

Securing SharePoint 101

Rob Rachwald
Imperva



OWASP

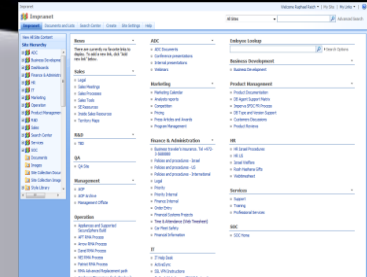
The Open Web Application Security Project

Major SharePoint Deployment Types



Internal Portal

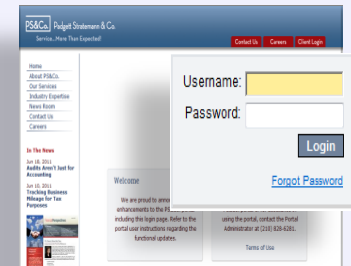
- Uses include SharePoint as a file repository
- Only accessible by internal users



Company Intranet

External Portal

- Uses include SharePoint as a file repository
- Accessible from the Internet
- For customers, partners or the public



Client access

Internet Website

- SharePoint as the Web site infrastructure
- Not used as a file repository



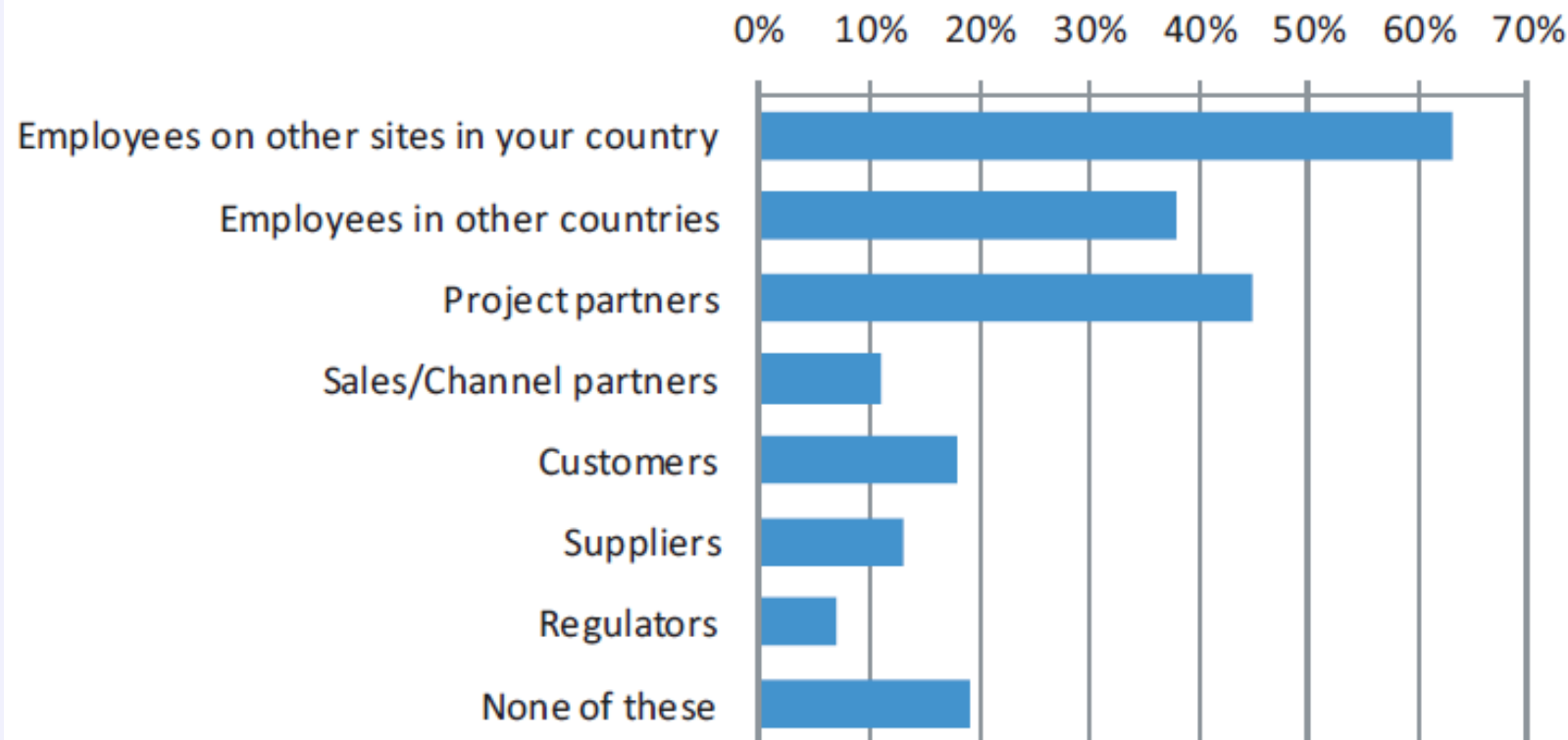
Public website



OWASP

The Open Web Application Security Project

Do you use SharePoint for collaboration with any of the following?



The SharePoint Footprint



← → ↻ www.wssdemo.com/livepivot/ 🔍 ⌵ ⌵ ⌵ ⌵ ⌵

Top SharePoint Internet Sites WSSDemo.com All Internet Sites 2010 Internet Sites SharePoint Books

Top SharePoint Internet Sites Sort Order: Industry ▾ 📊 📈 📉 +

Search here... 🔍

Industry

Sort Order: Quantity

- ☐ Government 326
- ☐ MS Certified Partners 223
- ☐ Education 212
- ☐ Industrial 208
- ☐ Health 194
- ☐ Financial 179
- ☐ Technology 171
- ☐ Professional Services 143
- ☐ Charity/Club/Community 123
- ☐ Retail 91
- ☐ Transportation 89
- ☐ Professional Association 88
- ☐ Entertainment 78
- ☐ Utilities and Energy 77
- ☐ Other 63
- ☐ Tourism 63
- ☐ Education - School District 53
- ☐ Education - University 51
- ☐ Food and Beverage 42
- ☐ Telecommunications 15

Country

Platform

Rating

Created

SharePoint Sidesteps IT—and Security



OWASP

The Open Web Application Security Project

“Much of SharePoint's appeal is that it enables users to bypass the explicit and organizational and process barriers of the organization.”

