DATA RISK & PRIVACY SURVEY RESULTS

How Concerned are Organizations with Data Risk?

GUIDANCE SOFTWARE™

From beginning to endpoint.

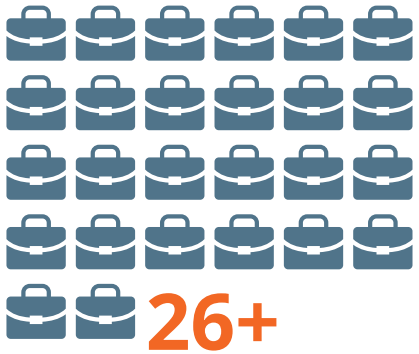
OVERVIEW

The exponential growth of data, and the parallel growth of private and sensitive information embedded within that data, presents unique challenges to organizations today. More restrictive worldwide data compliance mandates combined with recent changes to the U.S. Federal Rules of Civil Procedure (FRCP) all impact how organizations should recognize, manage, and execute their data governance policies. It is more important than ever to make data-driven decisions about the best strategy for managing information, rather than doing nothing as a result of 'fear.'

The notion of identifying and classifying sensitive data across the entire enterprise is an incredibly daunting proposition – especially in light of shadow IT, data sprawl, and other data-related challenges. In order to gain insight into the market drivers, pain points, and priorities related to data risk management, Guidance Software administered a data risk and privacy survey to regulatory compliance, information security, IT, legal, and risk management professionals across a variety of industries including government, technology, education, manufacturing, healthcare, and financial services. The survey, which concluded in January 2016, generated more than 580 responses.

guidancesoftware.com | experts@guid.com

580+ RESPONDENTS
ACROSS THE UNITED STATES



26+
Respondent Job Titles

SITUATION

PROTECTING SENSITIVE & PRIVATE DATA IS A TOP PRIORITY

There is hardly a lack of projects within any given organization. Often, there are hundreds, or even thousands, of competing projects. And priorities are usually measured against return on investment (ROI), regulatory mandates, strategic alignment, or customer demand.

Most respondents – 46% – identified 'sensitive data and privacy protection' as a top three initiative. This is not surprising since data privacy projects generally involve multiple considerations such as weighing the hard benefits (e.g., reducing surface area of risk, optimizing storage, mitigating risk of fines) and soft benefits (e.g., corporate responsibility, reputational integrity, customer confidence).

Government (19%), IT (15%), financial services (11%), and healthcare (10%) comprised the top five industries that consider data privacy protection initiatives as a high priority.

What is the

CURRENT PRIORITY

of your organization's sensitive data and privacy protection initiatives?

