Making Everything Easier!™

Data Classification

FOR DUMMIES®

A Wiley Brand

Brought to you by

SPIRION™

Todd M Feinman

Data Classification

FOR DUMMIES®

A Wiley Brand

Spirion® Special Edition

by Todd M Feinman

FOR DUMMIES®

A Wiley Brand

Data Classification For Dummies®, Spirion Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-23612-2 (pbk); ISBN 978-1-119-23613-9 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Project Editor: Kim Darosett
Acquisitions Editor: Amy Fandrei
Editorial Manager: Rev Mengle
Business Development Representative: Christiane Cormier
Production Editor: Antony Sami

Table of Contents

Introduction

Due to the rapidly changing landscape of data creation, storage, and use, the crucial business processes of sensitive data classification and management have recently become a hot topic across board rooms and c-suite officers, as well as among regulatory bodies.

If you have a clear plan and use innovative technologies that simplify and facilitate these processes, you can now make data classification — the enabling centerpiece of sensitive data management — part of your everyday business operations, decreasing risk and security costs, and improving your overall security posture.

About This Book

In today's world, data breaches are an increasingly common occurrence. The greatest financial damage typically comes when breaches expose sensitive data, such as social security numbers, credit card data, health information, business secrets, government records, and other valuable data that is costly to lose, especially when a breach captures the media's attention. Once public, such breaches result in tens or hundreds of millions of dollars in post-breach losses.

The underlying reasons for these breaches are the uncontrolled handling of data and misallocation of security controls: You can't protect data that's unknown to you. Your greatest defense against financial and reputational post-breach losses is to know what your sensitive data is, restrict where it's stored, limit who has access to it, protect it, and monitor its usage as well as the creation of new sensitive data. To effectively accomplish each of these tasks, you must first find and classify your sensitive data.

When you know where your data is and what is sensitive (as well as what isn't), you're empowered to control and protect information to prevent a security incident from becoming

a data breach. An appropriately classified file would not be accidentally emailed by an employee. And, even if it were, that classified file could be blocked from being sent by a security technology configured to automatically read and act on its classification.

Finally, by identifying and minimizing your sensitive data footprint and ensuring that sensitive data is seen and used only by authorized individuals, you can reduce the risk of unauthorized disclosure and data leaks.

How This Book Is Organized

In this book, you'll discover how to identify sensitive data, implement a data classification process, and minimize the risk of data breaches. You'll also learn about the risks of not classifying data and the components of a data classification and sensitive data management life cycle. This book will arm you with the tools for managing risks and preventing the next financially damaging breach of sensitive data.

Icons Used in This Book

Throughout this book, you'll find the following icons in the margins.

This icon points out helpful information.

You'll want to commit this information to memory.

Chapter 1

What Is Classified Data?

In This Chapter

- Exploring what sensitive data is
- Understanding when you need to classify data

When most people hear the term *classified,* they think of a government agency that stamps "top secret" on a document for a limited group of people's eyes only. While this is an accurate example, the broader definition of data classification is the act of separating data into groups, or *classes,* based on shared characteristics with the intent of treating those groups differently. Businesses classify documents primarily to find and manage sensitive data to ensure it's not exposed to unauthorized eyes.

Classification lets you identify and tag the sensitive information from within the ocean of data stored across your enterprise and in cloud file synchronization and sharing platforms. You can then focus resources and apply protections appropriately to reduce the risk of data exposure.

This chapter explains what makes data sensitive, how to determine how sensitive the data is, and when and how to classify it.

Understanding What Makes Data Sensitive

Sensitive data is information that, if accessed by an adversary or otherwise made public, would create a liability. While this statement may seem self-explanatory, let's take a closer look:

- **Information:** Information of any type may become sensitive data. Personally identifiable information (PII), protected health information (PHI), payment card industry (PCI) data, and other specifically regulated information are examples of common sensitive data.

  Intellectual property, trade secrets, and company financial records are also sensitive data. While they may not be governed by regulations, the fact that such data is highly valuable classifies it as sensitive, and thus worthy of special treatment and protection.

- **Adversary:** Adversaries are not just the proverbial bad guys wearing masks. They may be trusted insiders engaged in industrial espionage, hackers, or individuals defined by the company as "unauthorized" people, even if they're innocent employees in good standing.

- **Access:** Adversaries use a variety of methods to *access* sensitive data, but it doesn't necessarily mean the data is taken; it may simply be viewed. For example, access methods may include social engineering, theft, hacking, or simple Internet searches for old, forgotten data. Adversaries often take advantage of under-trained, over-burdened, or well intentioned but not security minded employees.