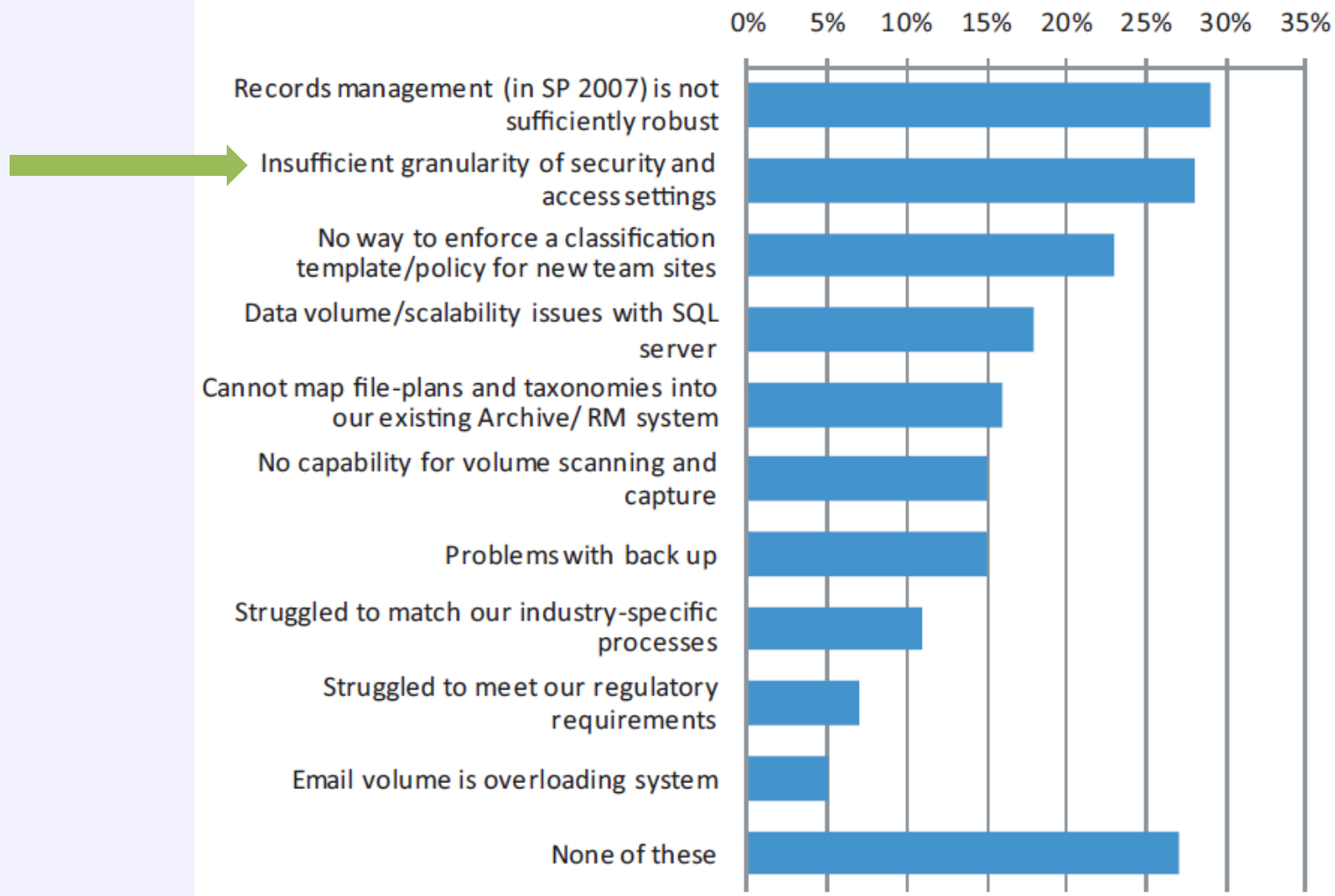
—Gartner, 2009

Key Issues With SharePoint



OWASP

The Open Web Application Security Project

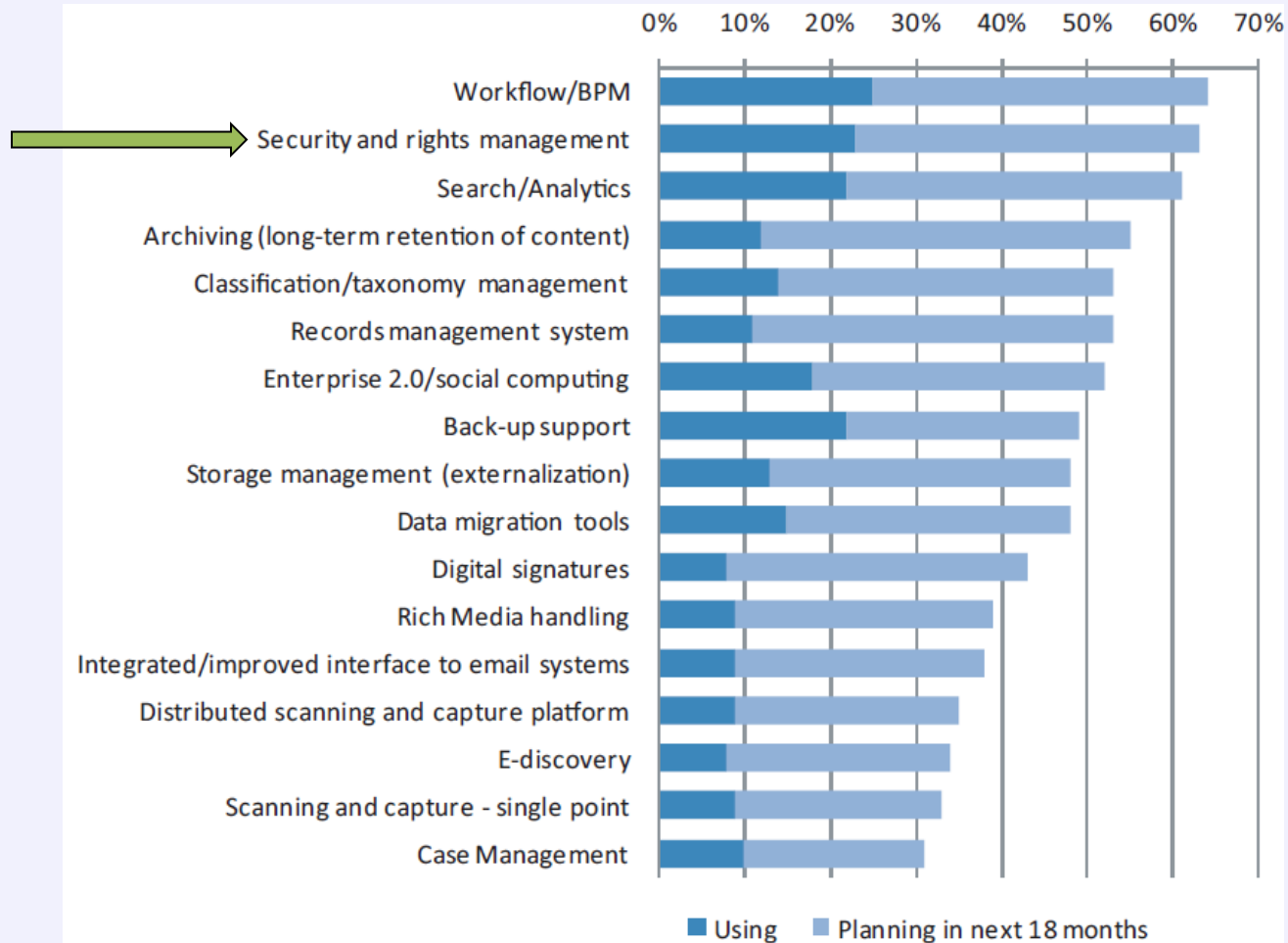


Third-Party Additions



OWASP

The Open Web Application Security Project



SharePoint Admins Gone Wild



OWASP

The Open Web Application Security Project

The Register[®]

SharePoint gods peek into colleagues' info – poll

Security is for other people

By **Gavin Clarke** • [Get more from this author](#)

Posted in [Software](#), 23rd January 2012 13:22 GMT

[Free whitepaper – Reshaping IT](#)

SharePoint admins are abusing their privileged status to sneak a peak at classified documents according to a poll that shows consistent abuse of security in Microsoft's business collaboration server.

A third of IT administrators or somebody they know with admin rights have read documents hosted in Microsoft's collaboration server that they are not meant to read.

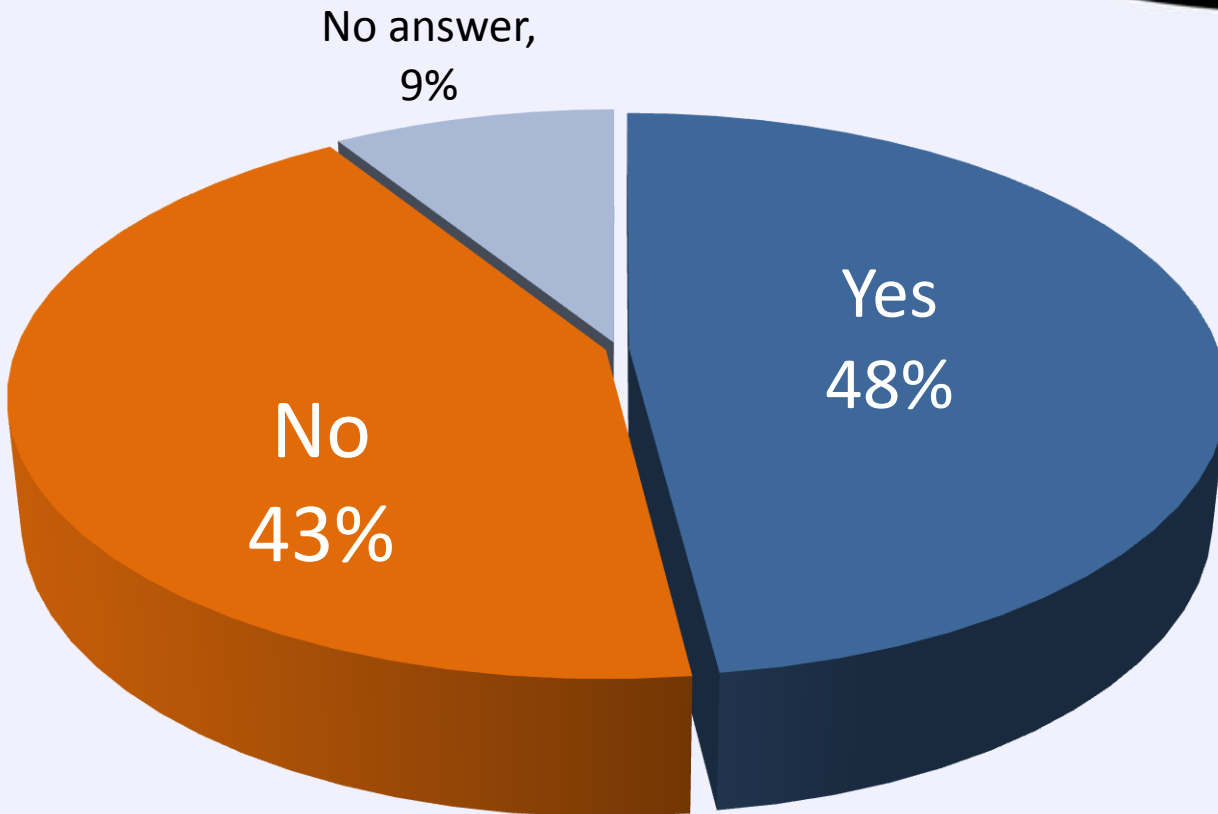
Most popular documents eyeballed were those containing the details of their fellow employees, 34 per cent, followed by salary – 23 per cent – and 30 per cent said "other."

Have Your Shared Privileged Info via SharePoint?



