types of files?

- Database or application data: 94%
- Documents and file systems: 92%
- Email: 88%
- Content management system such as SharePoint: 82%
- Fax: 61%
- Voicemail: 60%
- Instant Messenger (IM): 53%
- SMS Text and PIM-to-PIM on BlackBerry devices: 52%
- Social media: 41%

When you are no longer required to keep a set of electronic information, which of the following actions do you take? Mark all that apply.

(Email)

- Delete the file right from primary storage: 50%
- Archive the file: 27%
- Backup the file: 22%
- Delete the file from all archive media: 21%
When you are no longer required to keep a set of electronic information, which of the following actions do you take? Mark all that apply.

(SharePoint)

- Archive the file: 28%
- Delete the file right from primary storage: 28%
- Delete the file from all archive media: 24%
- Backup the file: 20%

When you are no longer required to keep a set of electronic information, which of the following actions do you take? Mark all that apply.

(Files and documents)

- Archive the file: 31%
- Delete the file right from primary storage: 24%
- Delete the file from all archive media: 23%
- Backup the file: 22%
**IT Department: Compliance with Plan Section**

When you are no longer required to keep a set of electronic information, which of the following actions do you take? Mark all that apply.

(Social media)

- Delete the file right from primary storage: 43%
- Delete the file from all archive media: 22%
- Archive the file: 21%
- Backup the file: 14%

How do you ensure compliance with your formal retention plan? (Mark all that apply.)

- We ask IT to comply with the plan: 62%
- We have technology that automates compliance and policies: 63%
- We ask users to comply with the plan: 45%
- Third party services company: 19%
Legal Department: General Section

Why don’t you have a formal retention plan or plans to create one?

- We don’t see a need for it: 41%
- Nobody is chartered with that responsibility: 39%
- Cost: 26%
- We don’t have time: 22%
- We lack the expertise to build such a plan: 14%

What is your job title?

- Corporate attorney: 37%
- Legal liaison to IT: 51%
- Legal project manager: 23%
- General counsel: 8%
- Paralegal: 4%
Legal Department: eDiscovery Section

When you are implementing a legal hold on email, what actions do you take? (Mark all that apply.)

- IT uses an automated archiving system that handles this: 39%
- We ask IT to image the entire mailbox, directory, database, etc.: 51%
- We ask IT to preserve an entire backup set: 24%
- We have enterprise search and collection tool: 0%
- We ask the end user to copy files to new location: 2%
- We ask the end user not to delete items: 1%
When you are implementing a legal hold on SharePoint, what actions do you take? (Mark all that apply.)

- We ask IT to preserve an entire backup set: 55%
- IT uses an automated archiving system that handles this: 28%
- We ask IT to image the entire mailbox, directory, database, etc.: 17%
- We have enterprise search and collection tool: 16%
- We ask the end user to copy files to new location: 5%
- We ask the end user not to delete items: 4%

When you are implementing a legal hold on files and documents, what actions do you take? (Mark all that apply.)

- We ask IT to preserve an entire backup set: 27%
- IT uses an automated archiving system that handles this: 27%
- We have enterprise search and collection tool: 23%
- We ask IT to image the entire mailbox, directory, database, etc.: 18%
- We ask the end user not to delete items: 5%
- We ask the end user to copy files to new location: 2%
Have you ever rehearsed legal hold scenarios?

- No: 20%
- Yes: 80%

Are you aware of anyone within your organization that has been deposed around information management practices and technology?

- No: 19%
- Yes: 81%
Have you identified an individual responsible for depositions concerning information management practices and technology?

- Yes 84%
- No 16%

What percentage of information that is placed on legal hold is not specifically relevant for that litigation?

- Median 40%
What consequences have flowed from preserving more than you needed to?

- Increased time spent to collect, review, and analyze information: 76%
- Increased costs associated with collection, review, and analysis: 69%
- Risk that sensitive information may be disclosed: 66%
- Compromising your position in potential or actual litigation: 48%
- Unintentionally made information available for potential future litigation: 22%

Do you believe that a proper information retention strategy/policy should allow you to delete unnecessary information?

- Yes: 94%
- No: 6%
How many days does it take IT to give the legal department information you need to make an early case assessment?

Imagine the following medium to low risk scenario:
You receive a request to produce all email and electronic information from five of your organization's executives. Which would you (or IT on your behalf) be likely to search?

0% 20% 40% 60% 80% 100%

- Their local machines
- Their archives
- All other mailboxes in your organization looking for emails too
- Their personal share files
- Backup images
- Common file shares
- Content management systems, such as SharePoint
- The mailboxes for these five executives
- Database or applications
- SMS texts or BlackBerry PIN-to-PIN messages
- IM messages
- Their social media traffic (Twitter, Facebook, etc.)
- Their volumual
- Their faxes
Legal Department: Information Retention
Section
How many times in the past year has your company had to respond to a legal, compliance or regulatory request for electronically stored information?