SITUATION

WHY **REGULATORY COMPLIANCE**

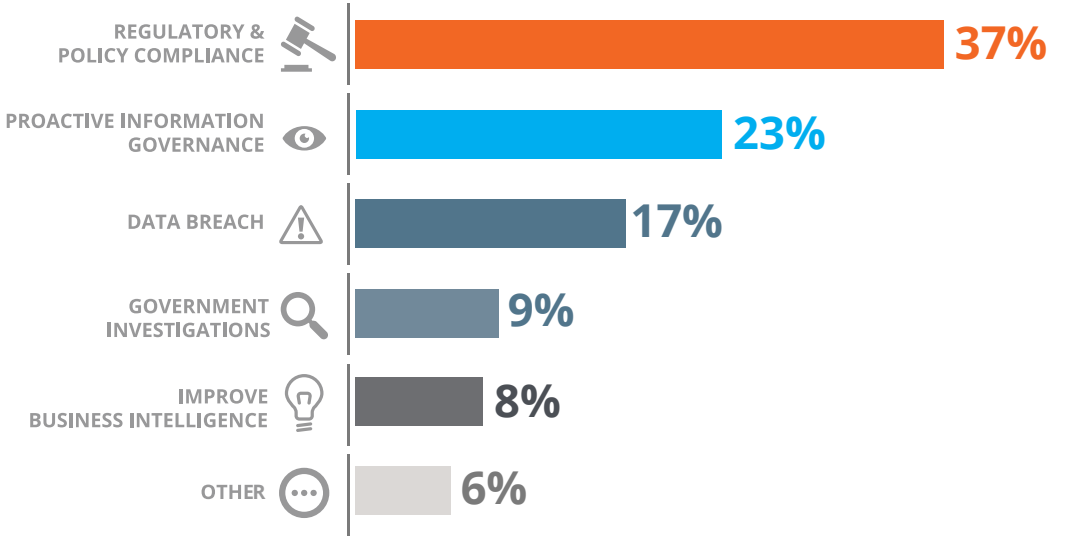
WHAT **CUSTOMER DATA**

Regulatory and policy compliance is a primary driver for adopting technology designed to manage sensitive or private data. The evolution and development of data governance policies to ensure compliance coupled with increasing risk of fines for regulatory violations have created a heightened sense of urgency related to sensitive data management. This is especially true among highly regulated industries with 38 percent of respondents in government, healthcare and financial services selecting regulatory and policy compliance as the main reason they have or will invest in a solution to manage sensitive or private data. Fourteen percent of individuals in the IT sector, which viewed information as central to their business, also listed compliance as a key factor.

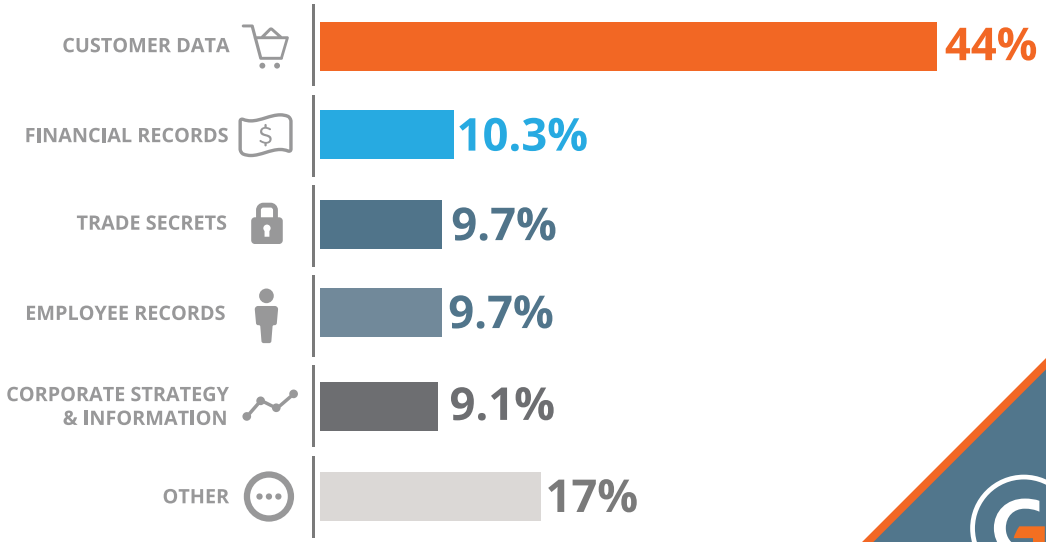
The overwhelming majority of respondents were mostly concerned about protecting customer data. Customers' increasing expectations for privacy, a greater emphasis on social expectations and more stringent regulatory mandates may result in greater focus on customer data.

guidancesoftware.com | experts@guid.com

What reasons have prompted you or will likely prompt you to invest in a solution to manage sensitive or private data?



What kind of Sensitive Data are you most concerned about protecting?