OWASP

The Open Web Application Security Project

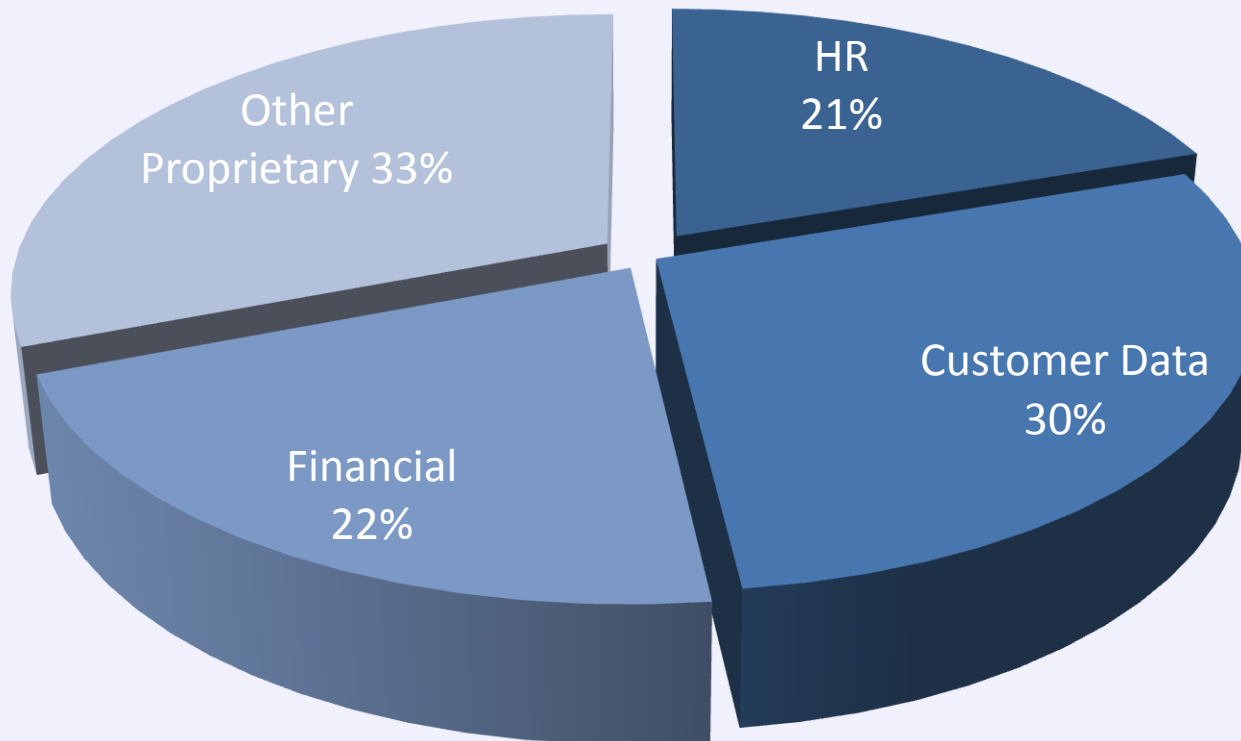


Type of Content Shared



OWASP

The Open Web Application Security Project



Impact of SharePoint Insecurity



OWASP

The Open Web Application Security Project

“[Investor]
Manning’s
SharePoint
He ran the
then down
publish



cripts on
Microsoft
ocuments.
cuments,
eaks had
same.”

SharePoint Security Capabilities: 2007 vs 2010



OWASP

The Open Web Application Security Project

2007

- Encryption
- Authentication
- Permissions

2010

- Encryption
- Authentication
- Permissions
- Some policy management
- Metadata tagging
- Versioning
- Workflow
- Info rights management



OWASP

The Open Web Application Security Project

- **Functionality**
 - Proper auditing
 - Web-based protection
 - Security-centric reporting
 - Security-centric policies
- **Bottom line**
 - SharePoint is built for collaboration first.
 - Features may provide security, but aren't inherent security tools
 - Did you know?
 - SSL is NOT turned on by default for downloading.
 - Remote binary large object (BLOB) storage does not coordinate underlying storage permissions with its own access control lists.



“In general, SharePoint involves a complex set of interactions that makes it difficult for security teams to know if all their concerns are covered.”

—Burton Group, 2010

Key SharePoint Security Issues

#1: Getting Permissions Right



OWASP

The Open Web Application Security Project

- Summary:
 - Microsoft's advice begins with permissions
 - "Content should not be available to all users... information should be accessible on a need-to-know basis"
- Why challenging?
 - Difficult to track and maintain
 - Constantly change
 - No automation or aggregation
- What is Required?
 - Automated permissions review tools
 - Baseline and change reports
 - Simplify rights reviews
- Example: If a hospital uses SharePoint for patient data and the system is managed by hospital staff, then who keeps track of which doctors, nurses, or administrators can see patient data? Further, who maintains and updates these permissions over time? How are they able to do what they do? How do you identify excessive or dormant rights?

SharePoint Access Controls



OWASP

The Open Web Application Security Project

Permissions: Home - Windows Internet Explorer

http://192.168.77.79/_layouts/user.aspx

File Edit View Favorites Tools Help

Share Browser WebEx

Favorites Imperva stuff Technology DEMO GEAR Mifi

Permissions: Home

Site Actions Browse

Permission Tools

Edit

Grant Permissions Create Group Edit User Permissions Remove User Permissions Check Permissions

Grant Modify Check Manage

Permission Levels Site Collection Administrators

	Name	Type	Permission Levels
<input type="checkbox"/>	Alfred LOPEZ (DARK\ALOPEZ)	User	Full Control
<input type="checkbox"/>	Bobby R. Hernandez (DARK\bhernandez)	User	Full Control
<input type="checkbox"/>	Chester COX (DARK\ccox)	User	Full Control
<input type="checkbox"/>	Cosmo Romero Admin Account (DARK\cromeroadmin)	User	Full Control
<input type="checkbox"/>	DARK\Administrator (DARK\administrator)	User	Limited Access
<input type="checkbox"/>	Home Members	SharePoint Group	Contribute
<input type="checkbox"/>	Home Owners	SharePoint Group	Full Control
<input type="checkbox"/>	Home Visitors	SharePoint Group	Read
<input type="checkbox"/>	Ian Shiff (DARK\shiff)	User	Full Control
<input type="checkbox"/>	Melissa Warwick (DARK\mwarwick)	User	Full Control
<input type="checkbox"/>	Neil R. Hunt (DARK\nhunt)	User	Full Control
<input type="checkbox"/>	RequestedAccess	SharePoint Group	Full Control
<input type="checkbox"/>	SharePoint Users	SharePoint Group	Read

Libraries

Site Pages

Shared Documents

Lists

Calendar

Tasks

Discussions

Team Discussion

Recycle Bin

All Site Content

Basic Elements: User Rights Management



- Aggregate user rights across systems
- Identify data owners
- Detect excessive rights, reduce access to business-need-to-know
- Formalize and automate approval cycle



Finding Excessive Permissions



OWASP

The Open Web Application Security Project

Focus on access to HIPAA regulated data

What departments have access?

Why does G&A have access?

Who are the users?
What type of access do they have?

How did they get the access?

Edward WILSON (USER) → Office Administrators (AD GROUP) → G&A (AD GROUP) → Medical Records.xls (File)

Automatic Identification of Excessive Rights



OWASP

The Open Web Application Security Project

Bad Practices

81 [Dormant Users](#)

381 [Unused files](#)

1 Files Accessible by [Global Groups](#) (everyone)

4 Permissions [Directly Assigned to Users](#) Who Are Not Owners

Should “Everyone” have access to sensitive data?

- “Everyone” group literally means all users

Are there any direct user permissions?

Account Name ▲	Account Department ▼	Permission ▼	Type ▼	Full Path ▲	File Owner ▼	Data Types ▼	Last activity (from audit) ▼
Albert HARRIS	HR	Read	Library	Finance/Budgets	Chester COX	Financial Data	09/02/2011 12:00:00 AM
Arthur JACKSON	HR	Read	Library	Finance/Budgets	Chester COX	Financial Data	
Daniel REED	Finance	Read	Library	Finance/Budgets	Chester COX	Financial Data	09/02/2011 12:00:00 AM
Edward WILSON	G&A	Read	Library	Finance/Budgets	Chester COX	Financial Data	
Eugene EVANS	Finance	Read	Library	Finance/Budgets	Chester COX	Financial Data	
Floyd EDWARDS	Finance	Read	Library	Finance/Budgets	Chester COX	Financial Data	
Harold WHITE	HR	Read	Library	Finance/Budgets	Chester COX	Financial Data	09/02/2011 12:00:00 AM

What rights are not used?