- **Liability:** Liability takes many forms. Regulated data might carry legal fines for mishandling. Proprietary information in the wrong hands can devastate stock value. Breached client information can spawn lawsuits, tarnish your company's reputation, and reduce goodwill. And mishandling of sensitive information can result in embarrassment for clients and loss of future revenue.

The definition of sensitive information continues to evolve as businesses grow, technologies advance, laws are created, and

new uses for information are developed. A good rule of thumb is that the more valuable the data is and the bigger the impact it would have on your business if compromised, the more sensitive it probably is.

Determining the Sensitivity of Information

One way to try and determine how sensitive certain data is, and therefore how it should be classified, is to think about how the loss of the confidentiality, integrity, or availability of that information would impact your organization.

The following bullets are based on Federal Information Processing Standards (FIPS) publication 199 published by the National Institute of Standards and Technology. It provides a framework for determining the impact that can be applied to the sensitivity of information.

Here are the three security objectives and how to determine the level of impact (low, moderate, or high):

- **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

  Potential impact: The unauthorized disclosure of information could be expected to have a limited (low), serious (moderate), or severe/catastrophic (high) adverse effect on organizational operations, organizational assets, or individuals.

- **Integrity:** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

  Potential impact: The unauthorized modification or destruction of information could be expected to have a limited (low), serious (moderate), or severe/catastrophic (high) adverse effect on organizational operations, organizational assets, or individuals.

- **Availability:** Ensuring timely and reliable access to and use of information.

> *Potential impact:* The disruption of access to or use of information or an information system could be expected to have a limited (low), serious (moderate), or severe/catastrophic (high) adverse effect on organizational operations, organizational assets, or individuals.

As the potential impact moves from low to high, the sensitivity increases, and therefore, the classification level of data should become higher and more restrictive. If your classification schema ranges from *public* to *top secret,* for example, data with a low impact across the board might be classified as public, while data with a high impact in any one area might be considered top secret.

Once you've developed a framework for classifying data, you develop your business's classification schema with additional business criteria and an understanding of your specific types of sensitive data.

Examining the Types of Sensitive Data

Sensitive data falls into two broad categories: regulated and unregulated data. *Regulated data* is always sensitive, though to varying degrees, and should always be classified. The vast majority of *unregulated data* (which includes all publically known information) is not always sensitive. However, unregulated data can also include highly sensitive information, so you must apply your data classification process to all of your data.

Regulated sensitive data

In the United States, certain classes of information are always deemed sensitive because law and regulation impose liability for improper or unauthorized access. Legislative definitions of personal information have broadened over time, led primarily by the state of California. In other countries, such as within the EU, data protection laws tend to be more comprehensive.

One of the most well-known types of sensitive data laws are breach notification laws. Starting with California's Security Breach Information Act of 2003, the majority of states have enacted breach notification laws. These laws require companies to notify consumers when sensitive personal information is accessed by an unauthorized person. The notification requirement often creates publicity that results in loss of goodwill and class action lawsuits.

In addition to notification obligations, breach notification laws often impose additional duties, which vary depending on the storage media. For example, as outlined in the California Civil Code, businesses have a duty to "provide reasonable security" for personal information. Legislative findings in several states emphasize the importance of preserving trust and confidentiality. Others emphasize the need to protect consumers from identity theft.

Consult with an attorney specializing in this area of law to become more familiar with data protection laws in your country, state, and industry, especially as they relate to cloud computing and the storage of sensitive information. Each regulation has varying levels of compliance requirements. The HIPAA regulation has up to 18 identifiers of sensitive data that must be protected, ranging from Name or Phone Number to highly confidential Social Security Number or Medical Record data. On the flipside, the PCI-DSS regulation essentially has one identifier — cardholder data — which is actually the Primary Account Number (PAN) or magnetic strip and the Name, Expiration Date, or Service Code. You can use these regulations as classification levels within your schema.

Unregulated sensitive data

In many cases, unregulated data, such as intellectual property, operational business data, and certain financial information, are also highly sensitive and critical to protect. Data classification of unregulated sensitive data typically happens through a multi-step process that begins with interviewing the data owners. These individuals will help define the level of sensitivity and what information would cause a risk to the company if leaked. If this process doesn't occur, it's unreasonable to expect the business to protect sensitive information that falls outside of regulations.

