CISO's Guide to Securing SharePoint

Tsvika Klein

Imperva

OWASP
The Open Web Application Security Project

Introduction to SharePoint

- One of the fastest selling products
- On its way to being the first $2 billion business
- 30% year over year growth
- More than 125 million licenses
- Over 65,000 customers
- Revenue comes from ECM, team collaborative applications and enterprise portals
- Security and rights management is #2 add-on

Sites
Composites
Communities
Microsoft SharePoint
Insights
Content
Search

Source: http://www.fiercecontentmanagement.com/story/sharepoint-numbers/2011-10-10

Impact of SharePoint Insecurity

“[Inves ripts on

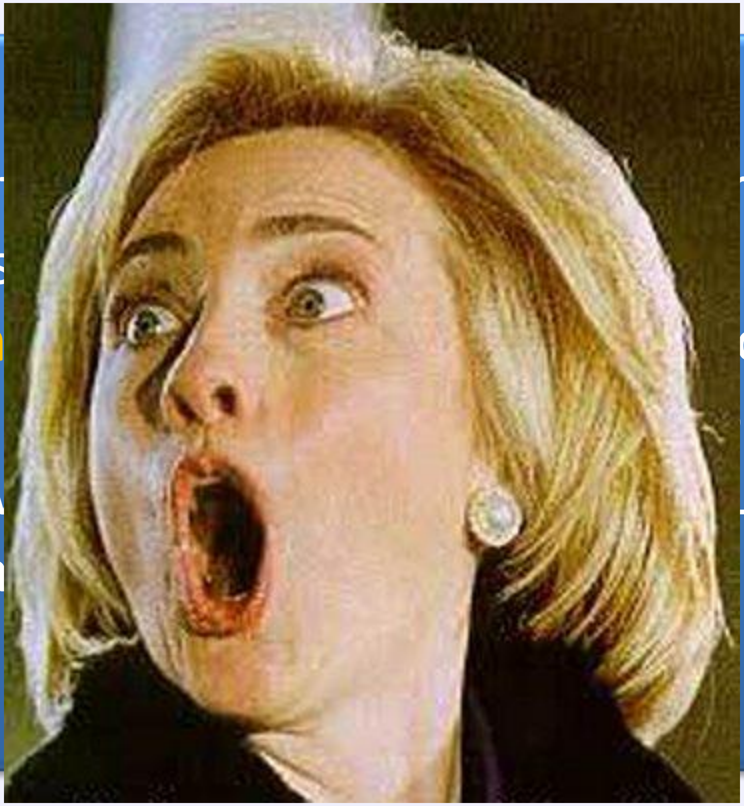
Manning’s Microsoft

SharePoin ocuments.

