Randy Franklin Smith's ULTIMATE WINDOWS SECURITY .COM ™

SharePoint: What's Going on Behind the Curtain?

- Made possible by both:
  - GFI EventsManager — Automated network-wide event log management
  - LOGbinder SP™

LOGbinder SP™
GFI EventsManager

Brought to you by

GFI EventsManager
http://www.gfi.com/eventsmanager

&

LOGbinder SP™
http://www.logbinder.com/products/logbindersp/

Speaker

- Randy Franklin Smith, Creator of LOGbinder
- Gill Langston, Sales Engineer Manager, Americas

LOGbinder SP™
GFI EventsManager

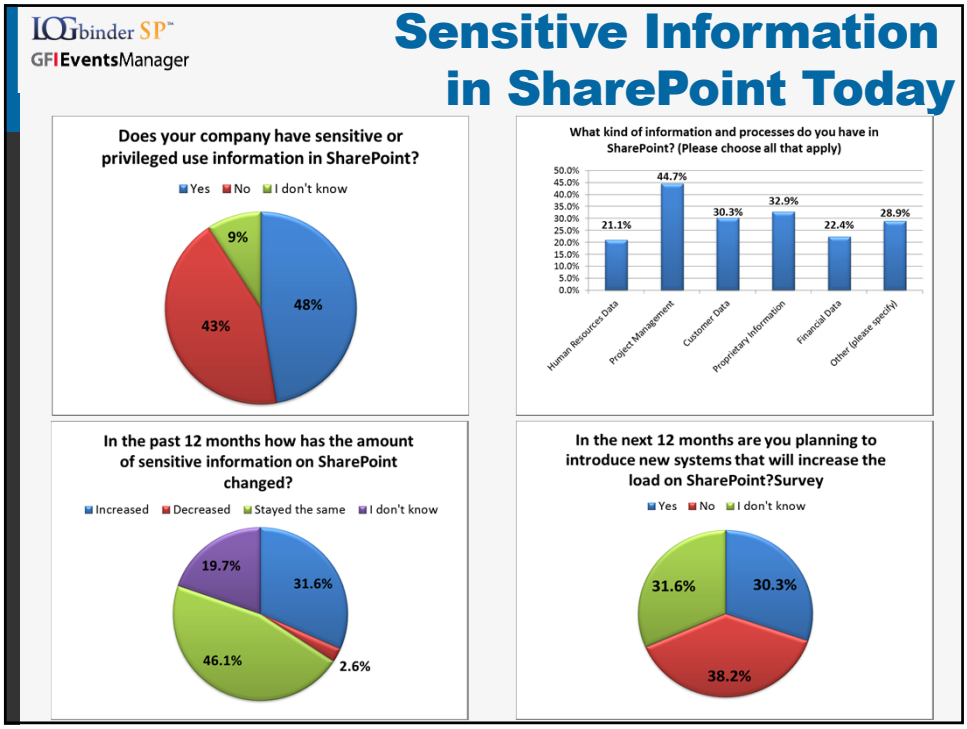
Preview of Key Points

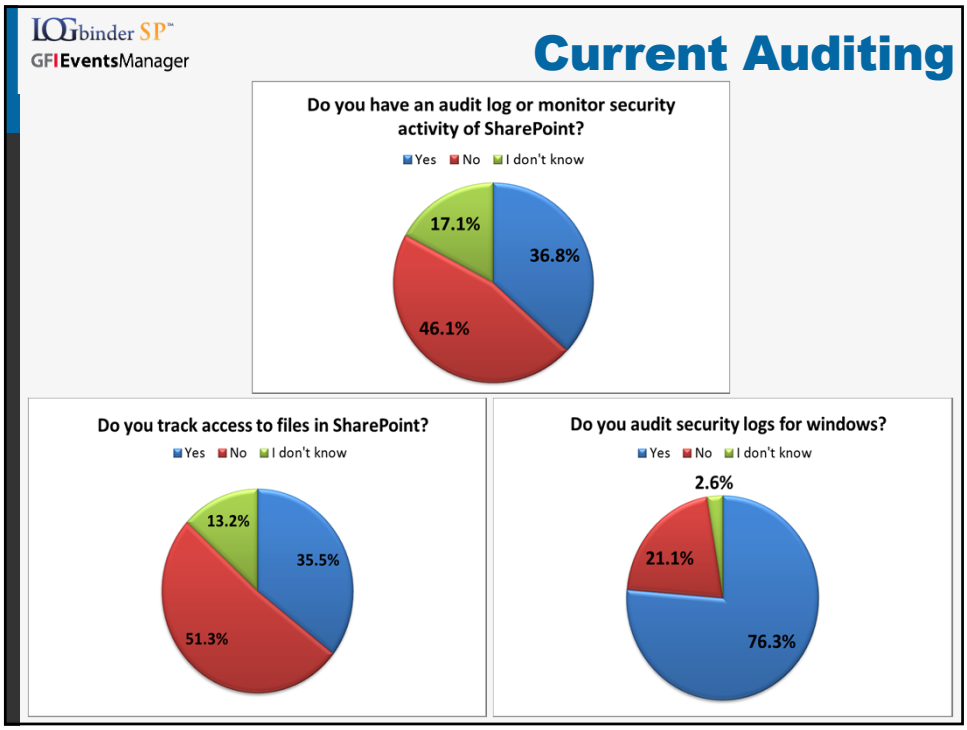
- Sensitive information in SharePoint today
- Risks of not auditing SharePoint
- Native SharePoint audit foundation
- Building on the foundation
  - LOGbinder SP
  - GFI EventsManager

LOGbinder SP™
GFI EventsManager

Sensitive information in SharePoint today

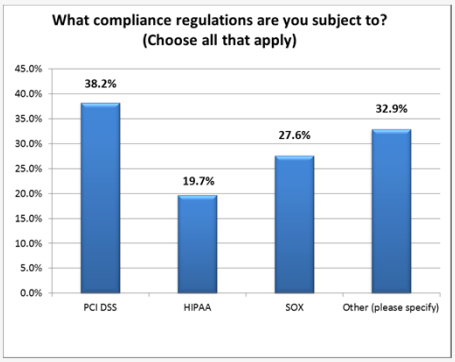
- Survey results
  - Sensitive information