SITUATION

WHERE **SERVERS AND ENDPOINTS**

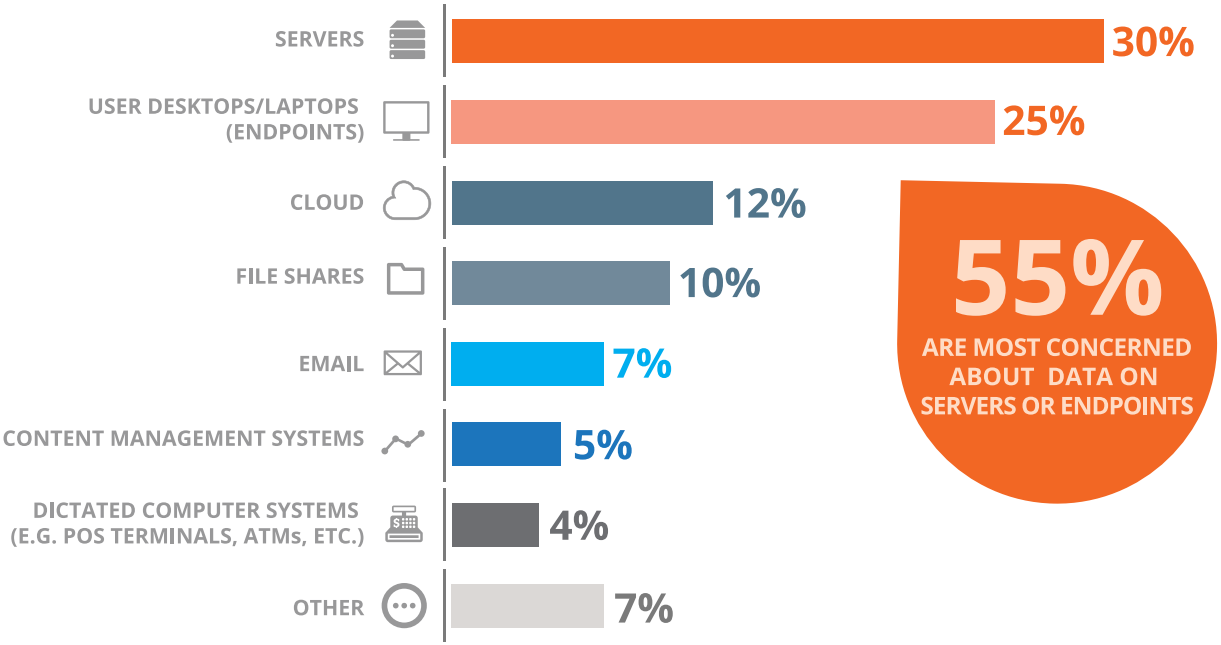
HOW **SYSTEMATICALLY**

Sensitive data can reside in a number of places, both known and unknown. If your organization is connected to the Internet, then your data is at risk. A common, and quite vulnerable, point of entry for malicious attacks is at the endpoint (e.g., desktops, laptops, workstations). One out of every four respondents were most concerned about protecting sensitive data on endpoints – more than twice the number who were concerned about file shares. The majority of respondents (around 55 percent) selected endpoints and servers.

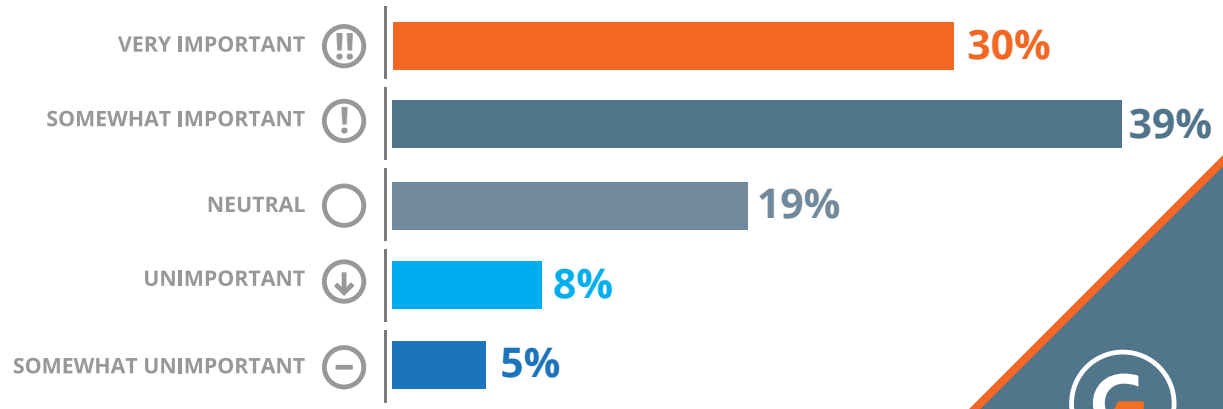
The proliferation of aged or stale data has further complicated the sensitive data landscape. The inability to effectively execute on data retention policies increases an organization's overall level of data-related risk. Poor data hygiene can also lead to operational inefficiencies, unnecessary storage costs, and improper business decisions. Approximately 69% of respondents agreed that the ability to systematically delete stale and obsolete data was important. Reasons for implementing automated remediation capabilities ranged from reducing storage (33%) and reducing the surface area of sensitive data (32%) to reducing the volume of discoverable content (19%).

guidancesoftware.com | experts@guid.com

Which of the following locations is your organization's highest concern for protecting sensitive data?



How important is the ability to systematically delete data that has become stale and has no business value?