He ran th cuments,

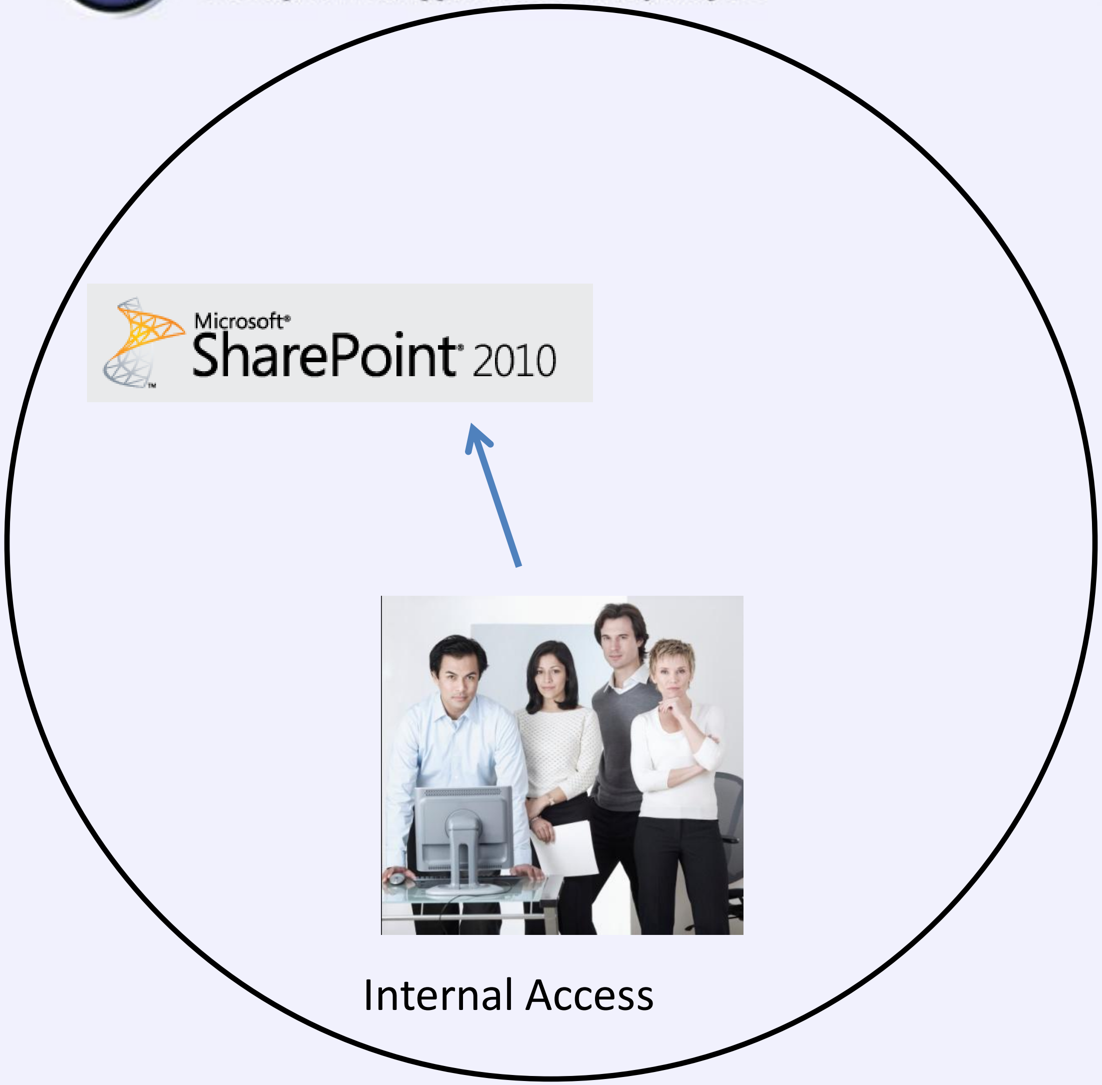
then dow eaks had

publish same.”