When asked to respond to a legal, compliance or regulatory request for electronically stored information, what percentage of the time do you do each of the following?

(Medians shown)
In those cases where you were asked to respond to a legal, compliance or regulatory request for electronically stored information and were either late, partially, or completely unsuccessful, which of the following consequences did you experience?

- Flaws: 41%
- Compromised legal position: 32%
- Damage to Enterprise reputation or embarrassment: 32%
- Sanctions by courts: 6%
- Hampered our ability to make decisions in a timely fashion: 6%
- Raised our profile as a potential litigation target: 3%

What is the status of your formal information retention plan (if any)?

- Don't have one and no plans to create one: 4%
- We are in the discussion/planning phase: 49%
- We are currently implementing our plan: 19%
- We have a plan in place: 29%
Legal Department: Drivers Section

Please rate the following drivers in terms of their importance in setting policies about how long to retain versus when to delete electronic files.

- 1 - Extremely unimportant
- 2 - Somewhat unimportant
- 3 - Neutral
- 4 - Somewhat important
- 5 - Extremely important

![Bar chart showing driver importance ratings]

What is your timeframe for implementing your formal information retention plan?

- Within 30 days: 7%
- 1 to 3 months: 12%
- 3 to 6 months: 32%
- 6 months to 1 year: 10%
- 1 to 2 years: 5%
- More than 2 years: 3%
- No set timeframe: 7%
**When did you implement your plan?**

- Within 30 days: 3%
- 1 to 3 months: 13%
- 3 to 6 months: 42%
- 6 months to 1 year: 17%
- 1 to 2 years: 35%
- More than 2 years: 10%

**How many different classes of data retention does your company have at this time?**

- Median: 5
Does your formal policy specify how long you are required to keep these types of files?

- Email: 100%
- Files and documents: 97%
- Database or application data: 97%
- SharePoint: 90%
- Instant messenger (IM): 72%
- Faces: 72%
- SMS Text and PIM-to-PIM on blackberry devices: 67%
- Voicemail: 60%
- Social media: 53%

When you are no longer required to keep a set of electronic information, which of the following actions are supposed to be taken? Mark all that apply.

(Email)
- Delete the file from all archive media: 30%
- Delete the file from primary storage: 25%
- Backup the file: 25%
- Archive the file: 20%
When you are no longer required to keep a set of electronic information, which of the following actions are supposed to be taken? Mark all that apply.

**SharePoint**

- Delete the file from primary storage: 28%
- Delete the file from all archivemedia: 27%
- Backup the file: 25%
- Archive the file: 20%

**Files and documents**

- Backup the file: 58%
- Delete the file from all archivemedia: 16%
- Archive the file: 10%
- Delete the file from primary storage: 13%
When you are no longer required to keep a set of electronic information, which of the following actions are supposed to be taken? Mark all that apply. (Social media)

- Delete the file from all archive media: 35%
- Delete the file from primary storage: 27%
- Archive the file: 22%
- Backup the file: 17%

How do you ensure compliance with your formal retention plan? (Mark all that apply.)

- We ask IT to comply with the plan: 77%
- We have technology that automates compliance and policies: 77%
- We ask users to comply with the plan: 60%
- Third-party services company: 23%
What does your compliance automation technology do?
(Mark all that apply.)

- Reports problems/exceptions to policy: 50%
- Automatically archives files: 91%
- Automatically deletes files beyond their retention period but this feature is not yet activated: 59%
- Automatically deletes files beyond their retention period and this feature is active: 20%

How well does each of these constituents understand your enterprise information retention plan?

- Compliance or legal personnel: 40% (33%), 42% (50%), 42% (40%)
- IT: 55% (50%), 50% (40%)
- End users: 5% (8%), 3% (2%)
How well do each of these constituents comply with your enterprise information plan?

- Compliance or legal personnel: 38% do not comply at all, 53% comply somewhat, 45% comply well, 13% comply very well, 3% comply excellent.
- IT: 4% do not comply at all, 13% comply somewhat, 50% comply well, 17% comply very well, 3% comply excellent.
- End users: 8% do not comply at all, 13% comply somewhat, 50% comply well, 17% comply very well, 3% comply excellent.

Why do you have no plans to create a formal information retention plan?

- Cost: 58%
- We lack the expertise to build such a plan: 48%
- Nobody is chartered with that responsibility: 40%
- We don't have time: 23%
- We don't see a need for it: 10%