- Users with access they appear not to need

Identifying Dormant Users



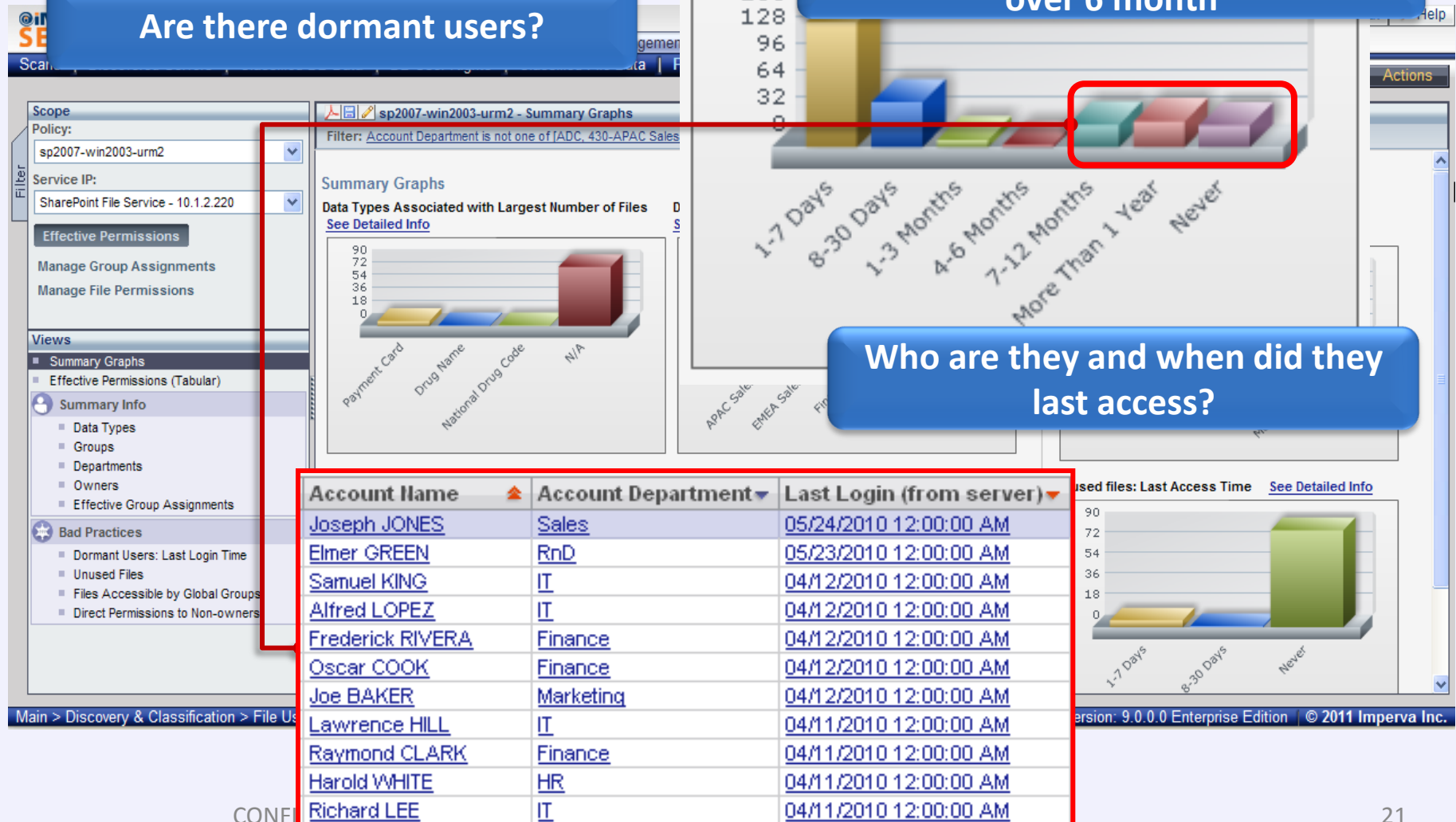
OWASP

The Open Web Application Security Project

Are there dormant users?

Focus on users that are dormant for over 6 month

Who are they and when did they last access?



Reviewing User Rights with Data Owners



The Open Web Application Security Project



Create permission reports for data owners

Grantee Type	Grantee Name	Permission	Full Path	File Owner	Data Types
User	Administrator	Change Permissions	Finance	Chester COX	Financial Data
User	Administrator	Create	Finance	Chester COX	Financial Data
User	Administrator	Delete	Finance	Chester COX	Financial Data
User	Administrator	Read	Finance	Chester COX	Financial Data
User	Administrator	Write	Finance	Chester COX	Financial Data

Select Columns | Page 1 of 1 | Showing records 1-20 out of 20 available

 Approve
 Reject
 Review
 Users

Status	Grantee Type	Grantee Name	Permission	Full Path	File Owner	Data Types	Status Change Date
✓ Approved	User	Administrator	Change Permissions	Finance/Budgets	Chester COX	Financial Data	09/09/2011 11:14:40 AM
🔍 In Review	User	Administrator	Change Permissions	Finance/Budgets	Chester COX	Financial Data	09/09/2011 11:14:21 AM
✓ Approved	User	Administrator	Change Permissions	Finance/Budgets	Chester COX	Financial Data	09/09/2011 11:14:40 AM
✓ Approved	User	Administrator	Change Permissions	Finance/Budgets	Chester COX	Financial Data	09/09/2011 11:14:40 AM
🔍 In Review	User	Administrator	Change Permissions	Finance/Budgets	Chester COX	Financial Data	09/09/2011 11:14:21 AM
Unmanaged	AD Group	Finance	Create	Finance/Budgets	Chester COX	Financial Data	
Unmanaged	AD Group	Finance	Delete	Finance/Budgets	Chester COX	Financial Data	
Unmanaged	AD Group	Finance	Read	Finance/Budgets	Chester COX	Financial Data	
Unmanaged	AD Group	Finance	Write	Finance/Budgets	Chester COX	Financial Data	
🚫 Reject	AD Group	Finance	Change Permissions	Finance/Budgets	Chester COX	Financial Data	09/09/2011 11:13:57 AM
✓ Approved	SP Group	Home/Home Members	Read	Finance/Budgets	Chester COX	Financial Data	09/09/2011 11:14:10 AM
✓ Approved	SP Group	Home/Home Members	Write	Finance/Budgets	Chester COX	Financial Data	09/09/2011 11:14:10 AM
✓ Approved	SP Group	Home/Home Owners	Change Permissions	Finance/Budgets	Chester COX	Financial Data	09/09/2011 11:14:10 AM
✓ Approved	SP Group	Home/Home Owners	Create	Finance/Budgets	Chester COX	Financial Data	09/09/2011 11:14:10 AM
✓ Approved	SP Group	Home/Home Owners	Delete	Finance/Budgets	Chester COX	Financial Data	09/09/2011 11:14:10 AM
✓ Approved	SP Group	Home/Home Owners	Read	Finance/Budgets	Chester COX	Financial Data	09/09/2011 11:14:10 AM
✓ Approved	SP Group	Home/Home Owners	Write	Finance/Budgets	Chester COX	Financial Data	09/09/2011 11:14:10 AM
✓ Approved	SP Group	Home/Home Visitors	Read	Finance/Budgets	Chester COX	Financial Data	09/09/2011 11:14:10 AM

Allow data owners to manage their permissions

Create a baseline: review only changed permissions

Log decisions for future audit

#2: Automate Compliance Reporting



- Summary:
 - SharePoint makes collaboration and document storage easy
 - If you store business data, you must be able to demonstrate compliance with regulations and mandates
- Why challenging?
 - Manual process – minimal inherent data audit capability
 - Native audit trail is not usable/readable
- What is Required?
 - Automated, human-readable activity auditing and reporting
 - Blended with enrichment data to simplify compliance process
- Example: In August 2011, Bloomberg reported on 300,000 healthcare records that appeared in an Excel file. No one knows where the file came from, indicating a lack of auditing.



Site Id	Item Id	Item Type	User Id	Document Location	Occurred (GMT)	Event	Event Data
98625596-3626-4005-83171f424dd-6697-4d3a-8		Folder	IL\moshe <IL\Moshe>	tsvikalib/testDocSet	2011-06-22T13:20:01	Update	<Version><Major>1</Major><Minor>0</Minor></Version> <url>tsvikalib/testDocSet</url><scope>518B480E-3D18-422D62E7DE67</scope>
98625596-3626-4005-83171f424dd-6697-4d3a-8		Site	IL\moshe <IL\Moshe>	tsvikalib/testDocSet	2011-06-22T13:20:50	Security Role Bind Break Inhe	464B-B376-422D62E7DE67</scope> <roleid>1073741829</roleid><principalid>16</principalid><scope>518B480E-3D18-464B-B376-422D62E7DE67</scope><operation>ensure added</operation>
98625596-3626-4005-83171f424dd-6697-4d3a-8		Site	IL\moshe <IL\Moshe>	tsvikalib/testDocSet	2011-06-22T13:21:09	Security Role Bind Update	added</operation>

Basic Elements: Access Auditing and Alerting



OWASP

The Open Web Application Security Project

- Full audit trail
 - Audit all access activity
 - No performance impact
- Analytics and reporting
 - Automatic reports to data owners
 - Forensics for incidents
 - Compliance reporting