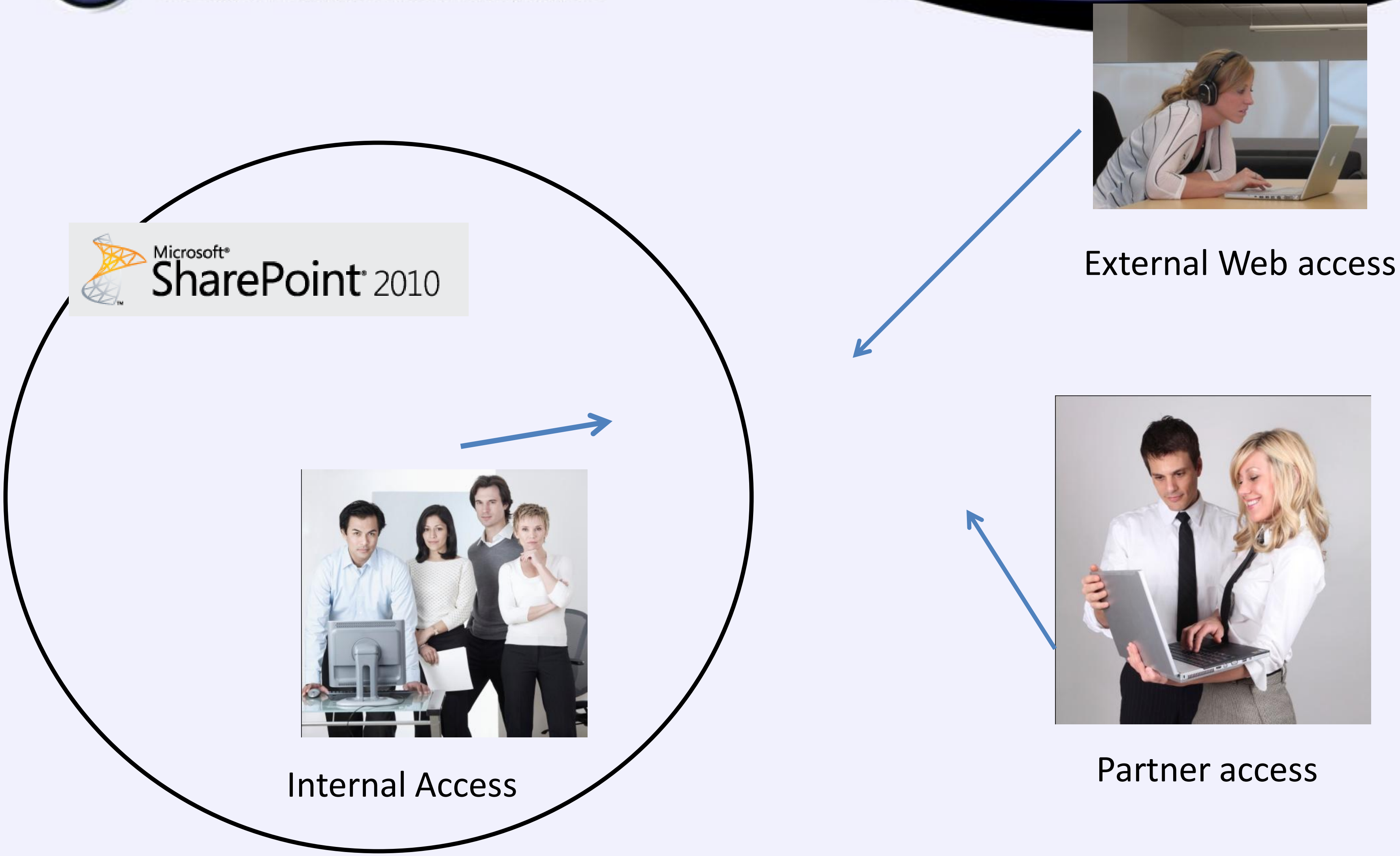
Source: http://www.wired.com/threatlevel/2011/12/cables-scripts-manning/

In the Beginning…



Internal Access

Food Brings Along Appetite



Microsoft SharePoint 2010

External Web access

Partner access

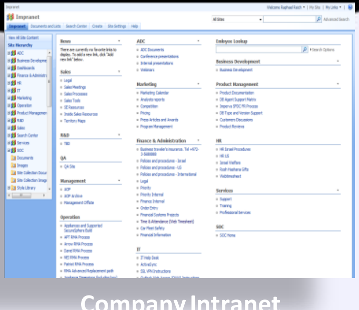
Internal Access

Major SharePoint Deployment Types

OWASP
The Open Web Application Security Project

Internal Portal

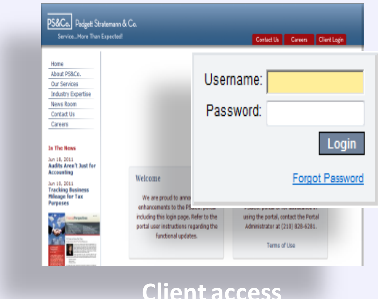
- Uses include SharePoint as a file repository
- Only accessible by internal users