  - Current auditing
  - Compliance

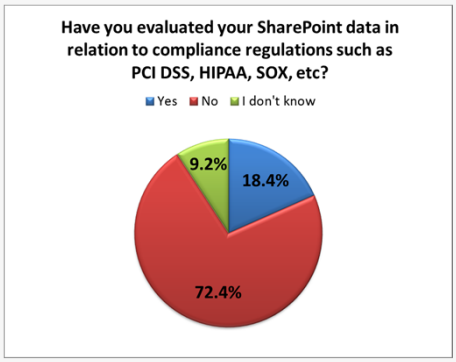




LOGbinder SP™
GFIEventsManager

Compliance





LOGbinder SP™
GFIEventsManager

Risks of not auditing SharePoint

- **Customer information disclosure**
  - Liability, notification costs, loss of good will
- **Trade secrets and intellectual property**
- **Human resources data**
- **Regulatory penalties and liability**
  - SOX
  - PCI
  - HIPAA
  - GLBA

LOGbinder SP™
GFIEventsManager

Native SharePoint audit foundation

- **Available in**
  - WSS 3.0
    - Not exposed in the interface
  - SharePoint 2007
  - SharePoint Foundation
    - Not exposed in the interface
  - SharePoint 2010

LOGbinder SP™
GFIEventsManager

Native SharePoint audit foundation

- **Audit policy defined at the site collection level**
  - Changes to audit policy
  - Permission changes
  - Group membership changes
  - View
  - Check in/out
  - Delete/Update
  - Schema changes
  - Workflow
  - Search