After you define your classification levels and establish a process for applying those classifications to data based on specific criteria, you're ready to classify your data.

When to Classify Data

The easy answer to when you should classify data is as soon as it's created. However, as data moves through each stage of the life cycle, it's important to evaluate and update its classification, as necessary. The phases of the data life cycle include:

- **Creation:** This is when sensitive data is first generated by machines, people, or automated processes.
- **Use:** Once a file is created, it's used. During this stage, data is viewed, processed, modified, and saved. Security controls should be applied to data at point of use.
- **Storage:** After every use, data is stored on media. Sensitive data should be stored in a protected manner, such as with access controls and encryption.
- **Sharing:** Information is often valuable only if it can be shared with others. Examples of sharing may include emailing an attachment, sharing a Google doc, syncing to a cloud provider, backing up a database, sharing the information on social media, or uploading to a website.
- **Deletion:** *Deletion* is when the data is not immediately destroyed, but made available for future overwriting by a computer. Simply hitting the Delete key and emptying the Recycle Bin won't completely remove personal information from your hard drive. Files can sometimes be undeleted or recovered until you *wipe* the drive.
- **Old, forgotten data:** Because data storage is cheap and plentiful, most data is stored and forgotten. Old, forgotten data is perhaps the most at-risk phase for data, because it often lacks adequate controls and protections.

Chapter 2

Why Classify Data?

In This Chapter

- Understanding the risks associated with sensitive data
- Examining the causes and costs of breached sensitive data

When your company has a well-defined data classification program, it greatly reduces the potential for sensitive data loss in the event of a breach and reduces data ownership and management costs. This chapter examines why it's important to build a program to manage your sensitive data.

Avoid the Hidden Cost of Classified Data

All sensitive data owned, managed, or handled by your company creates risk. While this may seem obvious, you might be surprised to learn that there are costs associated with storing sensitive data.

Maintaining sensitive data is analogous to maintaining physical inventory and what accountants call *carrying costs.* While businesses regularly account for the carrying costs of physical inventory and assets, most ignore the carrying costs of data, except for hard drives and hosted storage.

By thinking about the carrying cost of data in your business, you raise the stakes of owning classified data, and develop a culture that reduces the amount of stored classified data. This is a beneficial process because the less classified data you own, the lower your risk and liability.

To calculate the carrying costs of data, you must:

- **Inventory all data.** How much data is there, where is it stored, and how accessible is it?
- **Classify the data inventory.** Not all data is of equal value or liability. Determine the classification level for various types of data.
- **Account for risk.** What is the liability if the data is lost, stolen, or abused?

Here are steps you can take to reduce those carrying costs:

- **Eliminate excess inventory.** Shred classified information whose potential liability exceeds the present business value and carrying costs.
- **Reduce the number of classified data stores.** Decrease the number of devices storing classified data.
- **Secure your classified data store.** Use encryption, roles-based access, strong authentication, and other protection techniques.
- **Train employees how to properly handle classified data.** Also train them to be aware of and eliminate excess inventory.
- **Decrease access to classified data.** This reduces the risk of theft or mishandling.

Increase Data Awareness

Users are often the weakest link when protecting data. While malicious users do exist and can cause harm, well-intentioned employees often inadvertently create risk by mishandling data while doing their jobs.

If you try to stop certain behaviors by forcibly preventing employees with technology, they'll often be blind to the reason and feel the company is impeding their work. Without awareness, employees will always find ways to circumvent policies. In the age of cloud computing, data is often no longer in a well-controlled environment. This situation puts your company at increased risk because your employees (and the sensitive data they use and create) will begin to operate *outside* your security controls.

A better approach is to focus on solutions that help employees do their jobs while increasing their awareness of sensitive data. For example:

- Allow employees to send emails with Excel spreadsheet attachments, but when they attach the file, notify them that it contains social security numbers.
- Allow employees to sync their business files to the cloud so they can work with them remotely. However, make them aware of which files contain credit card data so they don't share links to those files.

Not all employees may need to be perform such tasks; however, once classified, security controls can now allow or deny these actions. Well-classified data will raise the visibly of its importance and allow users to become more aware of its value, changing their behavior to properly handle it.

Reduce Your Risk

Because of the sheer volume of new data created daily and the mountains of historical data stored over time, businesses have an almost incomprehensible amount of data. Most of this data would be innocuous to your business if leaked (for example, already released product information or sales reps' phone numbers), but small amounts of highly sensitive data can severely damage your business.

