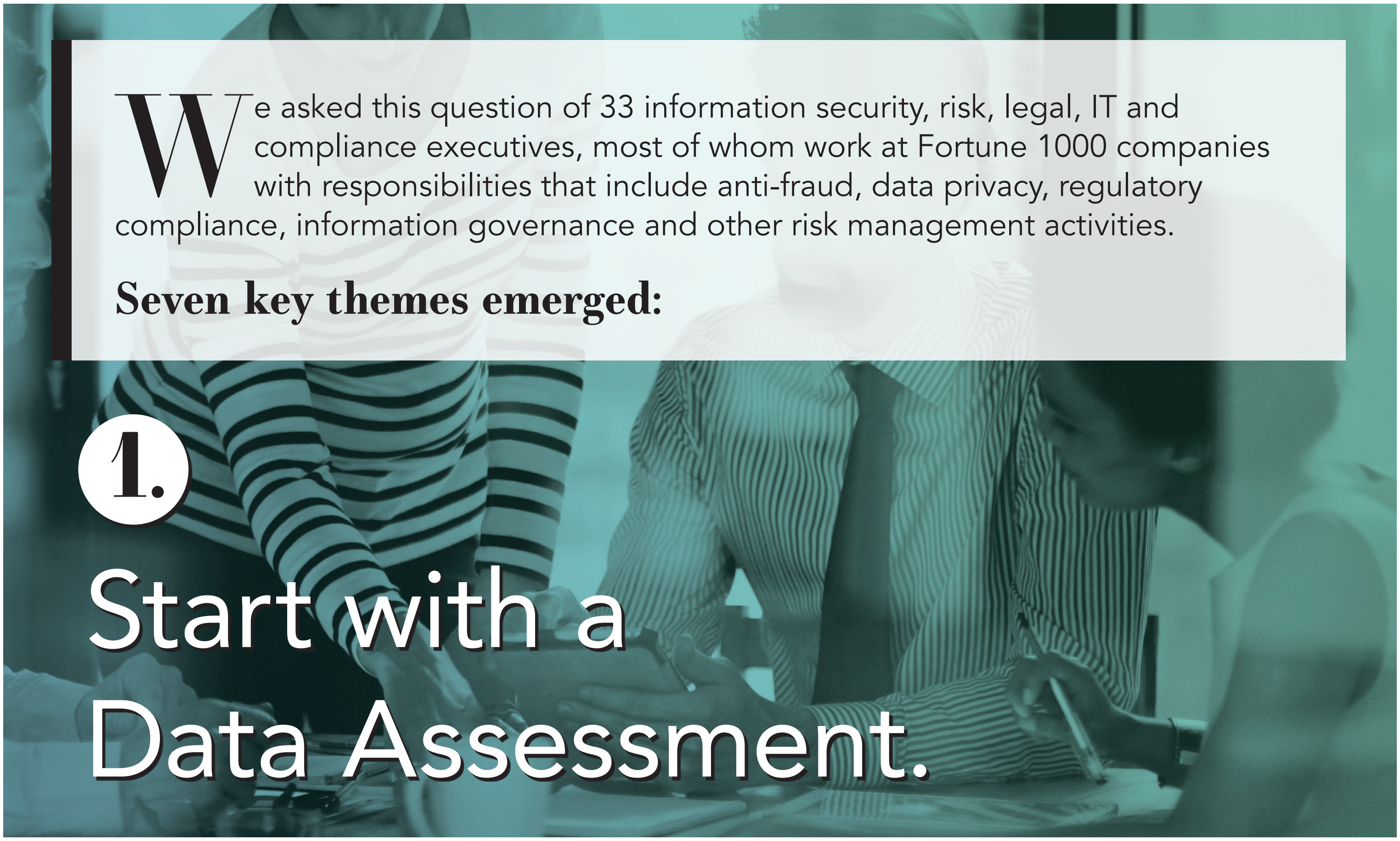
ADVICE™
FROM COUNSEL

Tackling Data Security Risks

Data breaches. Employee fraud. Regulatory change.

These headline-grabbing business challenges are keeping many legal, information security, IT and compliance departments up at night. Organizations are challenged to support the modern workplace environment – mobile phones, remote employees, cloud collaboration sites, social media, IM platforms and chatrooms – while keeping this data secure and easily retrievable for legal or regulatory needs. How can organizations create an information governance framework that protects data while staying adaptive to the rapidly evolving business landscape (*GDPR, Brexit, Privacy Shield, etc.*)?

FTI™ CONSULTING | TECHNOLOGY



We asked this question of 33 information security, risk, legal, IT and compliance executives, most of whom work at Fortune 1000 companies with responsibilities that include anti-fraud, data privacy, regulatory compliance, information governance and other risk management activities.