Company Intranet

External Portal

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



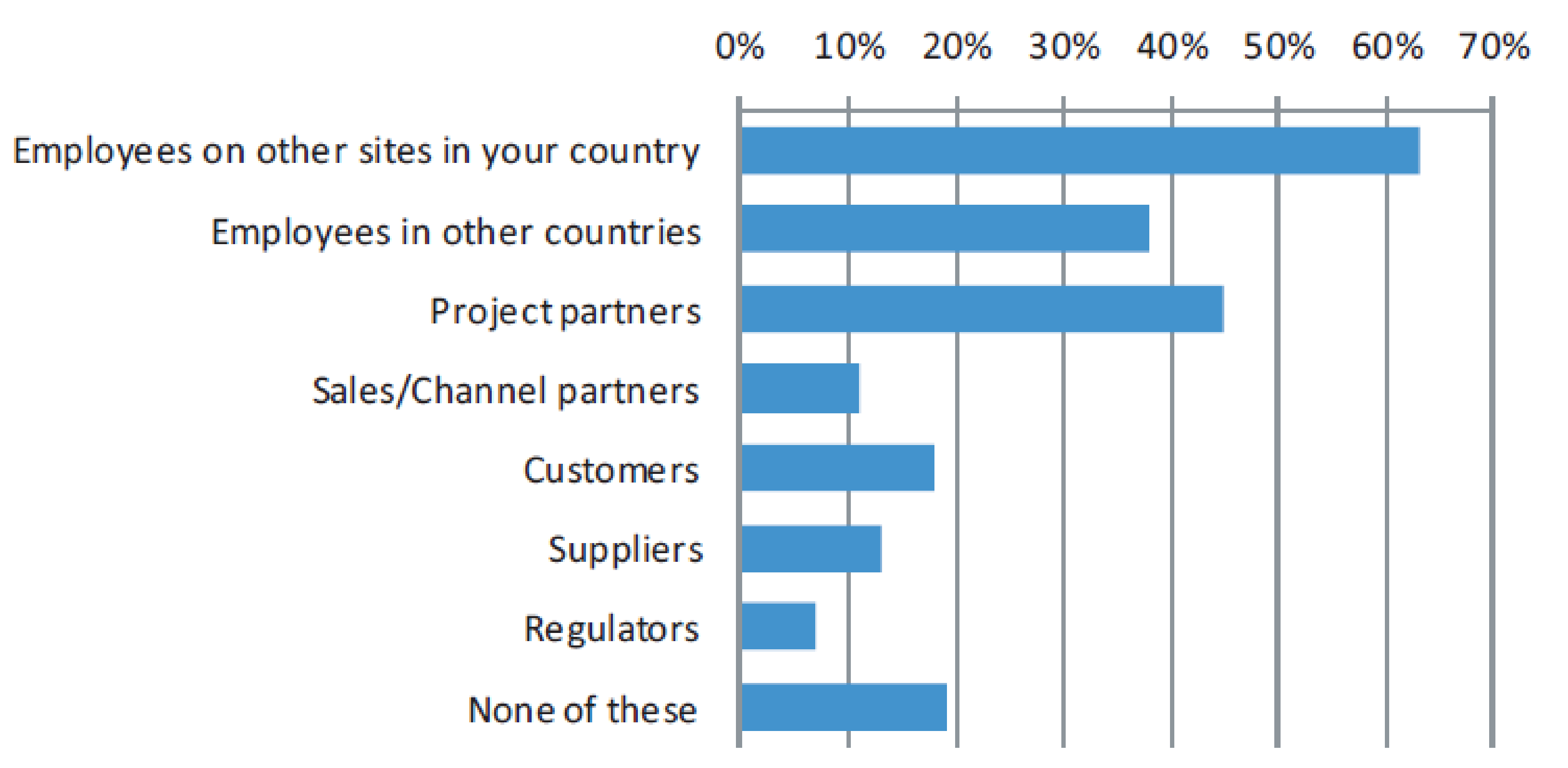
Client access

Internet Website

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