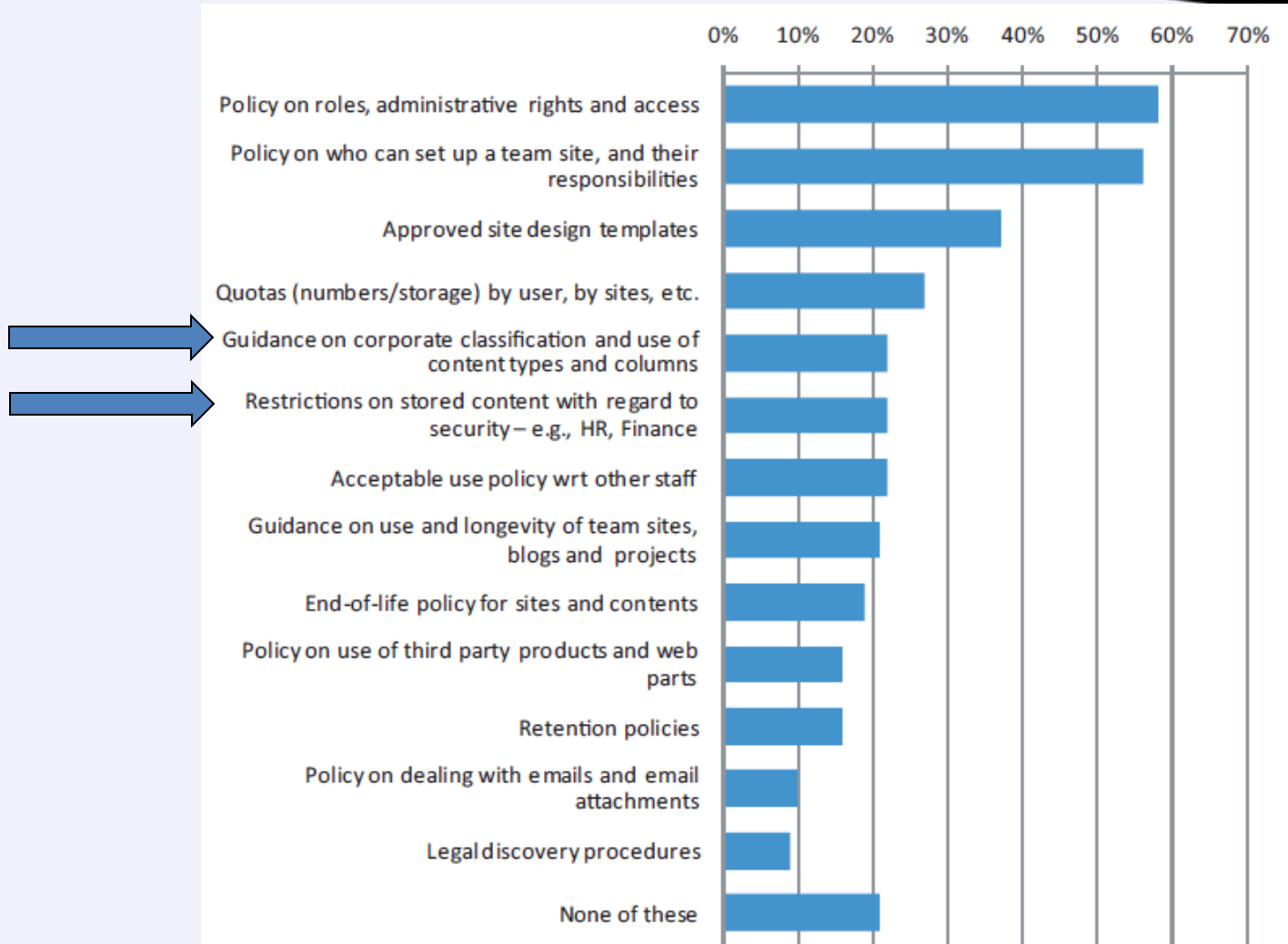


Governance Policies in Place



OWASP

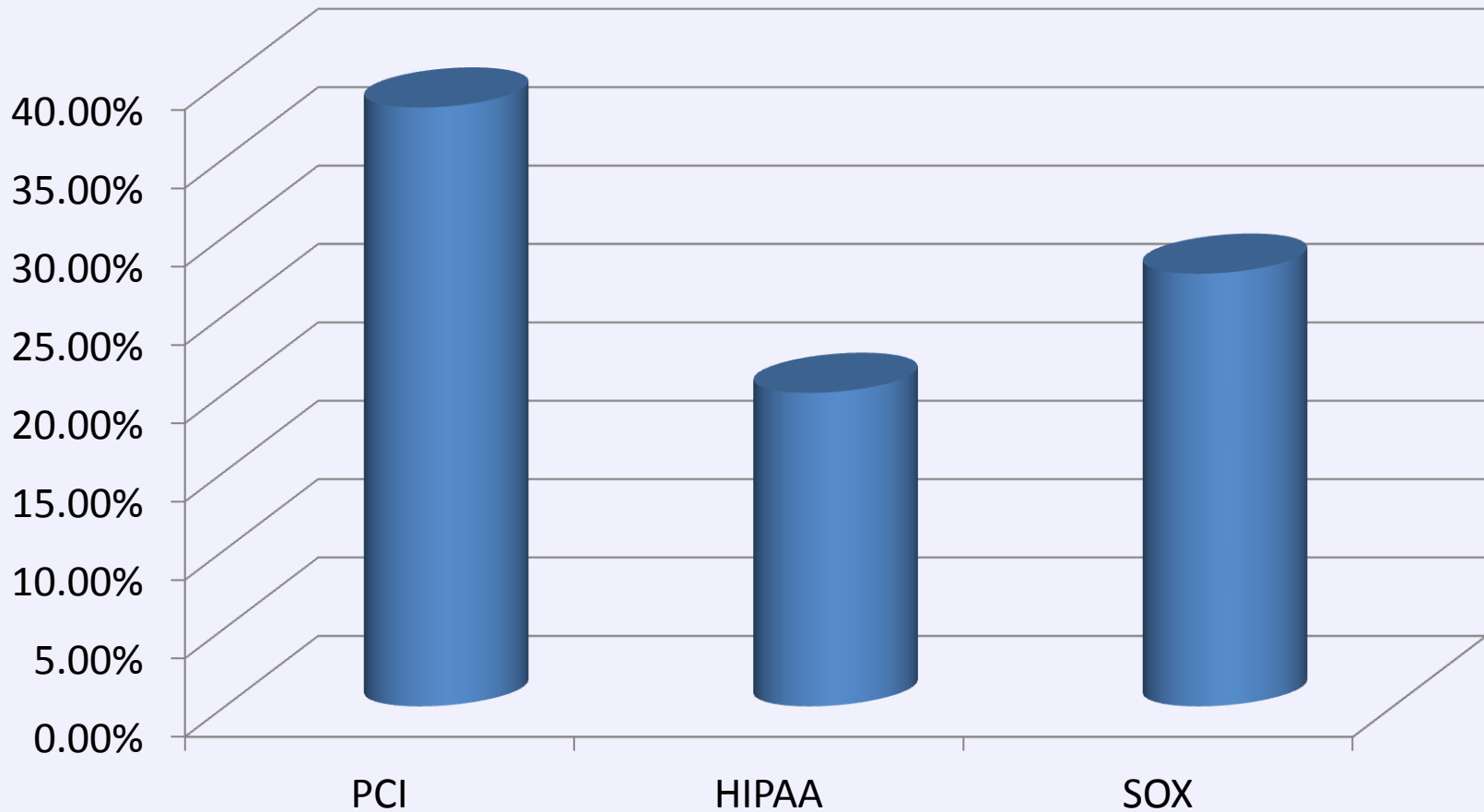
The Open Web Application Security Project

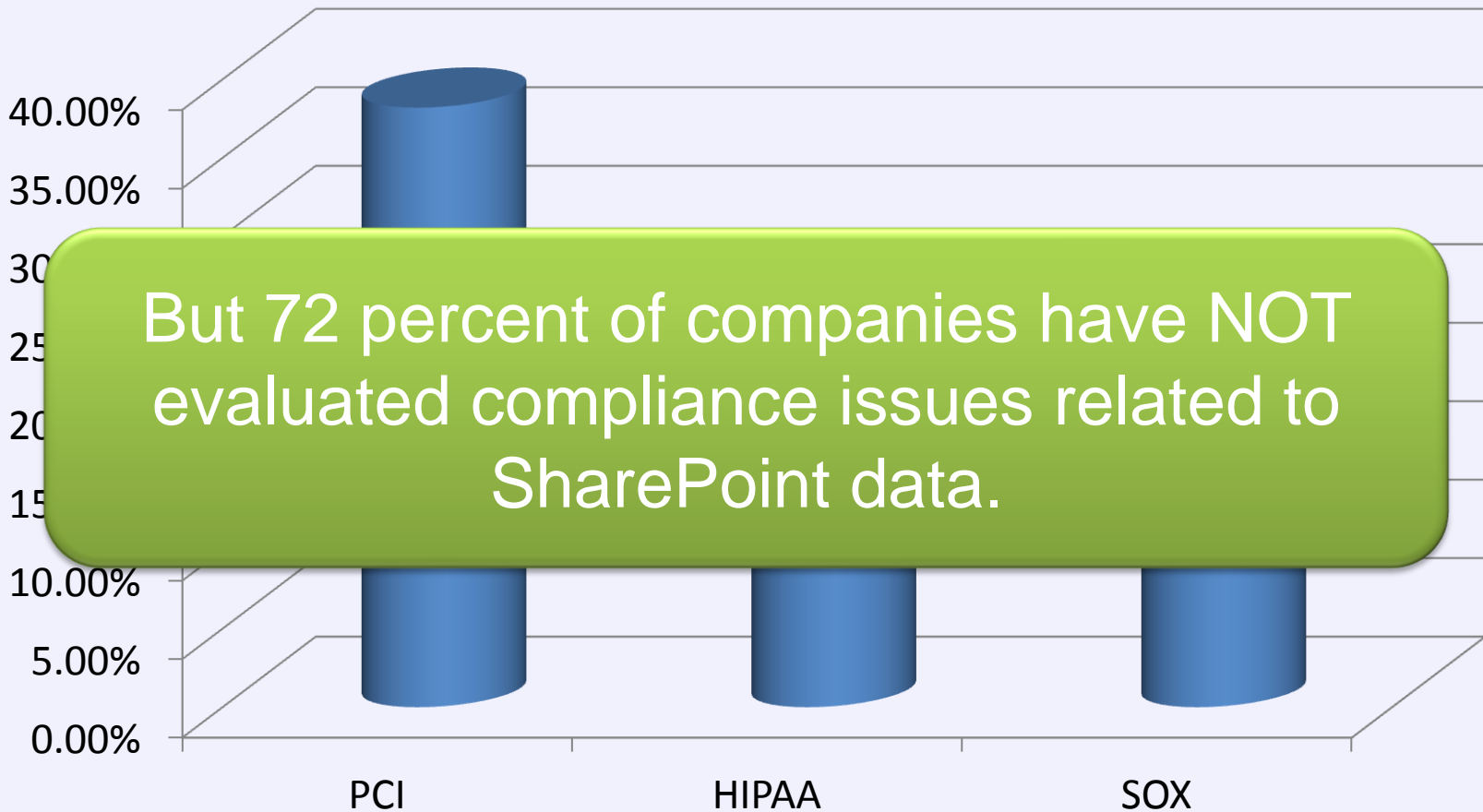




OWASP

The Open Web Application Security Project







Full Audit Trail



The Open Web Application Security Project

Discovery & Classification Setup Profile Risk Management Policies **Audit** Reports Monitor ThreatRadar

[Main](#)
[Admin](#)
[Preferences](#)
[Tasks](#)
[✕ Log out](#)
[? Help](#)