Seven key themes emerged:

1. Start with a Data Assessment.

For many, the process of beginning an information governance program can be daunting. *Where do you begin? Who should be involved? How do you ensure the right executive buy-in? How do you keep momentum going?*

To help answer these questions and focus the project, a third of respondents recommended conducting a data assessment at the outset.

Advice:

Ⓐ

"Conduct a baseline assessment without any assumptions and understand the company's culture."

Ⓑ

"Start with an assessment and determine what is already being managed; since you cannot boil the ocean, you need to figure out where to start and where you need to go."

Ⓒ

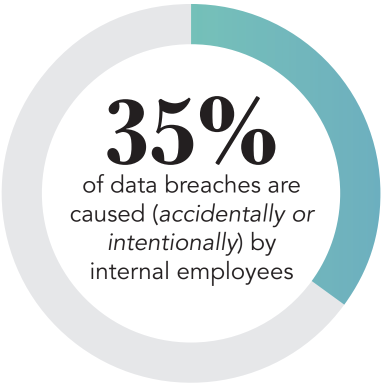
"That risk assessment should drive where you need to focus your efforts."

Benefit:

Have a clear roadmap that will help you prioritize projects.

2. Engage Internal and External Experts.

Because of the risks involved, data security is now an enterprise-wide endeavor, and not just the concern of IT or information security teams. External data breach threats are rapidly evolving, and recent research from Forrester indicates that 35% of data breaches are caused (accidentally or intentionally) by internal employees.



To help offset this, most respondents recommended recruiting expert analysis to "determine where your weaknesses and gaps are" since "it's hard to do that internally." Or, as another respondent said, "Seek out external expertise because the field is too complex for any one individual to manage and the risks are too high."

Advice:

Ⓐ

"If it is just you on an island, you will not succeed; tap into industry analysts and thought leaders for guidance since you cannot do it alone."

Ⓑ

"Hire someone with a good deep knowledge of technical implementation and crafting policy."

Ⓒ

"You need to ask someone and figure out what others are doing; engage a full cross-section of business personnel beyond senior leadership."

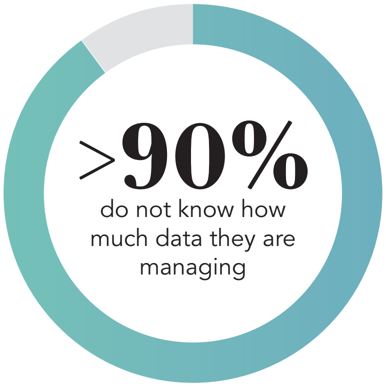
Benefit:

Subject matter experts can ensure your program is up-to-date, and internal leaders can aid in company adoption of best practices.

3. Prioritize Data Remediation.

Across the board, respondents expressed frustration at runaway data volumes, with over 90% saying they do not know how much data they are managing. Keeping redundant, outdated or trivial (ROT) information can make it harder to find and protect the truly sensitive information under the company's care.

Respondents recommend creating or updating an organizational data map, especially as part of a data assessment, and using data remediation to regularly cull out unimportant information.



Advice:

Ⓐ

> “Data has a lifecycle and represents a huge liability today. At the end of its useful life, a company needs to purge it to promote an environment of data minimization.”

Ⓑ

> “The most important data held in Salesforce is not that substantial, but shared folders are filled with significantly more data. The key data is not that substantial.”

Benefit:

Less data means lower storage costs and the ability to focus on protecting sensitive information.

4. Prepare for the General Data Protection Regulation (GDPR).

The impending GDPR regulation, set to go into effect in May of 2018, is top of mind for respondents with employees, customers or partners within Europe. The European data privacy law will harmonize European data privacy laws to ensure that data transferred from Europe to the US is appropriately handled and that personally identifiable information (PII) remains secure.

Respondents recommended conducting an analysis of the law to understand how this will impact current processes and systems.

Advice:

A

"The company is developing a cross-functional task force to evaluate the different options supported by an external law firm."

B

"The company will focus on alternatives, including implementing the model clauses, which will be part of an overall third party risk strategy."

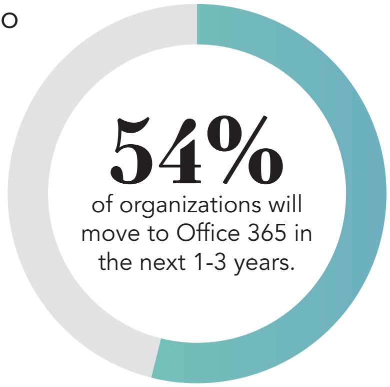
Benefit:

Understanding and acting in compliance with GDPR from the outset of implementation can help your company avoid costly fines and reputational risk.