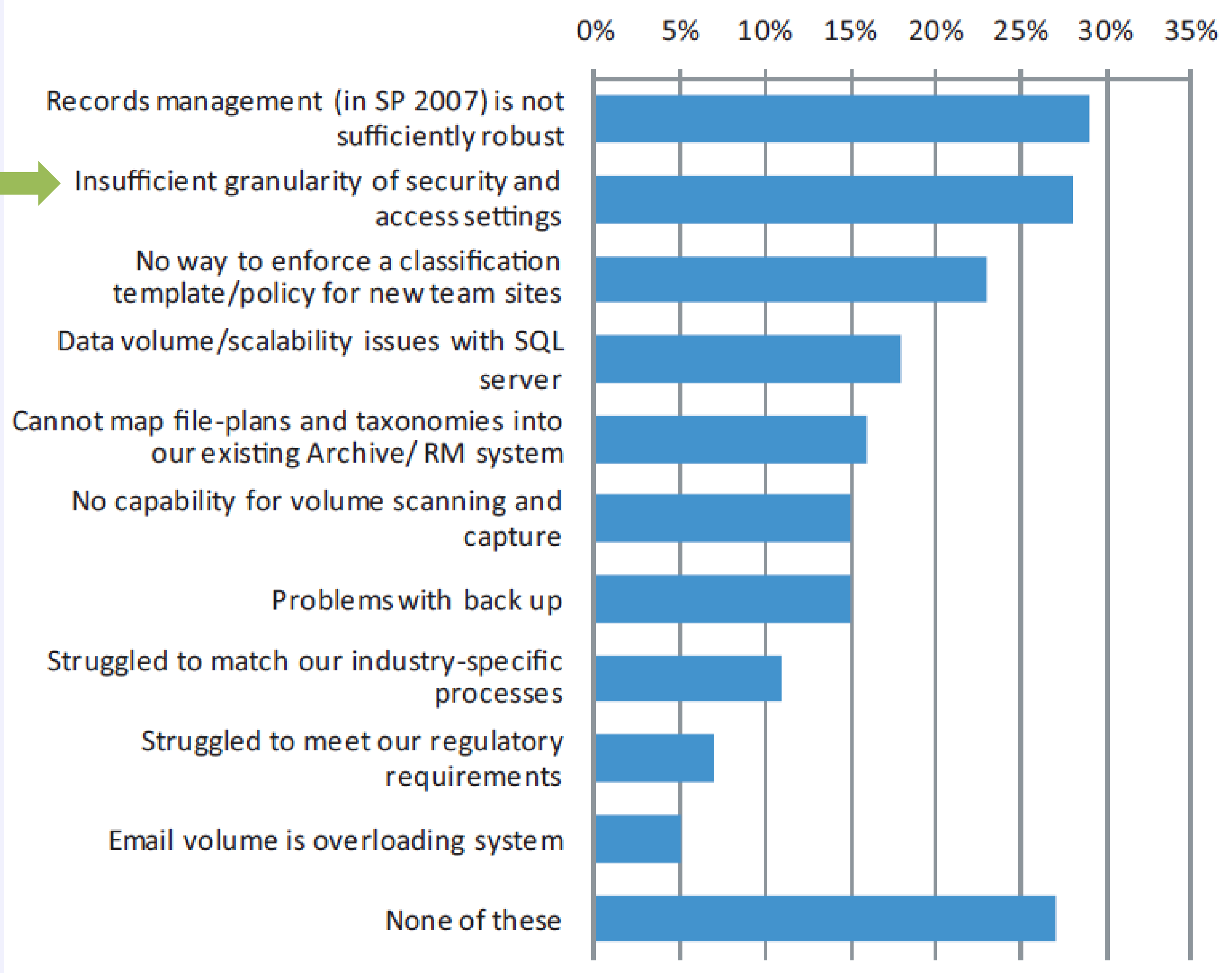
Public website

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



Source: ***SharePoint: Strategies and Experiences***, September 2011