Activate Save As Actions

What

Event Date and Time ▲	User Name ▼	User Department ▼	Operation ▼	Full Path ▼	Data Type ▼
September 2, 2011 5:01:48 AM	administrator		Read	Finance/Teams/Forms	Financial Data
September 2, 2011 5:02:49 AM	administrator		Read	Finance/Teams/Forms	Financial Data
September 2, 2011 5:03:51 AM	ccox	Finance	Read	Finance/Teams/Payable	Financial Data
September 2, 2011 5:06:55 AM	system		Read	Finance/Teams/Payable	Financial Data
September 2, 2011 5:08:56 AM	ccox	Finance	Read	Finance/Management Documents	Financial Data
September 2, 2011 5:08:56 AM	ccox	Finance	Read	Finance/Management Documents/Committees.rtf	Financial Data
September 2, 2011 5:12:58 AM	AHARRIS	HR	Read	HR/Benefits	HR Data
September 2, 2011 5:12:58 AM	AHARRIS	HR	Read	HR/Benefits/Forms	HR Data
September 2, 2011 5:12:58 AM	AHARRIS	HR	Read	HR/Benefits/HR Budget.doc	HR Data

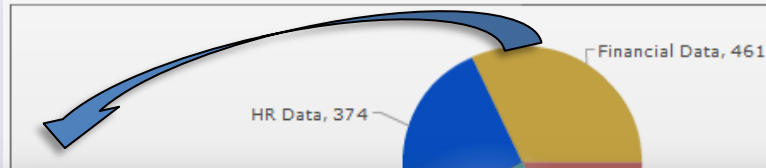
- | system | | | | | | | | |
|---------------|-----------|--------|--------------------------|------------------------------|----------------|-------------|-------------------------|-------------------------|
| RDAVIS | Sales | Read | Customers | Sales/Inside Sales | Sales Data | 3 | SharePoint File Service | |
| DREED | Finance | Modify | Lexicality - 2003b.xlsx | Sales/Inside Sales/Customers | Sales Data | 3 | SharePoint File Service | |
| DREED | Finance | Read | Forms | Finance/Teams | Financial Data | 3 | SharePoint File Service | |
| RDAVIS | Sales | Read | Customers | Sales/Inside Sales | Sales Data | 3 | SharePoint File Service | |
| DREED | Finance | Read | Committees.rtf | Finance/Management Documents | Financial Data | 3 | SharePoint File Service | |
| AHARRIS | HR | Create | Bob Lash - new.docx | HR/Resumes | HR Data | 2 | SharePoint File Service | |
| AHARRIS | HR | Modify | Wage Type.xls | HR/Benefits | HR Data | 2 | SharePoint File Service | |
| JCARTER | Marketing | Read | Calendar | Lists | N/A | 2 | SharePoint File Service | |
| administrator | | Read | Forms | Sales/Inside Sales | Sales Data | 2 | SharePoint File Service | |
| administrator | | Read | Forms | Finance/Shared Documents | Financial Data | Chester COX | 2 | SharePoint File Service |
| administrator | | Read | Management Documents | Finance | Financial Data | | 2 | SharePoint File Service |
| administrator | | Read | Risk Burndown - FY07.xls | Finance/Management Documents | Financial Data | | 2 | SharePoint File Service |
| | | | | HR/Resumes | HR Data | | 2 | SharePoint File Service |
| | | | | HR/Benefits | HR Data | | 2 | SharePoint File Service |
| | | | | HR/Benefits | HR Data | | 2 | SharePoint File Service |
| | | | | Sales/Inside Sales | Sales Data | | 2 | SharePoint File Service |
| | | | | Sales/Inside Sales/Leads | Sales Data | | 2 | SharePoint File Service |

- Doesn't degrade performance

Detailed Analytics for Forensics



File Access Breakdown By Data Type



Focus on access to financial data

What are the primary departments accessing this data?

Why are G&A accessing financial data?

Who accessed this data?
When & what did they access?

Event Date and Time	User Name	User Department	Operation	Full Path	Data Type	Data Owner
September 9, 2011 8:21:59 AM	EWILSON	G&A	Read	Finance/Budgets	Financial Data	Chester COX
September 9, 2011 8:21:59 AM	EWILSON	G&A	Read	Finance/Budgets/Budget Prep FY10.pptx	Financial Data, National ID	Chester COX
September 9, 2011 8:21:59 AM	EWILSON	G&A	Read	Finance/Budgets/Forms	Financial Data	Chester COX
September 9, 2011 8:20:57 AM	EWILSON	G&A	Read	Finance/Budgets/Forms	Financial Data	Chester COX

Who owns this data?

#3: Respond to Suspicious Activity



- Summary:
 - SharePoint is used as a place to share information
 - A broad range of internal and external groups are given access
 - Organizations need to balance trust and openness with the ability to detect and alert on suspicious activity
- Why challenging?
 - No automated analysis of access activity
 - Rights management (RMS) is complex to configure and maintain
- What is Required?
 - Policy framework layered on top of the audit record can identify suspicious behavior
 - Pre-configured policies simplify monitoring and response processes
- Example: In the Wikileaks scenario, Manning used an automated process to crawl the SharePoint system and to siphon out available files. A simple occurrences policy would have alerted if a certain number of files were touched in a small timeframe.



Basic Elements: Alerting



OWASP

The Open Web Application Security Project

- Access control
 - Alert/Block access that violates corporate policies



Real-time Enforcement: Possible Data Leakage



OWASP

The Open Web Application Security Project

Is someone accessing large amounts of data?

IMPERVA SECURESPHERE

Discovery & Classification | Setup | Profile | Risk Management | Policies | Audit | Reports | Monitor | Threat Radar

Security | Audit | Data Enrichment | System Events | Action Sets

Activate | Save As | Actions

SharePoint - Suspicious Data Leakage Activity

Policy Configuration: File Operations is [Read] Occurrence definition

Match Criteria

File Operations

Operations: At least one

Operations:

- Checkin
- CheckOut
- Copy

Selected: Read

Occurrence

Occurred more than:	100	Times
Within:	3600	Seconds

Available Match Criteria

- Additional Operation Data
- Data Set: Attribute Lookup

Main > Policies > Security

1 Imperva Inc.

Out-of-the-box policies

Alert when a user reads 100 files
within the same hour

Real-time Enforcement: Possible Data Leakage



OWASP

The Open Web Application Security Project

See triggered alerts

IMPERVA SECURESPHERE

Dashboard | Alerts | Violations | Sys

Main Admin Preferences Tasks Log out Help

Save As Actions

Alerts (filtered)

Page 1 of 1

No. Updated # Alert Descr

Today (13)

No.	Updated	#	Alert Descr
150	14:35:08	1	SharePoint - Suspicious Data Leakage Activity
151	14:35:08	1	SharePoint - Suspicious Data Leakage Activity
152	14:35:08	1	SharePoint - Suspicious Data Leakage Activity
141	14:28:07	1	SharePoint - Suspicious Data Leakage Activity
137	14:27:07	1	SharePoint Changes to Permission Level
138	14:27:07	1	SharePoint Changes to Permission Level
139	14:27:07	1	SharePoint Changes to Permission Level
136			
135			
134			
131			
125			
127			

Yesterday (3)

No.	Updated	#	Alert Descr
106	7/10/11	1	SharePoint - Suspicious Data Leakage Activity
107	7/10/11	1	SharePoint - Suspicious Data Leakage Activity
108	7/10/11	1	SharePoint - Suspicious Data Leakage Activity

Event 8718634592694701531: Custom Rule Violation

Key	Value
Violation Type	file
Severity	High
Policy Name	SharePoint - Suspicious Data Leakage Activity
Alert Number	150
Violation Description	SharePoint - Suspicious Data Leakage Activity
Violated Item	Custom Violation
Immediate Action	None
Matched Patterns	

Owner Name Owner Domain Owner Group Owner Department

Full Path File Name File Extension

Main > Monitor > Alerts

admin | Version: 9.0.0.0 Enterprise Edition | © 2011 Imperva Inc.

Drill down for details on “who, what, when, where”

Following an alert:

- Send emails automatically
- Create security events in SIEM tools

CONFIDENTIAL

Data Owner Identification

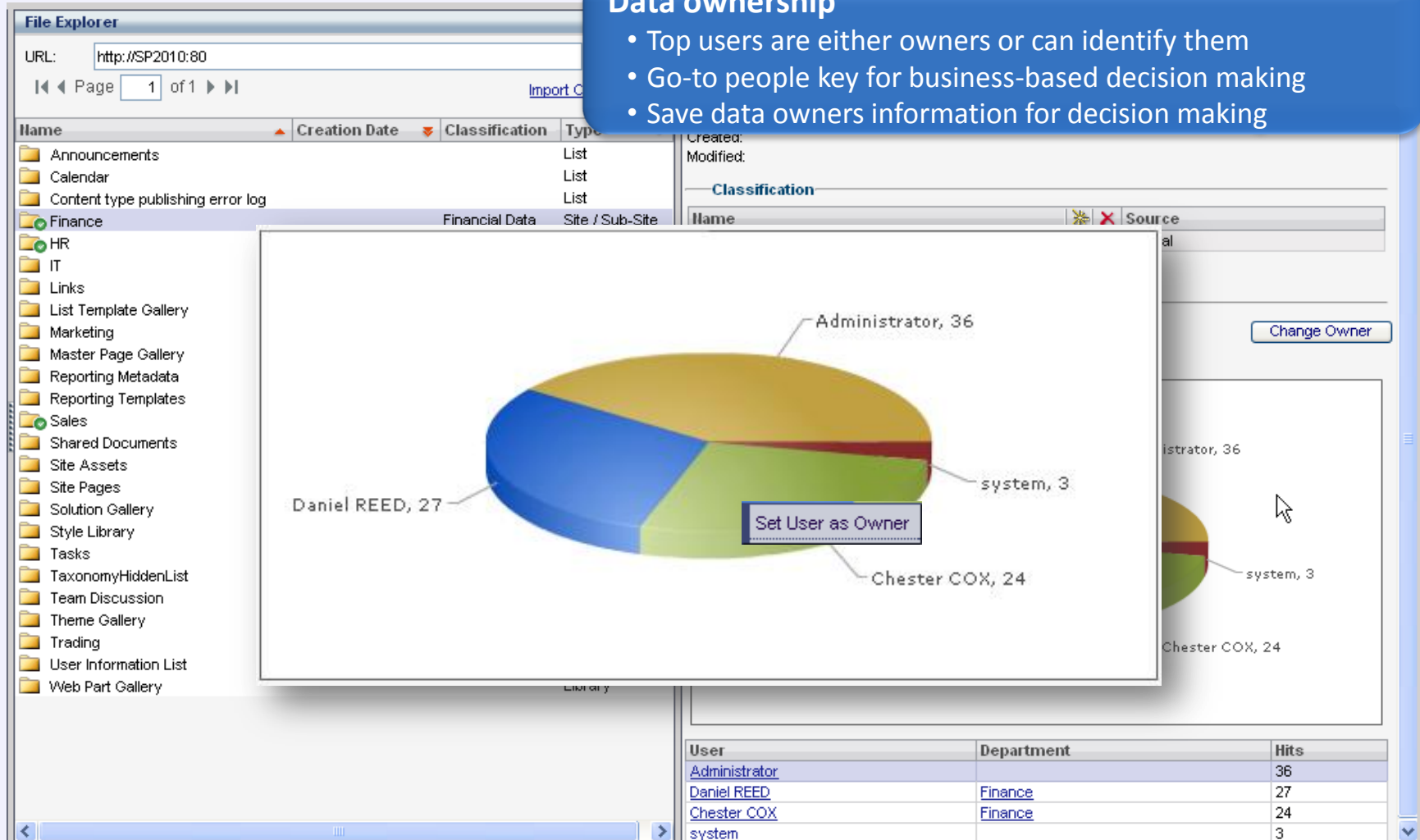


OWASP

The Open Web Application Security Project

Data ownership

- Top users are either owners or can identify them
- Go-to people key for business-based decision making
- Save data owners information for decision making



#4: Protect Web Applications



- Summary:
 - Web applications and portals are a common threat vector for hacker attacks
 - 30% of organizations have external-facing SharePoint sites
- Why challenging?
 - Time consuming process to discover, patch, and test vulnerabilities
- What is Required?
 - Real-time hack protection
 - Allows flexibility in resolution timelines
 - Includes out of the box policies to protect SharePoint
- **Example:** According to CVE details, XSS is the most commonly reported vulnerability in SharePoint.



What Do Hackers Think?



OWASP

The Open Web Application Security Project

Another thing, I have a registered account on there Sharepoint - if anyone knows any 2010 Sharepoint exploits/vulns please PM me them.

Example: April 2010, Microsoft reveals a SharePoint issue

The vulnerability could allow escalation of privilege (EoP) within the SharePoint site. If an attacker successfully exploits the vulnerability, the person could run commands against the SharePoint server with the privileges of the compromised user.

Source: <http://www.eweek.com/c/a/Security/Microsoft-Confirms-SharePoint-Security-Vulnerability-187410/>



- Web Application Firewall
 - Attack protection
 - Reputation controls
- Database protection
 - Fully audit SQL Server local activities
 - Block unapproved database changes
- SharePoint Web Policies
 - Out-of-the-box security and compliance
 - Always up-to-date



Attack Protection



The Open Web Application Security Project

The screenshot displays the Imperva SecureSphere management console. At the top, navigation tabs include Main, Admin, Preferences, Tasks, Log out, and Help. Below these are functional tabs: Discovery & Classification, Setup, Profile, Risk Management, Policies, Audit, Reports, Monitor, and ThreatRadar. The left sidebar shows a 'Sites Tree' with a hierarchy: All > Default Site > sharepoint 2010 - DB Cluster > SharePoint DB Service, and sharepoint 2010 - WFE Cluster > SharePoint File Service > SharePoint Http Service. The main content area is titled 'WAF Policies customized for SharePoint based sites'. It features a 'Basic Security Policies' section with a dropdown menu currently showing 'SharePoint Web Protocol Policy'. Below this is an 'Additional Security Policies' section with a table listing various policies. An orange callout box points to the 'SharePoint - Repeated Failed Login Attempts' policy, asking 'Repeated failed login attempts?'. Another orange callout box points to the 'SharePoint - External Access to Admin URLs' policy, asking 'Are external users accessing admin pages?'. The bottom status bar shows 'Main > Setup > Sites', 'User: admin', 'Version: 9.0.0.0 Enterprise Edition', and '© 2011 Imperva Inc.'.

WAF Policies customized for SharePoint based sites

OOTB Security Policies

Are external users accessing admin pages?

Repeated failed login attempts?

Main > Setup > Sites User: admin Version: 9.0.0.0 Enterprise Edition © 2011 Imperva Inc.

Google Diggity Project



OWASP

The Open Web Application Security Project

Search Diggity

File Options Help

GoogleDiggity CodeSearchDiggity BingDiggity LinkFromDomainDiggity DLPDiggity FlashDiggity MalwareDiggity

Advanced Simple

Query Appender

Queries

- ☐ FSDB
- ☐ GHDB
- ☐ GHDBReborn
- ☐ SLDB
- ☐ SLDBNEW
- ☒ SharePoint Diggity
- ☐ FlashDiggity Initial
- ☐ DLPDiggity Initial

SCAN Cancel Download

API Key: [Create](#)

☐ Hide

Google Custom Search ID: [Create](#)

☐ Hide

Sites/Domains Add

[Import](#)

[Clear](#)

[explore.lsc.edu](#) [\[Remove\]](#)

Category	Subcategory	Search String	Page Title	URL
SharePoint Diggity	Forms	inurl:"/forms/allitems.aspx" ext:aspx site:[redacted].edu	Video - All Pictures	http://[redacted].edu/tsc/Video/Forms/AllItems.aspx
SharePoint Diggity	Forms	inurl:"/forms/allitems.aspx" ext:aspx site:[redacted].edu	Calendars - All Documents	http://[redacted].edu/Hours/Forms/AllItems.aspx
SharePoint Diggity	Forms	inurl:"/forms/allitems.aspx" ext:aspx site:[redacted].edu	Video - All Pictures	http://[redacted].edu/tsc/Video/Forms/AllItems.aspx
SharePoint Diggity	Forms	inurl:"/forms/allitems.aspx" ext:aspx site:[redacted].edu	Calendars - All Documents	http://[redacted].edu/Hours/Forms/AllItems.aspx
SharePoint Diggity	Forms	inurl:"/forms/allitems.aspx" ext:aspx site:[redacted].edu	Video - All Pictures	http://[redacted].edu/tsc/Video/Forms/AllItems.aspx
SharePoint Diggity	Forms	inurl:"/forms/allitems.aspx" ext:aspx site:[redacted].edu	Calendars - All Documents	http://[redacted].edu/Hours/Forms/AllItems.aspx
SharePoint Diggity	Forms	inurl:"/forms/allitems.aspx" ext:aspx site:[redacted].edu	Video - All Pictures	http://[redacted].edu/tsc/Video/Forms/AllItems.aspx
SharePoint Diggity	Forms	inurl:"/forms/allitems.aspx" ext:aspx site:[redacted].edu	Calendars - All Documents	http://[redacted].edu/Hours/Forms/AllItems.aspx
SharePoint Diggity	Forms	inurl:"/forms/allitems.aspx" ext:aspx site:[redacted].edu	Video - All Pictures	http://[redacted].edu/tsc/Video/Forms/AllItems.aspx
SharePoint Diggity	Forms	inurl:"/forms/allitems.aspx" ext:aspx site:[redacted].edu	Calendars - All Documents	http://[redacted].edu/Hours/Forms/AllItems.aspx

Output Selected Result

The remote server returned an error: (403) Forbidden.
Error at query, "inurl:"/_vti_bin/UserProfileService.aspx" ext:asmx":
The remote server returned an error: (403) Forbidden.
Error at query, "inurl:"/_vti_bin/spscrawl.aspx" ext:asmx":
The remote server returned an error: (403) Forbidden.
Error at query, "inurl:"/_vti_bin/AreaService.aspx" ext:asmx":
The remote server returned an error: (403) Forbidden.
Error at query, "inurl:"/_vti_bin/WebPartPages.aspx" ext:asmx":
The remote server returned an error: (403) Forbidden.
Error at query, "inurl:"/_vti_bin/spsearch.aspx" ext:asmx":
The remote server returned an error: (403) Forbidden.
Total Results: 126.
Scan Complete. [12/13/2011 5:38:35 PM]

Google Status: Ready Download Progress: Idle [Open Folder](#)

#5: Take Control When Migrating Data



- Summary:
 - SharePoint 2010 deployments are up 5X
 - Companies are using SharePoint as a replacement for other data repositories
 - Migration projects are a good time to remediate permissions chaos
- Why challenging?
 - AD users and groups fall out of sync with business requirements
 - Unused (stale) data accumulates over time
 - Manual approaches are overly time consuming
- What is Required?
 - Visibility and rights review tools reduce cost and streamline migrations



A Checklist to Securing SharePoint



OWASP

The Open Web Application Security Project

Get ahead of all SharePoint deployments

- Implement a SharePoint governance policy.
- Put in place security requirements when SharePoint instances go live.
- Don't trust native security features.
- Specify what kind of information can be put in SharePoint.