Rather than try to protect 100% of your company's data, classify your data so you can prioritize your resources to focus on the sensitive data that would constitute a breach.

The bigger your data footprint, the bigger your risk, and the higher your audit and compliance costs. But if you get rid of sensitive data and clean up your business processes, you can shrink your audit and compliance costs.

Prevent Costly Data Breaches

According to the Ponemon Institute's latest study, 2015 Cost of Data Breach Study – Global Analysis, the average cost of damages resulting from data breaches in the United States

alone is $6.5 million. Regulated industries such as finance, healthcare, technology, pharmaceuticals, and education were found to experience substantially higher costs.

Breach expenses include notification costs to inform your customers, obligatory identity protection services for the victims, fines and legal costs associated with non-compliance with regulations, and investigative costs to understand the root cause to prevent future incidents.

Rather than try to protect every piece of data with the same level of security controls, it's more organizationally achievable to classify data and develop robust processes around protecting classified data. Most security technologies are siloed off from one another and operate independently, but once your data is classified, it can be protected similarly by each security technology. For example, encryption, content filtering, and access control security technologies can all protect top-secret classified data with their highest level of security, and can be configured to ignore public data.

Traditional Approaches Have Reached Their Limitations

Traditionally, businesses have invested mainly in protecting the *edge* of the data center, the boundary that protects the network from the external world. Such investments certainly are justified, but they address only part of the problem. By classifying data at its source, you can focus on protecting the data itself and mitigating these concerns:

- Focusing on network perimeter protection ignores the greatest threat vector: internally stored data that might never cross the perimeter. Many recent, high-profile breaches were not the result of failed perimeter security, but rather, the attackers used compromised user accounts to steal sensitive information.
- Through the use of cloud storage, VPN, and other connections to business partners and employees' home machines, the perimeter becomes increasingly nebulous and impractical to secure.
- As attackers become more sophisticated, edge defenses are unable to adapt and keep pace with their methods.

Chapter 3

Building a Data Classification Program

In This Chapter

- Discovering and identifying sensitive data
- Eliminating and protecting sensitive data

Data classification is a way to reduce risk without decreasing productivity. A solid data protection strategy includes capabilities, such as gaining a better understanding of what and where your classified, sensitive data is. It also gets rid of what you don't need and secures what you do.

What's left is a digestible amount of clearly classified data that helps increase employee awareness, decrease compliance costs, and enable existing technology investments to better protect against data leaks.

Accurately Discover Your Data

Protecting classified data is one of the core missions of security. At the end of the day, safeguarding your company's classified information is the reason you implement security policies and solutions. Many businesses have an abundance of structured and unstructured information — such as medical data, social security numbers, emails, and intellectual property — that shouldn't leave their premises, should have restricted access, and should be behind additional layers of security.

Understanding your data accurately is the foundation of your protection strategy and helps you determine where to apply your security controls. There's danger in assuming you know where the most sensitive data is located. When you think of sensitive and private data, human resources and finance immediately come to mind, but as many security professionals have discovered, sensitive data often turns up in places you'd never expect.

Data is shared across the company and ends up in the cloud or on USB drives. It can be in databases, Excel spreadsheets, and PDF documents. It might even be in images. You could have types of sensitive data unique to your business that find their way into unexpected locations throughout your environment. Clearly, there are a lot of challenges that come with locating, identifying, and classifying sensitive information.

Other drivers add to the complexity, such as adhering to data regulations — whether you're in a regulated industry that has to report on HIPAA or handling PCI data or PII.

It all starts with accurate discovery. Understanding what and where sensitive data is — and properly classifying it — allows you to take appropriate actions to protect your business.

Identify Your Most Important Data

Once you know where your data is and what it looks like, you need to properly classify it. Data classification is a simple concept: You assign a level of sensitivity to each piece of information, making it easier to locate and retrieve. However, historically this has been difficult to execute.

Accurate classification is essential to make sense of your vast amounts of data. Without data classification, you treat all data as if it were the same or make simple assumptions based on where the data is or who owns it. These methods for deciding how, where, and to what extent to assign security controls leads to poor allocation of limited resources and increases the risk of your sensitive data being compromised.

If your data classification method is user-driven, which is the case with most organizations, your employees may resist. Even if you could get everyone to comply, the process is time consuming and error-prone because you're asking employees to classify each piece of information they use. Even if employees made perfect assessments every time, they'd need to be aware of changing classification schemas, and all employees and systems would need to modify classifications as the underlying data was modified. And even if you could overcome those challenges, user-driven classification doesn't address the problem of unclassified historical data.