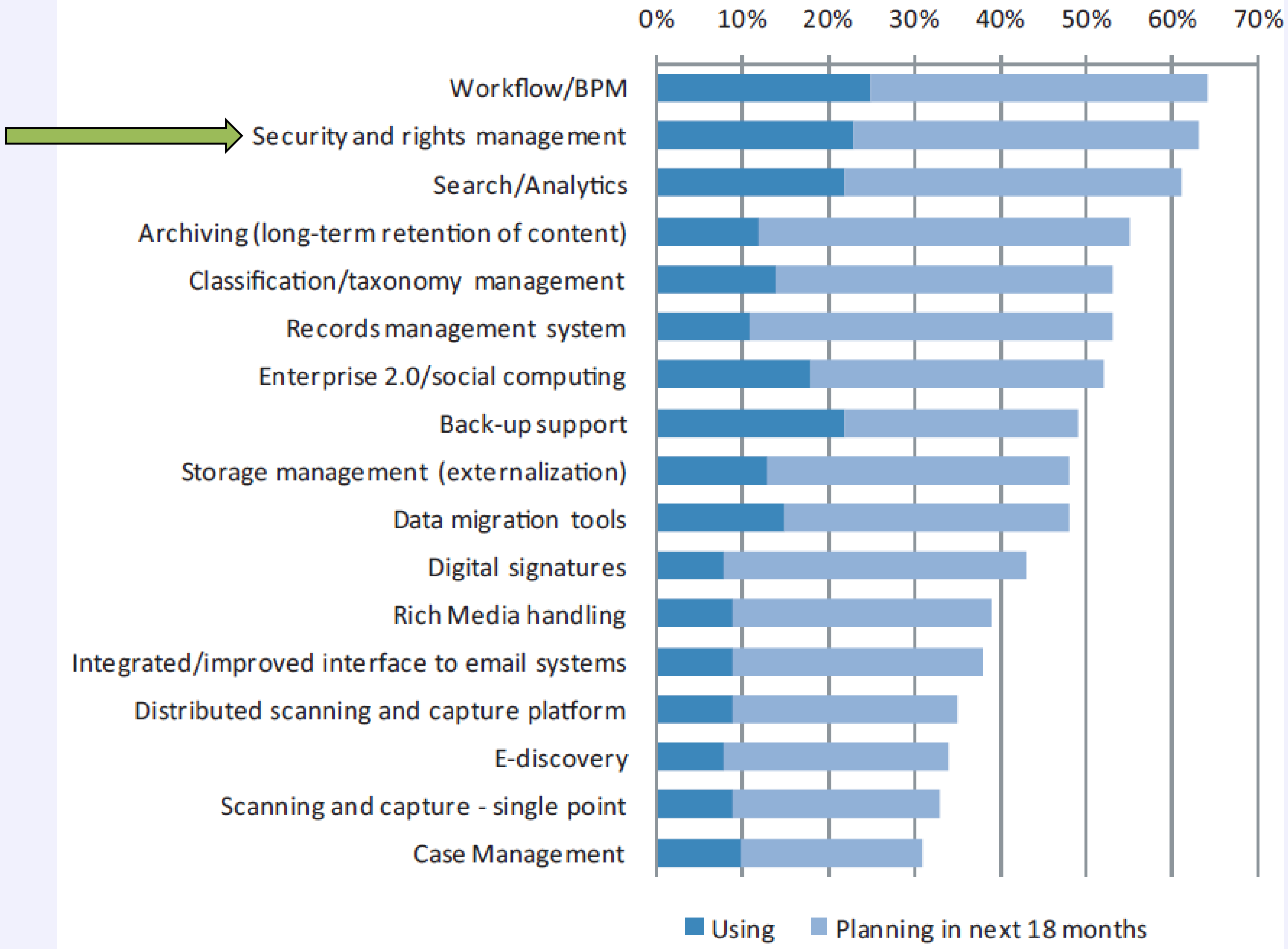
Key Issues With SharePoint



Source: ***SharePoint: Strategies and Experiences***, September 2011

Third-Party Additions

