Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **September 2021**
Sponsored by **ActiveNav**

Sensitive Data Discovery Rises as a Top Concern for Organizations

Executive Summary

Sensitive data protection has quickly become the new normal with the inherent certainty of data breaches and the rise of state and international privacy regulations. Sensitive data must be protected against unauthorized access and disclosure, but to enforce the required protections, organizations first need the ability to discover where sensitive data is created and stored. This first mile causes challenges for many organizations as they try to run before they can walk.

In this white paper, we look at the challenge of sensitive data discovery and how organizations are prioritizing and assigning responsibility for it.

KEY TAKEAWAYS

- **Discovering sensitive data is a high priority**
  Almost 90% of respondents say discovering sensitive data is a high or medium priority in their organization.

- **Sensitive data is a higher priority in several industries**
  Organizations in three industries—healthcare/pharma, technology, and financial services—were more likely to say discovering sensitive data was a high priority.

- **Compliance, IT, and "Other" departments are the ones usually tasked with sensitive data protection**
  Most organizations see the departments in these three categories as responsible for managing sensitive data risk.

ABOUT THIS WHITE PAPER

Osterman Research conducted a primary market survey of 100 people in the United States with responsibility for managing the risks associated with sensitive data. Roles included CIOs (20% of respondents), CISOs (12%), COOs (11%), Chief Risk Officers (7%), and people in legal and privacy positions (5%).

The survey and this white paper were sponsored by ActiveNav. Details about the company are at the end of this paper.

Sensitive data protection has quickly become the new normal with the inherent certainty of data breaches and the rise of state and international privacy regulations.

Discovering Sensitive Data is a High Priority

Most organizations view discovering sensitive data as a high priority. In this section, we define sensitive data and look at the responses regarding discovery and mapping.

DEFINING SENSITIVE DATA

Sensitive data refers to data that cannot be shared freely with everyone because certain people, the organization, or privacy regulations require that it is protected for personal or legal reasons. Examples include (but are not limited to):

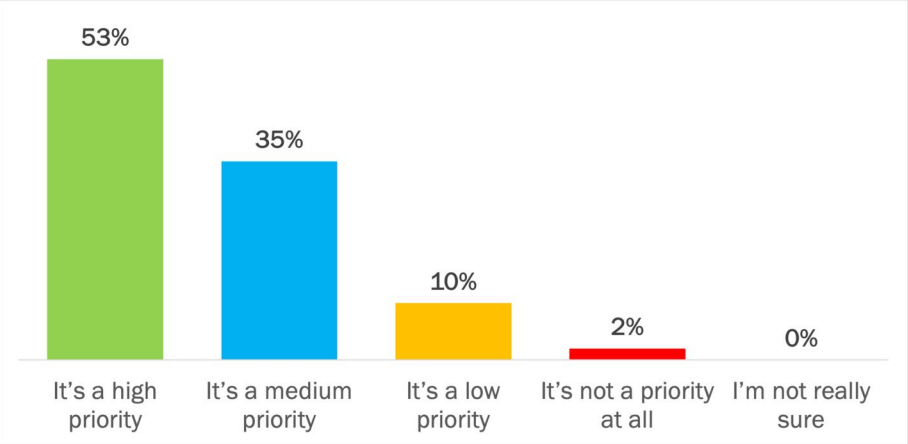
- The physical address and mobile phone numbers of a customer
- Sexual orientation of employees
- Business strategy documents
- Merger and acquisition targets
- Customer database

OVERALL PRIORITY FOR IDENTIFYING SENSITIVE DATA

Just under **nine out of 10 respondents say that discovering sensitive data is a high (53%) or medium (35%) priority in their organization.** Only 2% said it was not a priority at all, and no respondents said they were unclear on priority. See Figure 1.

Almost all organizations say discovering sensitive data is a significant priority.

Figure 1
Organizational Priority on Discovering Sensitive Data
Percentage of respondents



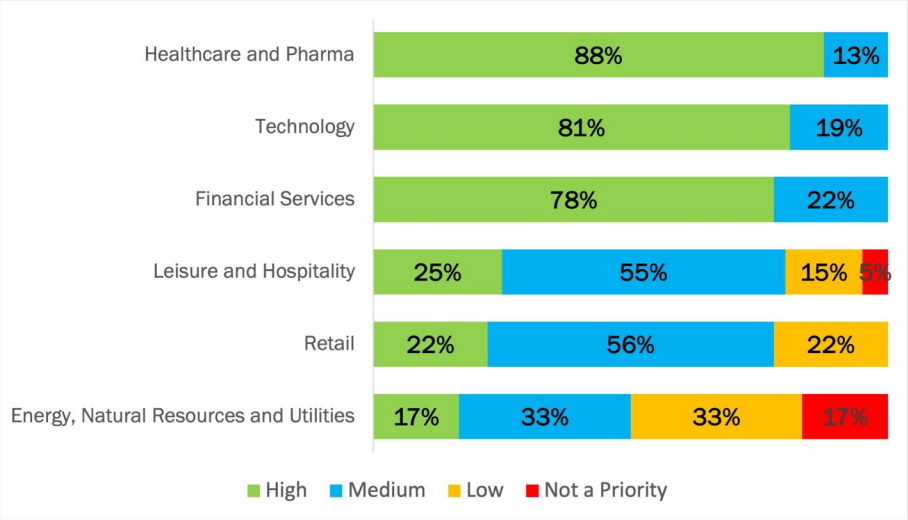
Source: Osterman Research (2021)