LOGbinder SP™
GFIEventsManager

Native SharePoint audit foundation

- **Audit records written to internal table within content database**
  - Inaccessible to log management solutions
  - Consumes expense SQL/SharePoint storage
  - Insecure to store audit logs on same system where they are generated
- **Rudimentary Excel reports available**
  - Audit codes, object ID numbers, user and group ID numbers not translated
    - Not readable or actionable
  - Criteria extremely limited
- **No alerting**
- **Audit log purging introduced with SP2010**
  - No archival capability

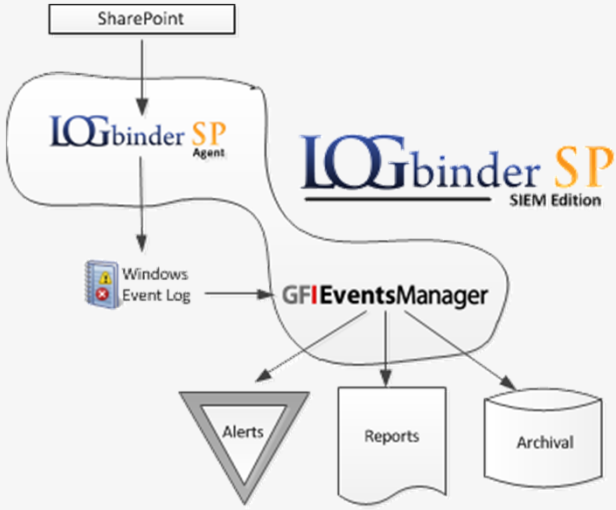
LOGbinder SP™
GFIEventsManager

Native SharePoint audit foundation

- **Limitations in WSS and Foundation**
  - Audit engine present but
    - Audit policy not exposed in the UI
    - No reporting
  - Auditing only possible through application that interfaces with SharePoint API

LOGbinder SP™
GFIEventsManager

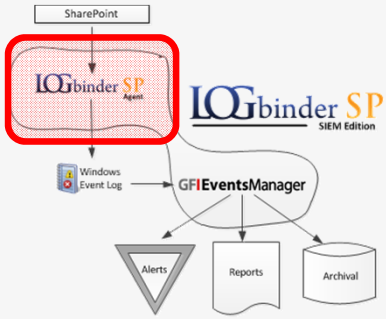
Building on the foundation



LOGbinder SP™
GFIEventsManager

Building on the foundation

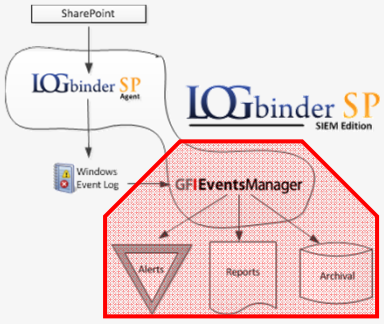
- **LOGbinder SP**
  - Translates SharePoint audit records into human readable audit trail
  - Sends SharePoint audit events to the Windows event log
  - Purges events after export



LOGbinder SP™
GFIEventsManager

Take action on the data

- **GFI EventsManager**
  - Secure log archival
    - Filter on specific fields in events
    - Assign different levels of importance to certain files/users
  - Alerting
    - Critical events can trigger email/SMS/Network message
    - Send alerts to responsible parties for event type
  - Reporting
    - Export events from Event Browser in HTML
    - Schedule reports daily, weekly, monthly



LOGbinder SP™
GFIEventsManager

Bottom Line

- **SharePoint increasingly used to store and process sensitive information**
- **Becoming an IT audit and compliance target**
- **Auditing, Alerting, Reporting is a must for any technology like SharePoint**
- **SharePoint native auditing is a foundation technology**
- **LOGbinder SP and GFI Events Manager build on that foundation to provide fully managed audit and security monitoring for SharePoint**