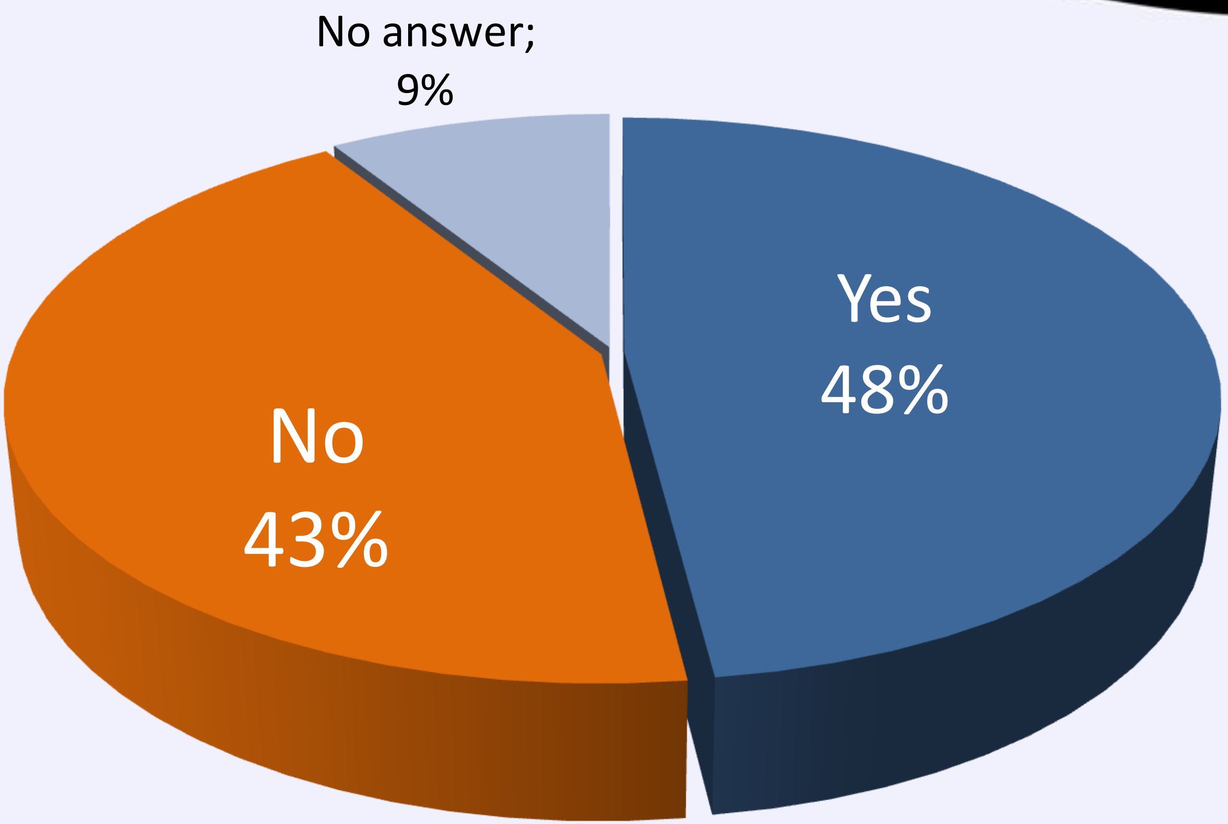
OWASP
The Open Web Application Security Project



Source: ***SharePoint: Strategies and Experiences***, September 2011

Have You Shared Privileged Info via SharePoint?