But data classification doesn't have to be cumbersome if you use automated systems to streamline the process and continually monitor your data. When new data is created or existing data is modified, the system can identify it in real time and automatically classify it based on your corporate policies. You can use automated systems with very low false positive rates to search through historical data and assign appropriate classification levels.

Another aspect of automation that helps ease the process is persistent classification, which helps ensure that no matter how many times data is moved or where it goes, its classification is maintained. This reduces risk exposure and increases employee awareness and participation.

Shrink Your Sensitive Data Footprint

Data security is comprised of two key principles: keeping bad guys away from target data and decreasing the quantity of valuable targets. As you store more and more sensitive information on your computers and networks, you're increasing the number of targets for hackers, viruses, thieves, spyware, botnets, dishonest insiders, physical intrusion, and social engineering.

To protect against threats, your security measures need to do two things: Let authorized people access the data they need and keep unauthorized people out.

For example, suppose that you store sensitive information in a password-protected database. When information is inside that database, it's relatively safe. But during the normal course of business, authorized employees access that data and bring it outside the database via an interface application or through exports or cached information to do their jobs. Once the information is outside the database, it can be saved, copied, emailed, printed, posted, stored, backed up, and shared with any number of people. In this case, the sensitive data footprint has increased considerably.

Now keeping the bad guys away from the target is harder because there are so many targets. This is what happened to Sony Pictures in December of 2014, when they were attacked by North Korea. The hackers were allegedly trying to steal one specific movie, but because there was so much sensitive data available in so many places, they attacked multiple targets and wound up stealing over 47,000 social security numbers.

Chief Technology Officer of the PCI Security Standards Council, Troy Leach, said minimizing your data footprint is the key to reducing risk and simplifying PCI compliance, but it's often overlooked.

Set Policies That Can Be Enforced and Monitored

The purpose of creating policies for your business is to outline essential roles and responsibilities, specify data identification and classification policies, and define procedures for protecting data that will maintain a safe environment. The classification policies will describe the criteria to identify and categorize sensitive data, as well as the control necessary to protect data according to those classifications.

Security policies also help establish a comprehensive data security program in compliance with applicable laws and regulations, such as PCI or HIPAA. You must constantly update your policies as your business's requirements change. However, it's also essential that the policies are easy to understand, realistic, enforceable, automated, and acceptable to users.

You can use sensitive data management solutions to help define and automatically enforce policies appropriate to your needs. That way, your employees will be more willing to follow the regulatory or corporate guidelines and be productive while using the systems and controls you have in place.

Trust, but Verify

Data security shouldn't get in the way of your employees' daily work. There must be a balance between protecting data and ensuring employees have access to the information they need. Being realistic about data security policies means understanding and taking into account employee behavior.

For example, technically savvy employees might place data in the cloud, or configure their own email access outside of corporate IT security guidelines. Security and IT teams need to acknowledge and define their policies based on these realities. Make it easy for your employees to do the right thing by using solutions that automate and continuously monitor data security, and trust them to appropriately identify, classify, and protect the sensitive data they're using. Trust, but verify!

Create a Culture of Data Awareness

Look for ways to incorporate data awareness into your employees' daily activities. Many companies conduct regular security training for that purpose. You can also use solutions that help you define policies. For example, use automated, persistent classification to ensure files and emails are protected no matter how many times they're shared, moved, or copied.

Automated, persistent classification can also protect data in the cloud, which may reside in such commercial applications as Microsoft, Google, or Dropbox. Using technology solutions that visibly display classification information will serve to reinforce good behavior and employee awareness.

Embed Classification in All Processes and Systems

An effective data protection program starts with well-defined regulatory and compliance policies and is turned into reality with security controls that include data discovery, data classification, monitoring, and reporting. It takes a bit of effort to put such a program in place, but compared to the effort and cost of repairing the damage from a data breach, it's clearly time well spent. The end result is embedding knowledge from classifications into existing business processes that mitigate mistakes and risk. Ultimately employees will change their behavior and avoid sharing sensitive data that could get the company into trouble.

When former Florida Governor Jeb Bush announced his candidacy for President of the United Sates, his campaign made public all of the emails he sent and received during his time in office. One of those emails, sent by an employee of Florida's Development Disabilities Program to the Governor, included a PowerPoint presentation with a single slide displaying a chart of the district level trends for a waitlist.