Identify sensitive data and protect it

- Use search capabilities to identify sensitive data.
- Sensitive data in databases: use database activity monitoring to identify and protect confidential data.
- Sensitive data transacted by SharePoint Web applications
- Secure sensitive data held in files: use file activity monitoring to apply user rights management and auditing capabilities.

A Checklist to Securing SharePoint



OWASP

The Open Web Application Security Project

Deploy user rights management to identify data ownership

- Ensure legitimate access to data.
- Accelerate permissions reviews and management.
- Identify and delete dormant users. Check for dormant users on a regular basis.
- Focus on regulated data and streamline access.
- Adjust department-level access.
- Create permission reports for data owners.
- Implement ownership policies – especially for alerts around unauthorized access.

Protect Web sites

- Identify sensitive data transacted by SharePoint Web applications and use Web application firewalls to monitor and protect intranets, portals, and Web sites.
- Log all failed login attempts.

A Checklist to Securing SharePoint



OWASP

The Open Web Application Security Project

Enable auditing for compliance and forensics

- Who accessed this data?
- When and what did they access?
- Who owns this data?
- Are external users accessing admin pages?
- Have there been repeat failed login attempts?



OWASP

The Open Web Application Security Project

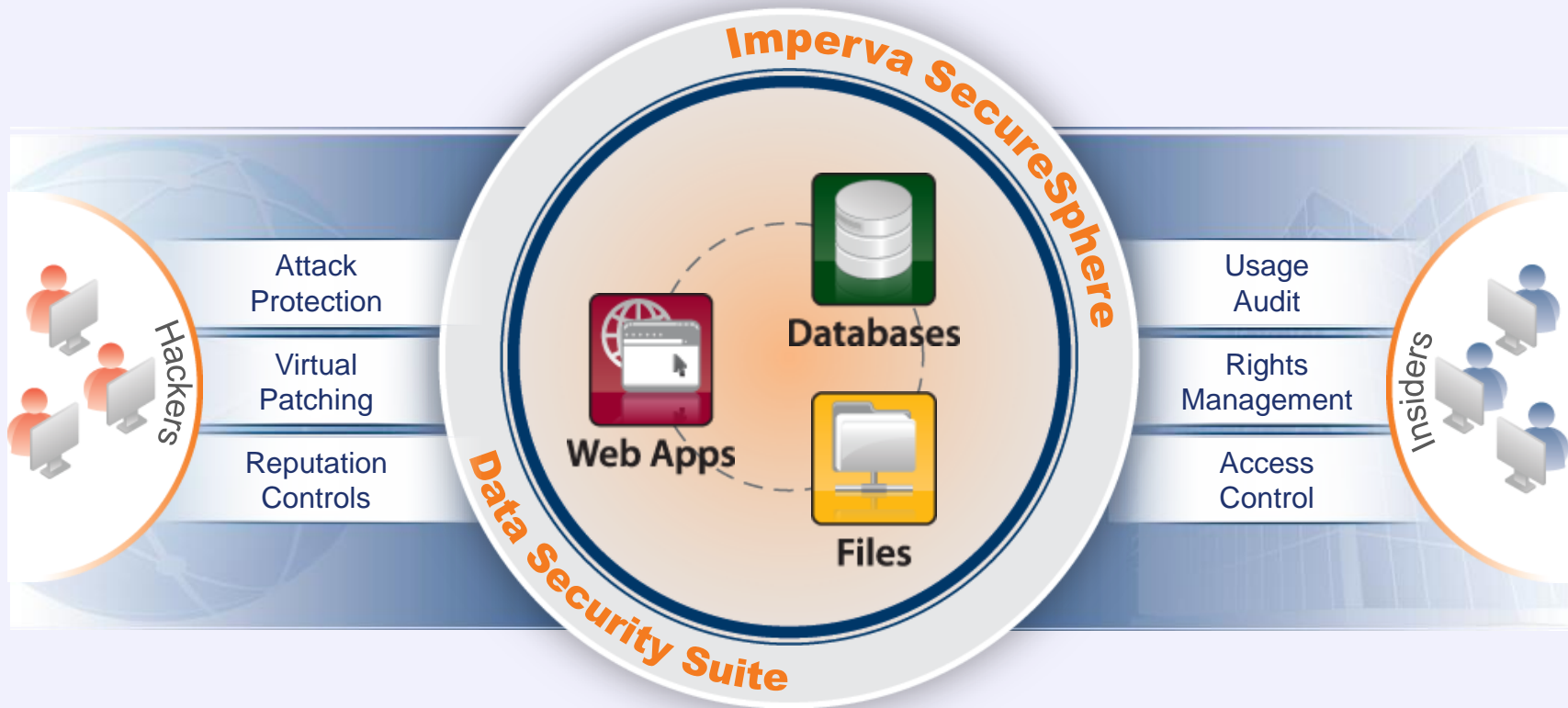
SecureSphere for SharePoint

Imperva Data Security in 60 Seconds



OWASP

The Open Web Application Security Project



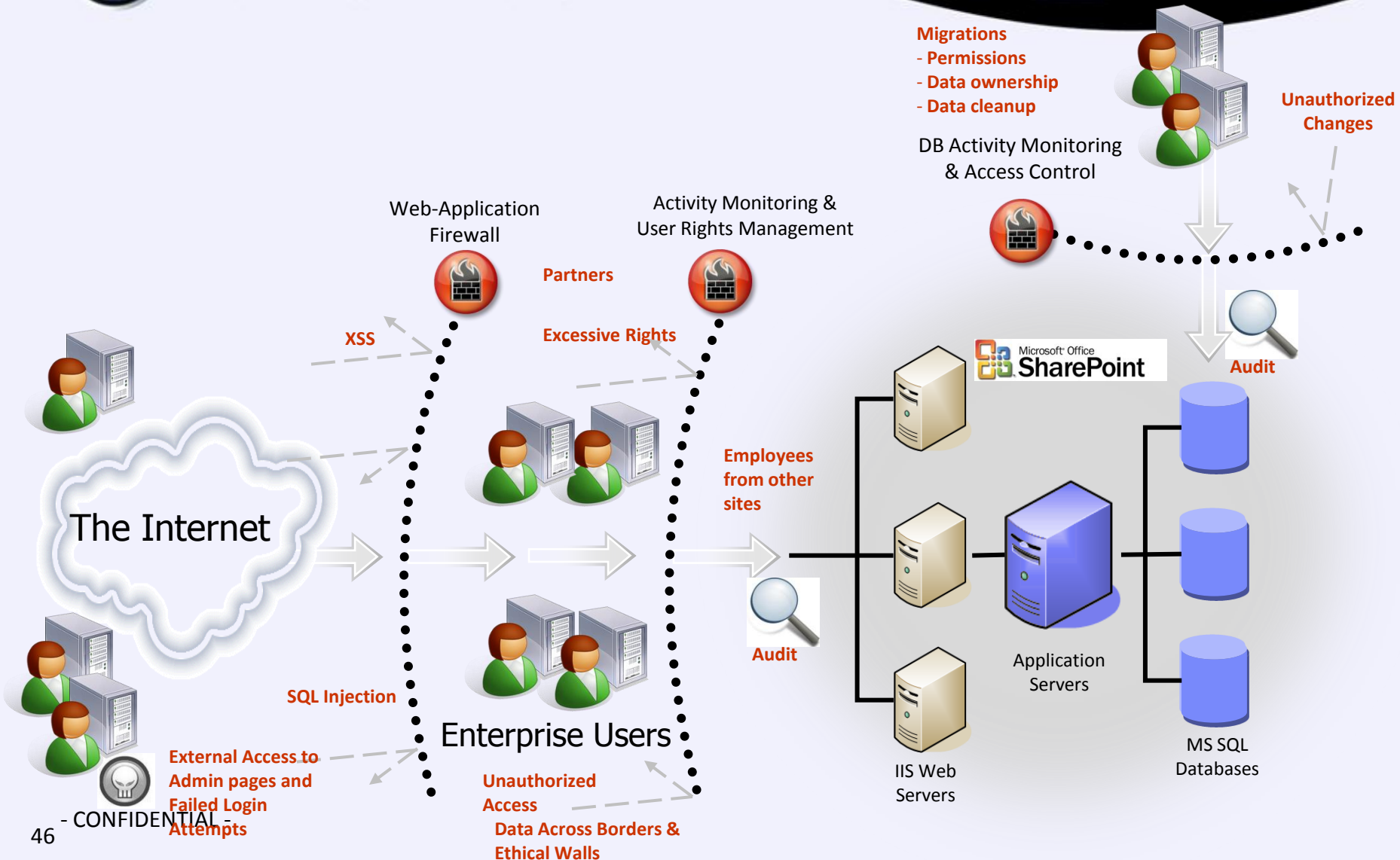
SharePoint & SecureSphere for SharePoint



OWASP

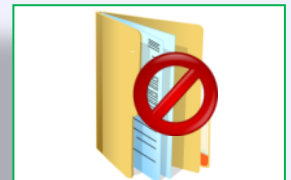
The Open Web Application Security Project

Administrators





- User rights management
 - Aggregate and visualize rights
 - Identify excessive and dormant rights
 - Streamline rights reviews
 - Identify data owners
- Activity monitoring
 - Monitor file & list access in real-time
 - Find unused data
- Policy based threat protection
 - Defend against file, Web and database threats





OWASP

The Open Web Application Security Project

Questions



- About Me

Company
Logo



OWASP

The Open Web Application Security Project