CONCLUSION

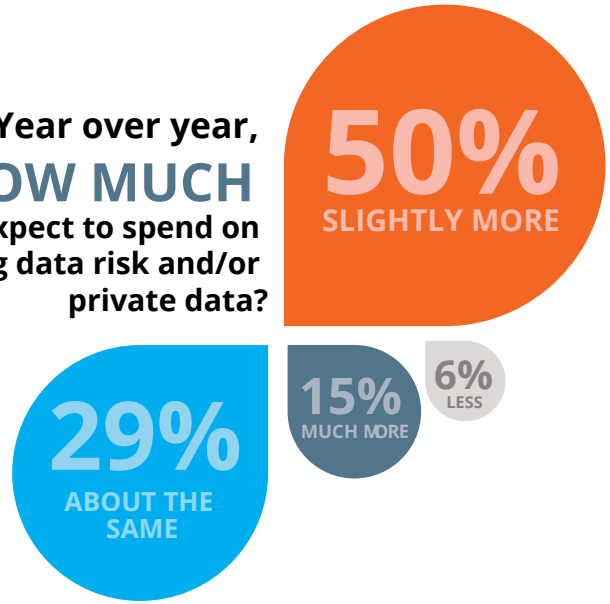
Our Data Risk & Privacy Survey revealed some interesting trends.

Nearly 52% of respondents claimed to use software designed to proactively identify, quantify, and remediate sensitive or private data. Without knowing more, we can assume this technology stems from one or more of the following categories: Governance Risk & Compliance (GRC), Data Loss & Prevention (DLP), Operational Risk Management, Data-Centric Audit and Protection (DCAP), or E-Discovery. Some of the functionality required for sensitive data management overlaps among these groups. Yet, none of the products within these categories can provide a single, purpose-built solution to proactively identify, classify, and remediate sensitive data across the entire enterprise - all endpoints, file shares, servers, cloud, and content repositories - without system dependencies.

We see a gap between perceived product capabilities and what is actually required to solve the private and sensitive data problems identified in this survey.

guidancesoftware.com | experts@guid.com

Year over year,
HOW MUCH
do you expect to spend on managing data risk and/or private data?



More than 60% of respondents claimed they did not have well-established organizational policies to address data privacy concerns (48% - currently being developed, 7% - does not exist, and 6% - not sure). This validates two ideas:

1. Technology is developing faster than the adoption of data governance policies; and
2. Organizations need technology to help them understand their sensitive data landscape (data about their data) to shape data governance policies.

IT IS CLEAR THAT PROTECTING SENSITIVE DATA IS A TOP PRIORITY,

and organizations are willing to invest budget in order to solve these real problems. Ninety-four percent of organizations are planning to spend the same amount or more, year-over-year, to manage data risk.

METHODOLOGY

ADMINISTERED BY GUIDANCE SOFTWARE, INC.

SURVEY BEGAN IN DECEMBER 2015 AND WAS COMPLETED IN JANUARY 2016.

584 RESPONDENTS FROM ACROSS VARIOUS JOB FUNCTIONS

Information Security (27%); Information Technology (25%); Regulatory Compliance (13%); Legal (7%); Internal Investigations (5%); Risk Management (5%); Records or Data Management (2%); Other (16%)

OVER 16 INDUSTRIES

Government, high tech/information technology, financial services, professional services, healthcare, education/academia, manufacturing, communications/telecommunications, insurance, aerospace and defense, transportation, non-profit, leisure and entertainment, retail/wholesale, utilities, oil and gas and other.

SIZE OF ORGANIZATIONS

1-50 (21%), 51-250 (14%), 251-1000 (17%),1001-3000 (14%), over 3001 (33%)

GUIDANCE SOFTWARE

ABOUT GUIDANCE

Guidance exists to turn chaos and the unknown into order and the known-so that companies and their customers can go about their daily lives as usual without worry or disruption, knowing their most valuable information is safe and secure. The makers of EnCase®, the gold standard in forensic security, Guidance provides a mission-critical foundation of market-leading applications that offer deep 360-degree visibility across all endpoints, devices and networks, allowing proactive identification and remediation of threats. From retail to financial institutions, our field-tested and court-proven solutions are deployed on an estimated 33 million endpoints at more than 70 of the Fortune 100 and hundreds of agencies worldwide, from beginning to endpoint.

guidancesoftware.com | experts@guid.com