When viewing this slide, there seemed to be no concern; however, the chart was pasted from Excel into PowerPoint as a Microsoft Office Excel Worksheet object, which embedded the entire spreadsheet into the presentation. Within the spreadsheet were 12,564 names, social security numbers, and dates of birth of Florida residents. While the goal of transparency was noble, the results were disastrous. Because the data was never properly classified, it was used, shared, transformed, and reused with no regard to the highly sensitive information contained within.

Once your organization has invested the time in classifying data, configure other business processes and technology systems to read that classification so that processes and systems behave differently when they encounter classified data.

Chapter 4

Top Ten Ways to Get Started with Data Classification

Now that we've covered the importance of data classification, here's a checklist to help get started on your strategy:

- **Don't go about it alone.** People are the key ingredient to making the end to end data classification solution a success. Determine your stakeholders and identify how they will be involved in the solution. The board needs to buy in and agree that this is important. Managers need to recognize that not classifying data is a risk to your business.
- **Make it a process, not a project.** No technology is a silver bullet. It requires processes to supplement and complement how it works. Create data classification policies and define procedures for protecting data. Security policies can help establish a comprehensive program in compliance with regulations.
- **Understand your data life cycle.** To protect your sensitive data effectively, it's helpful to understand its life cycle, from creation to destruction, so you can determine where to apply data classification controls.
- **Determine what is sensitive to your organization.** Sensitive data is any data that if lost, stolen, or exposed could financially harm your organization, cause reputational damage, or be a reason for termination. Once you have a definition, you can come up with the unique list of sensitive data types to find.

- **Define data roles.** Different individuals within your organization play different roles in creating and using sensitive data, but everyone should have a role in protecting it. It's essential to educate individuals about their responsibilities based on your organization's data security policies.
- **Locate your sensitive data.** Sensitive data often turns up in places you least expect, but unfortunately hackers know where to look. There is danger in assuming you know where your most sensitive data is located. Use a sensitive data management solution that can search accurately throughout your infrastructure, including images, email, databases, and the cloud.
- **Formulate classification levels.** As the potential impact moves from low to high, the sensitivity increases, and therefore, the classification level of data should become higher and more restrictive. Once you've developed a framework for classifying data, ensure you have a sensitive data management solution that can provide both automated and user-driven classification to increase adoption.
- **Monitor newly created data and existing classified data.** Data is constantly changing and being moved. It's critical that classified data be monitored to ensure it doesn't wind up in the wrong hands. Monitor new data to find and classify sensitive information.
- **Protect your sensitive data.** Once you know where your sensitive data is and you have classified it, you need to protect it. Encrypt critical data, shred or redact files, or quarantine them. Decide whether your end users and data owners should be empowered to perform remediation actions to reduce your sensitive data footprint.
- **Get serious. Get systematic. Get peace of mind.** An effective program for identifying, classifying, and protecting your sensitive data doesn't happen by chance. It requires a coordinated, ongoing effort. It may seem like a daunting task, but if you follow the recommendations in this book, it's more easily doable than you may think.

SPIRION™

PROTECT YOUR SENSITIVE DATA

AUTOMATED, PERSISTENT DATA CLASSIFICATION

www.spirion.com

Everything you need to know to create a solid data classification program

In today's world, data breaches are an increasingly common occurrence. The greatest financial damage typically comes when breaches expose sensitive data that was costly to lose and the business wasn't aware of. In this book, you'll discover how to identify sensitive data, implement a data classification program and minimize the risk of data breaches.

- ***Accurately discover your data* — explore what is and isn't sensitive and the impact of the loss of confidentiality, integrity, or availability of data**
- ***Understand when to classify data* — learn to implement security controls as data moves through its life cycle from creation to use, storage, and deletion**
- ***Set policies that can be enforced* — establish a comprehensive data security policy that increases employee participation and helps achieve compliance**
- ***Shrink your sensitive data footprint* — get tips on how to minimize your data footprint and reduce risk**

Open the book and find:

- **How to determine the sensitivity of data**
- **When and how to classify data**
- **Steps to reduce the hidden cost of data classification**
- **How to embed data awareness into business processes**
- **A checklist to easily create a data classification program**

Go to Dummies.com® for more!

Todd M Feinman, CEO of Spirion, has over 15 years of experience in the security industry and is an internationally published author and media personality. Todd received his B.S. from Lehigh University and MBA from Harvard.

DUMMIES A Wiley Brand

Also available as an e-book

ISBN: 978-1-119-23612-2
Not for resale

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.