SENSITIVE DATA IS A HIGHER PRIORITY IN SEVERAL INDUSTRIES

Respondents in three industries—healthcare/pharma, technology, and financial services—were much more likely to say discovering sensitive data was a high priority (see Figure 2). Organizations in these industries often deal with large volumes of sensitive data and more stringent regulations:

- **Healthcare and pharma (88% high priority)**
  Sensitive data is stored in electronic health records and clinical trial findings for new drug development, along with the communication and discussion surrounding these. HIPAA regulations require strong protections for personal health information.
- **Technology (81% high priority)**
  Firms offering social media platforms, search engines, and marketing optimization, among others, hold vast troves of personal and sensitive data on users. Data is both generated by end users and asserted by algorithms.
- **Financial services (78% high priority)**
  Financial records, wealth planning, and other sensitive personal data is held in abundance by organizations in the financial services sector. Communications within firms—e.g., user-generated data—are heavily regulated.

Figure 2
Organizational Priority on Discovering Sensitive Data: By Industry
Percentage of respondents in six industries



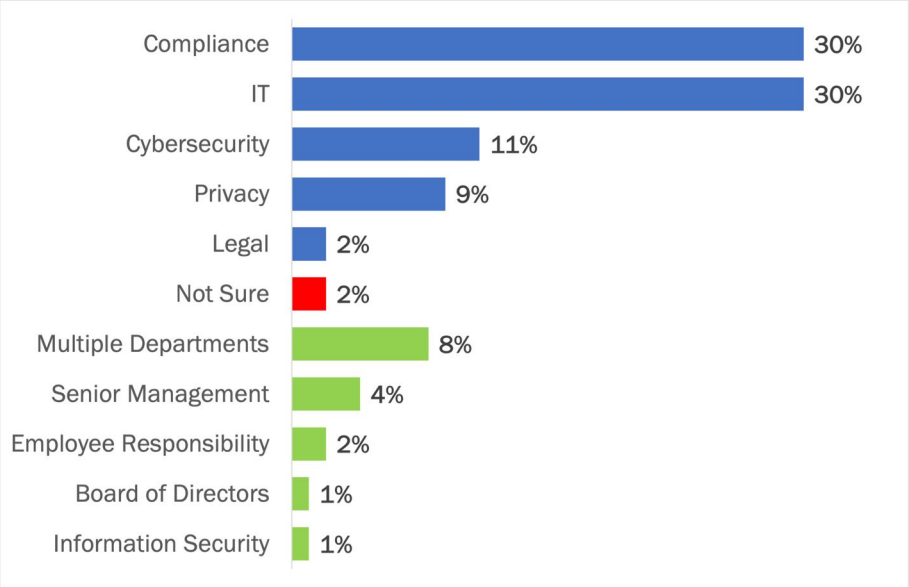
Source: Osterman Research (2021)

Respondents in three industries were much more likely to say discovering sensitive data was a high priority.

COMPLIANCE, IT, AND "OTHER" ARE RESPONSIBLE

Respondents indicated a diversity of responsibility for managing the risks with sensitive data in their organization. See Figure 3.

Figure 3
Department with the Primary Responsibility for Managing Sensitive Data Risk
Percentage of respondents



Source: Osterman Research (2021).

In looking at the data:

- **Compliance and IT departments**
  The compliance department (30%) and the IT department (30%) tied in first place among respondents for holding primary responsibility for managing sensitive data risk.
- **The "Other" category**
  In third place was the "Other" category (16% in combination), which is shown in Figure 3 as the five green bars. The common theme with the respondents who selected "Other" was that of joint ownership across multiple departments, or by all senior management, or that it was a responsibility for "each and every employee." If the positive side of joint ownership can be achieved, then the culture reinforces the need for protecting sensitive data. The risk, however, is that if "everyone" owns it, nobody actually does.

Most organizations see managing sensitive data risk as a responsibility for the compliance or IT department.

Summary and Next Actions

Discovering sensitive data wherever it is created or stored in organizations is a high priority, especially in the healthcare/pharma, technology, and financial services industries. Most organizations consider their Compliance, IT, or "Other" departments responsible for managing sensitive data risks.

To maintain compliance with the latest regulations and to protect themselves against the reality of data breaches, we recommend all organizations ensure they have solutions in place that cover the complete range of sensitive data.

Sponsored by ActiveNav

ActiveNav is a data privacy and governance software provider and innovator of DMaaS (Data Mapping as a Service). With ActiveNav, organizations can map, clean, classify, quarantine, and delete sensitive, redundant, obsolete, and trivial data. Hundreds of leading companies and government agencies trust ActiveNav to help them control sensitive data and support compliance with various data privacy regulations such as the CPRA, CCPA, and GDPR. ActiveNav Inc. is headquartered in the DC metro area and has offices in Europe and Australia.

For more information, please visit ActiveNav.com.

www.activenav.com

@ActiveNav

usa-sales@activenav.com

+1 571 375 2780