5. Use your Migration to Microsoft Office 365 as an Opportunity.

According to a recent Gartner survey, 54% of organizations will move to Office 365 in the next 1-3 years. The migration from one archive to another provides an opportunity for an organization to take stock of its email and data management practices and potentially update policies and remediate data for greater efficiency and security.

From legal holds to data retention and security policies, respondents in the process of migrating to Microsoft Office 365 shared how the procedure provides an opportunity to make additional process and policy improvements.



Advice:

A “Office 365 has new encryption technology to protect data better. The use of cloud-based storage for employees facilitates sharing, but opens up a new set of compliance standards and requirements.”

B “The company implemented a 90-day e-mail retention program along with Office 365 so if you do not manage your e-mail within 90 days, it is automatically deleted.”

C “Cloud e-mail in general has created information governance concerns, including expanded individual storage, which has created concerns about over retention resulting in litigation challenges, but there is better ability to search and manage the data, which is an advantage. The cloud system has inherent vulnerabilities, but Microsoft is a trusted partner.”

Benefit:

Take advantage of a company-wide migration to remediate old data and update important policies and processes.

6.

Right-Size Your Solutions.

Some organizations have faced major data breaches, regulatory investigations or large-scale litigation that warrants a complete audit and update of existing processes and technology. Other organizations may not have the same pressures, budget or appetite to make anything other than small changes to key processes.

Respondents repeatedly stressed the importance of fine-tuning any information governance and data security program to the particular needs of the organization.

Advice:

Ⓐ

“Know your audience and make sure the program is culturally adapted to the organization.”

Ⓑ

“Knowing the population of people you serve personally, figuring out how to make compliance a value-added part of their activities, and fully understanding the businesses that you support is key.”

Ⓒ

“The biggest thing is to engage the business and make sure that what you are doing is right-sized for the organization and that you have the resources to achieve success.”

Benefit:

Information governance and data security have a greater chance of success if the program is fine-tuned to the needs and culture of the organization.

7.

Data Security is a Multi-Faceted Challenge and Requires a Multi-Faceted Approach.

Given the complexities within the corporate data environment, there isn't a silver bullet technology, process or executive that can solve the immense problem of keeping data secure.

That said, respondents recommended a broad range of actions to ensure that an organization's people, processes and technology are all working in alignment to address various internal and external threats.

Advice:

Ⓐ "Encrypt data so that personally identifiable information is stored in a protected environment and access is limited to those with positions that require such access."

Ⓑ "Some competitors pay 'friendly hackers' to test their systems."

Ⓒ "Figure out how to get employees taking more training and determine how to make the training message more effective."

Ⓓ "The ability to be prepared to take the necessary steps to protect customers when the data breach happens is as important as prevention; there is just as much liability created by a poor reaction as by the fact that it happened in the first place."

Ⓔ "Encourage a clean desk policy so that information is secured at the end of the day and personal information is not left publicly available in breach of a client's security request."

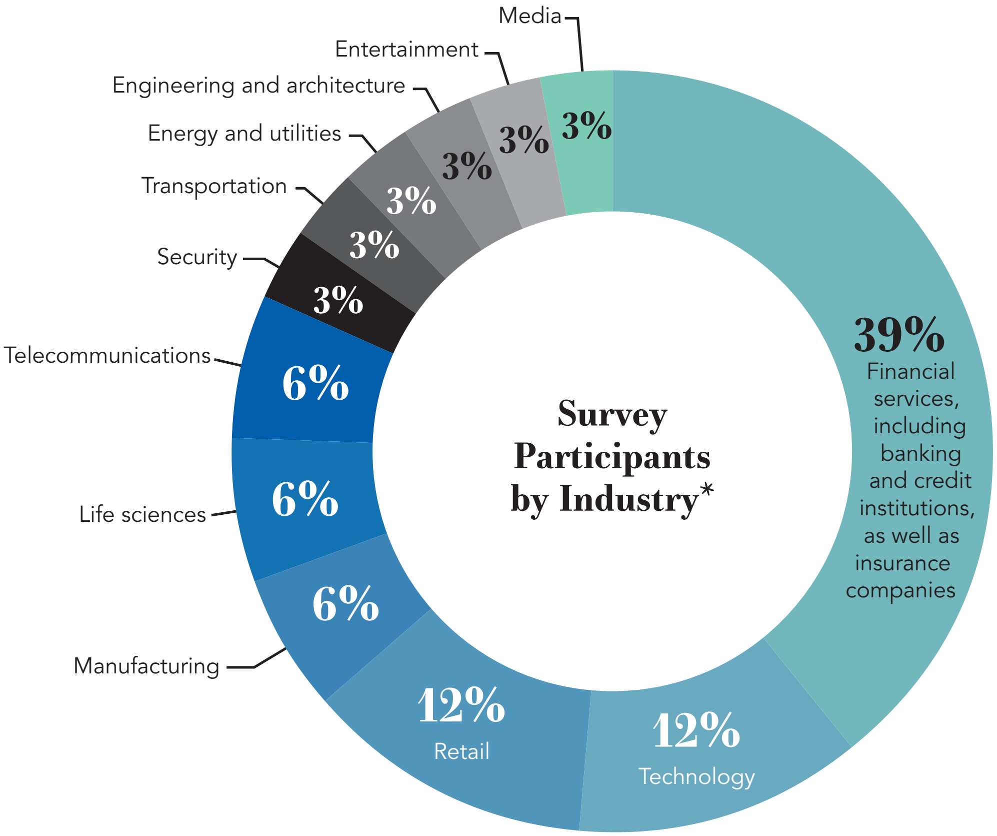
Benefit:

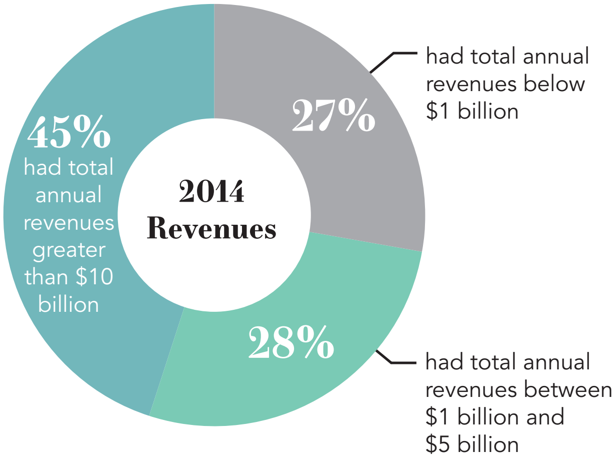
The adage "hackers only need to get it right once, whereas organizations have to get it right every time" is true, but implementing the right programs can help ensure better security. This includes regular employee trainings, using outside third parties to test your system, creating a tiered architecture to better secure sensitive information, and developing a data breach response plan.

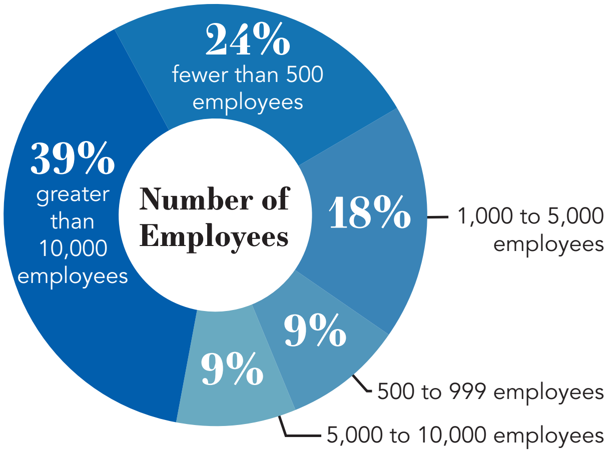
Appendix

FTI Technology partnered with Ari Kaplan Advisors to conduct the study by interviewing 33 in-house compliance leaders. Most participants were from Fortune 1000 corporations and all spoke by telephone, under condition of anonymity, during November and December of 2015.

Of this year's participants, 100 percent develop and implement compliance policies and processes, while 78 percent select, implement, or manage information governance software and service providers.







About Advice from Counsel

Through in-person events, virtual meetings, webcasts, surveys and reports, Advice from Counsel helps e-discovery leaders share ideas and advice with peers in an open and collaborative forum. Begun in 2008 as an annual survey and report on top e-discovery trends, Advice from Counsel has evolved into an interactive community of e-discovery professionals working to strengthen the people, process and technology at the core of e-discovery. Advice from Counsel is sponsored by FTI Technology.

ADVICE FROM COUNSEL™

FTI Technology solves data-related business challenges, with expertise in legal and regulatory matters.

As data grows in size and complexity, we help organizations better govern, secure, find, analyze and rapidly make sense of information. Innovative technology, expert services and tenacious problem-solving provide our global clients with defensible and repeatable solutions. Organizations rely on us to root out fraud, maintain regulatory compliance, reduce legal and IT costs, protect sensitive materials, quickly find facts and harness organizational data to create business value. For more information, please visit www.ftitechnology.com.

For more information:
ftitechsales@fticonsulting.com
www.ftitechnology.com

North America:	+1 (866) 454 3905
Europe:	+44 (0) 20 3727 1000
Australia:	+61 (2) 9235 9300
Hong Kong:	+852 3768 4500
Shanghai:	+86 21 5108 8002
Tokyo:	+81 3 5369 3939

FTI™ CONSULTING | TECHNOLOGY