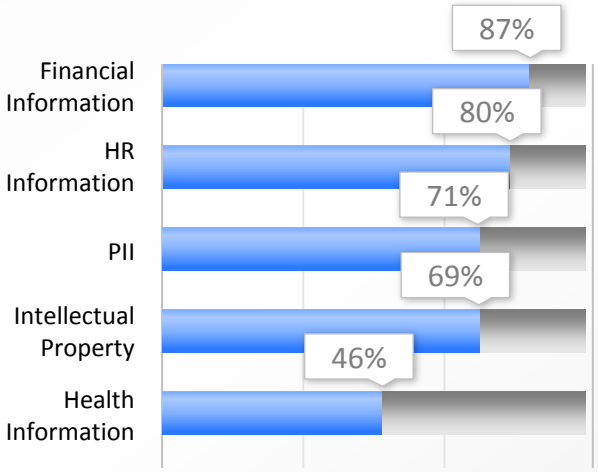
Take Control of SharePoint Security

Security and Data Governance Challenges and Recommendations

Has your SharePoint deployment "gone wild"? If so, you're not alone. Most organizations struggle with the huge volume of data being uploaded and shared in SharePoint. With powerful search capabilities that easily expose sensitive data, and no clear ownership or responsibility for that data, SharePoint presents a number of compliance and regulatory risks.

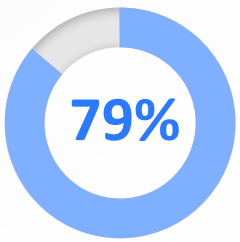
Sensitive Data

A recent TITUS survey showed that organizations are storing a wide variety of sensitive information in SharePoint.

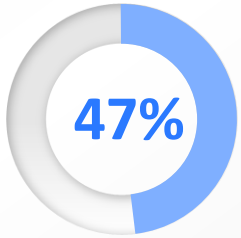


Top SharePoint Security Challenges

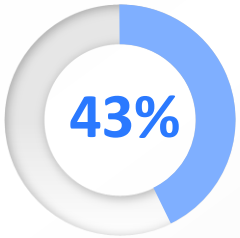
In the same survey, over 200 poll respondents shared their top SharePoint security challenges.



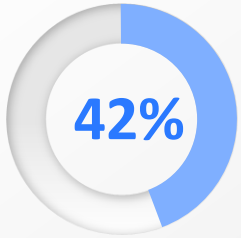
Permissions management and site ownership



Auditing for compliance



Secure external access (e.g. partners, contractors)



Controlling access to official corporate records

It's no surprise that permissions management is the greatest security challenge in SharePoint. While new SharePoint deployments often attempt to segregate sensitive content, most organizations quickly find that users prefer to store information based on topic, project, or group.

This raises some challenging issues: How do you know which information is sensitive? How do you know which users and groups should have access? How do you control access when content is dispersed across many libraries, lists, and sites?

SharePoint provides several features to control data access, including the ability to set permissions on sites, libraries, and documents. However, to support environments where sensitive data is stored alongside non-sensitive data, permissions must be assigned on a per-item basis. This is a manual process in SharePoint, and quickly becomes unmanageable in all but the smallest deployments.

A Different Approach

Automated, consistent security with metadata

With **TITUS Security Suite for SharePoint**, there is no need to manually define access rights for every document. Instead, permissions are applied automatically based on the document's metadata, such as sensitivity level, project code, or department. Permissions can also be applied based on the user's trusted attributes/claims, such as security clearance level or department.

User + **Metadata** = **Permissions**

The document's metadata can also be used to apply visual markings (headers, footers, watermarks) to identify document sensitivity. This promotes user awareness and accountability when handling sensitive information.

Key Benefits

TITUS Security Suite for SharePoint enables organizations to:

1. **Ensure the right people see the right information.** Support information sharing without putting your organization at risk.
2. **Safely store sensitive data alongside non-sensitive data.** Organize information by topic, project, or department – not by security level.
3. **Promote user awareness and accountability.** Automatically apply usernames, timestamps, and visual markings to downloaded documents.
4. **Automate security.** Use metadata and trusted user attributes (claims) to automatically control access to sensitive information.
5. **Ensure consistent and strong data governance.** Apply consistent security across all SharePoint content to support data governance and compliance initiatives.

TITUS Security Suite for SharePoint

TITUS Metadata Security for SharePoint protects sensitive information in SharePoint by enforcing access control policies that use document metadata and trusted user claims.

TITUS Document Policy Manager for SharePoint promotes awareness, compliance, and accountability by automatically applying visual markings and other document management policies.

WATCH → **VISIT** → **TRY**

Watch the webcast "Take Control of SharePoint Security"

Visit www.titus.com for more SharePoint security resources

Register for a free TITUS trial