identityfinder

How to Create an Effective Sensitive Data Protection Program

You can't protect what you can't see

Learn more

TABLE OF CONTENTS

Make it a process, not a project	3
Adopt a logical approach to data protection	4
Understand your data lifecycle	5
Define sensitive data	6
What are data roles?	7
Establish a data security process	8
Manage compliance and governance	9
Locate Sensitive Data	10
Use PPT to Protect New Data	11
Formulate Classification Levels	12
Get Serious, Get Systematic, Get Peace of Mind	13
About Sensitive Data Manager from Identity Finder	14

MAKE IT A PROCESS, NOT A PROJECT

What's the ultimate goal of information security? Protecting your organization's sensitive data. Doing that successfully, however, is a process, not a project, and it typically involves these steps:

- Adopt a logical approach to data protection
- Understand your data lifecycle
- Identify your sensitive data
- Establish data security practices
- Implement effective security controls

We'll cover each of those at a high level and explain why each is essential in arriving at a program that minimizes your sensitive data footprint and helps keep business-critical and regulated data secure and out of the hands of attackers.

ADOPT A LOGICAL APPROACH TO DATA PROTECTION

Your first step should be to make sure minimum security baselines are in place, including perimeter and end-point security. Then, to identify, find and protect data, it's essential to analyze how your business operates.

For example, an institution of higher learning is involved in teaching and research, and those activities involve generating, acquiring and protecting sensitive data connected with student health records, grades, intellectual property from research, credit card data from selling books, and more. Elements of that data are regulated by PCI, PHI, HIPAA, and other government regulations. So when a university undertakes the task of identifying, locating and protecting sensitive data, it needs to examine all those aspects of its operations. You should do the same for your organization and proceed to:

- Identify and locate your data
- Analyze how data is created and used
- Classify the data
- Prioritize data assets

UNDERSTAND YOUR DATA LIFECYCLE

To protect your sensitive data most effectively, it's helpful to understand its lifecycle, from creation to destruction. The stages in that lifecycle are:

Creation

Understand where data is created, which is essentially everywhere. There's danger in assuming that you know where your most sensitive data is located. As many security professionals have discovered, sensitive data often turns up in places you least expected. It can be in your emails, cloud, or even images. Be aware also that corporate activities such as mergers and acquisitions can add their own set of unique sensitive data to your environment.

Use

In almost all organizations, multiple people need access to sensitive data to do their jobs, which creates the issue of data drift. For example, data that may have been protected on a file server gets inserted into a PowerPoint presentation, where it's now at risk.

Archiving

This is largely the responsibility of the IT department, but all stakeholders should participate in deciding how long sensitive data needs to be kept. Clearly, you must save data that's covered by such regulations as HIPAA, PCI, and others, but keeping it longer than necessary means you're increasing your sensitive data footprint for no good reason.

Destruction

Although you may need to keep sensitive data for a specified period of time, do you need to keep it forever? In the case of medical records or data connected to litigation, you might; but for most sensitive data, destroying it at some point is the right decision.

DEFINE SENSITIVE DATA

Here's one commonly acceptable definition of sensitive data:

> *Sensitive data is information that must be protected from unauthorized access to safeguard the privacy or security of an individual or organization.*

A more-useful definition for purposes of identifying and prioritizing data to be protected is this one:

> *Sensitive data is any data that if lost, stolen or exposed, could financially harm an organization, cause reputational damage, or be reason for termination.*

Using that definition, your organization can come up with unique list of sensitive data, most of which will fall into one of these high-level categories:

Discrete groupings of data types—Includes PCI, PHI, GLBA, and data defined by state laws

Non-discrete groupings of data types—Company confidential, IP, research, sensitive internal memos, and other data critical to your organization

WHAT ARE DATA ROLES?

While individuals have different roles in creating and using sensitive data—and may play different roles at different times—everyone has a role in protecting it. Here are the roles in a typical organization.

Stakeholders

Can be anyone in the organization who derives benefit from the data, from C-level executives to analysts

Owners

Senior members of your organization whose job responsibilities include being responsible for the security of sensitive data, for example, your HR director

Stewards

Responsible for data quality standards and data security policies

Producers

Producers—Essentially everyone in your organization

Consumers

Consumers—Also essentially everyone

It's essential that your organization educates individuals about the data security responsibilities attached to their roles and impresses upon them how their actions regarding sensitive data can directly affect the organization's success and reputation.

ESTABLISH A DATA SECURITY PROCESS

Remember to approach data security as a project that will become a process. In the project phase, you need to consider:

RESOURCES

Consider the people, skill sets and resources, such as technology, you'll need. How will you get them? How much will they cost?

TIME

Key considerations that may affect the timeline for your program include:

- How much time do we have to establish our processes?
- Are we being audited?
- Are we a highly attractive target?
- Are we out of compliance?
- Is this in response to an incident?

BUY-IN

For a program to be successful, it needs buy-in from management and the user community. To get it, you'll need to clearly communicate the importance of change throughout the organization.

MANAGE COMPLIANCE AND GOVERNANCE

Compliance does not equal security. Too often, organizations think that because they're in compliance with PCI, HIPAA, SOX or other regulations, their data is secure. Not true. In fact, a smart strategy for increasing data security is to set more-stringent standards for data privacy and protection than the law requires.

Adding governance to your program ensures that the work you've done to increase security stays done, and that you're constantly verifying and enhancing the effectiveness of your program via:

- Auditing
- Proving the non-existence of sensitive data in non-secure locations
- Data destruction
- Data retention

LOCATE SENSITIVE DATA

Before you can protect it, you have to find it. Where should you look?

- Fileservers
- HR databases
- Your CMDB (configuration management database) or eGRC (Enterprise Government, Risk and Compliance) platform
- Any system of record

What questions should you ask?

- How do we receive this data?
- How is this data created?
- Who are the data operators?

Once you identify sensitive data, it's best to apply a hybrid approach to protecting it, that is, apply security controls to known data, enumerate the unknown data, and monitor the creation of new data.

USE PPT TO PROTECT NEW DATA

Let's say you know where all your sensitive data is and are confident it's protected. Great! But what about the new data, including company confidential data, that's constantly being created? For that, you should undertake data threat modeling to understand what data potential attackers want and how they're going to get it. To prepare for such threats, you should apply the PPT process:

P

PROCESS

Process for identifying and handling new data

P

PEOPLE

People need to be aware of the process

T

TECHNOLOGY

Technology to automate as much of the process as possible

Using PPT can help ensure that your data security program includes new data, that individuals recognize the importance of following the process for protecting it, and that as much of the process as possible is automated to minimize the chances that individuals will tire of performing manual processes and leave sensitive data exposed.

FORMULATE CLASSIFICATION LEVELS

Classifying data according to its level of sensitivity is essential to protecting it and meeting compliance requirements. There are several schemes you can evaluate to decide which works best for your organization.

They include:

- Role-based
- Data-oriented
- Access or location-based
- Hybrid

This chart offers some guidelines on how to classify data according to security objective, potential impact of unauthorized disclosure, and the types and severity of the impact of disclosure on the organization.

Formulating Classification Levels

	POTENTIAL IMPACT		
Security Objective	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** 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. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Impact Area	Low	Medium	High
Functional Impact	No loss, but lost efficiency.	Critical services lost to select users.	Critical services lost to all users.
Privacy Breach	None or limited. 10 or less PII records.	100 or less PII records exposed.	More than 100 PII records exposed.
Proprietary Breach	No exposure or limited value.	Exposure of IP, but less than $250K.	Exposure of IP, more than $250K.
Integrity Loss	No or limited data loss or compromise.	Moderate data loss or compromise.	Significant data loss or compromise.
Recoverability Effort	Not recoverable, or regular effort.	Supplemented effort to recover.	Extended effort to recover

GET SERIOUS, GET SYSTEMATIC, GET PEACE OF MIND

An effective program for protecting your sensitive data doesn't happen by chance. Complying with a diverse set of regulations, identifying and classifying sensitive data, and safeguarding data entrusted to you by customers, partners and employees—all while ensuring you preserve the data access necessary for staff members to do their jobs—requires a coordinated, ongoing effort. It may seem like a daunting task at the outset, but if you follow the recommendations in this eBook, take it step by step, and employ the right people and technology, it's more easily doable than you may think. And the alternative—ignoring data protection and hoping nothing bad happens—makes no sense for any responsible organization.

ABOUT SENSITIVE DATA MANAGER FROM IDENTITY FINDER

In Sensitive Data Manager, Identity Finder® has developed the next generation technology for accurately identifying and classifying structured and unstructured sensitive data such as medical data, credit card and Social Secure numbers and even data that is unique to your organization. Sensitive Data Manager provides a four-part methodology for managing sensitive data through its lifecycle.

Discover

Classify

Monitor

Protect

ABOUT IDENTITY FINDER

Identity Finder®, headquartered in New York City, is the leading provider of enterprise data management software to help businesses reduce their sensitive data footprint and proactively minimize the risks, costs and reputational damage of successful cyberattacks.

Sensitive Data Manager® helps organizations avoid costly data breaches by discovering, classifying, monitoring and protecting personal information, medical records, credit card numbers, and intellectual property stored across the enterprise, within e-mail, and in the cloud.

Identity Finder specializes in the high-precision search and automated classification of unstructured data using its AnyFind® engine's unparalleled accuracy when analyzing human-generated text and images. Identity Finder has thousands of customers among leading firms in the healthcare, public sector, retail, education, financial services, energy, industrial, and entertainment markets.

Contact Us

Identity Finder, LLC
1776 Broadway; Suite 803
New York, NY 10019 USA
+1 (646) 863-8301
info@identityfinder.com
www.identityfinder.com

Connect Online