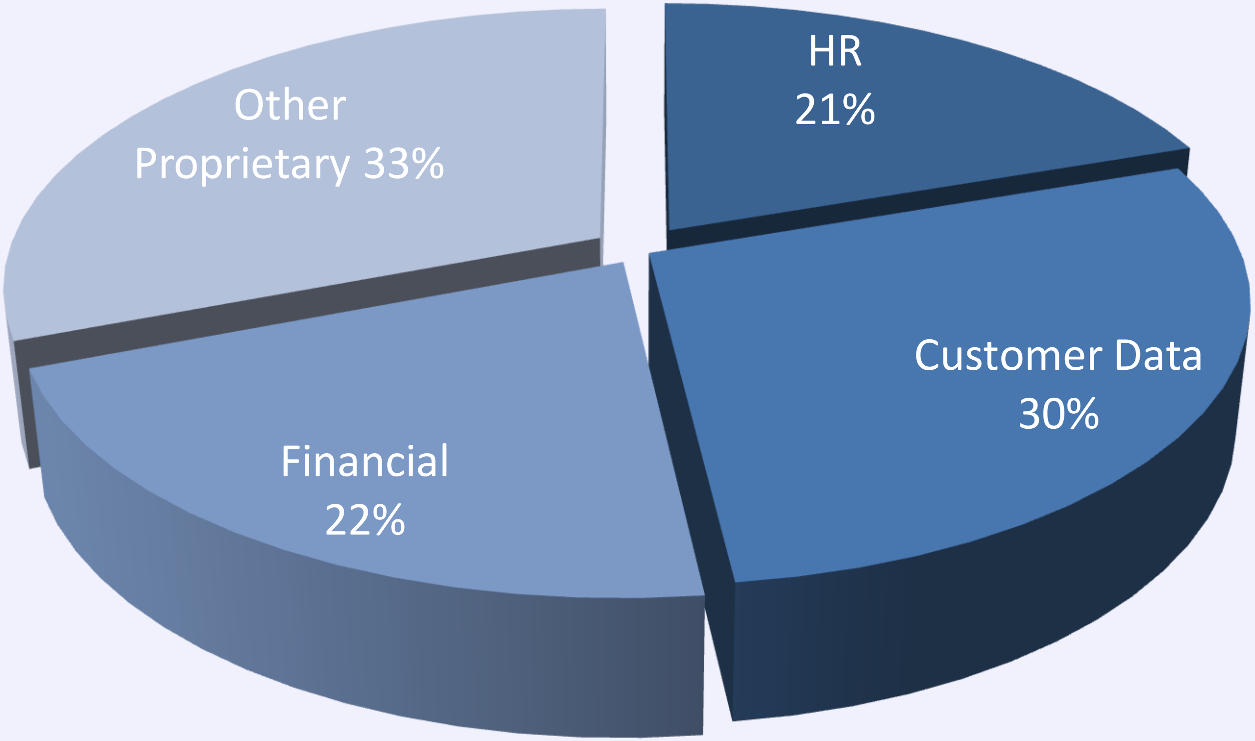
OWASP
The Open Web Application Security Project



Source: NetworkWorld, May 2, 2011

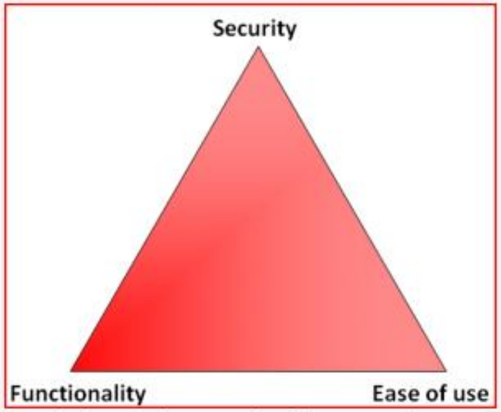
Type of Content Shared

OWASP
The Open Web Application Security Project



Source: NetworkWorld, May 2, 2011

SharePoint 2010 is Still Missing



- Functionality
  - Rights management
  - Proper auditing
  - Web and Database protection
  - Security-centric reporting
  - Security-centric policies
- Bottom line
  - SharePoint is built for collaboration first
  - Security comes second.

MORDAC, THE PREVENTER OF INFORMATION SERVICES.
SECURITY IS MORE IMPORTANT THAN USABILITY.
scottadams@aol.com
www.dilbert.com
IN A PERFECT WORLD, NO ONE WOULD BE ABLE TO USE ANYTHING.
©2007 Scott Adams, Inc./Dist. by UFS, Inc.
To complete the log-in procedure, stare directly at the sun.

© Scott Adams, Inc./Dist. by UFS, Inc.

Native SharePoint Security Capabilities

"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

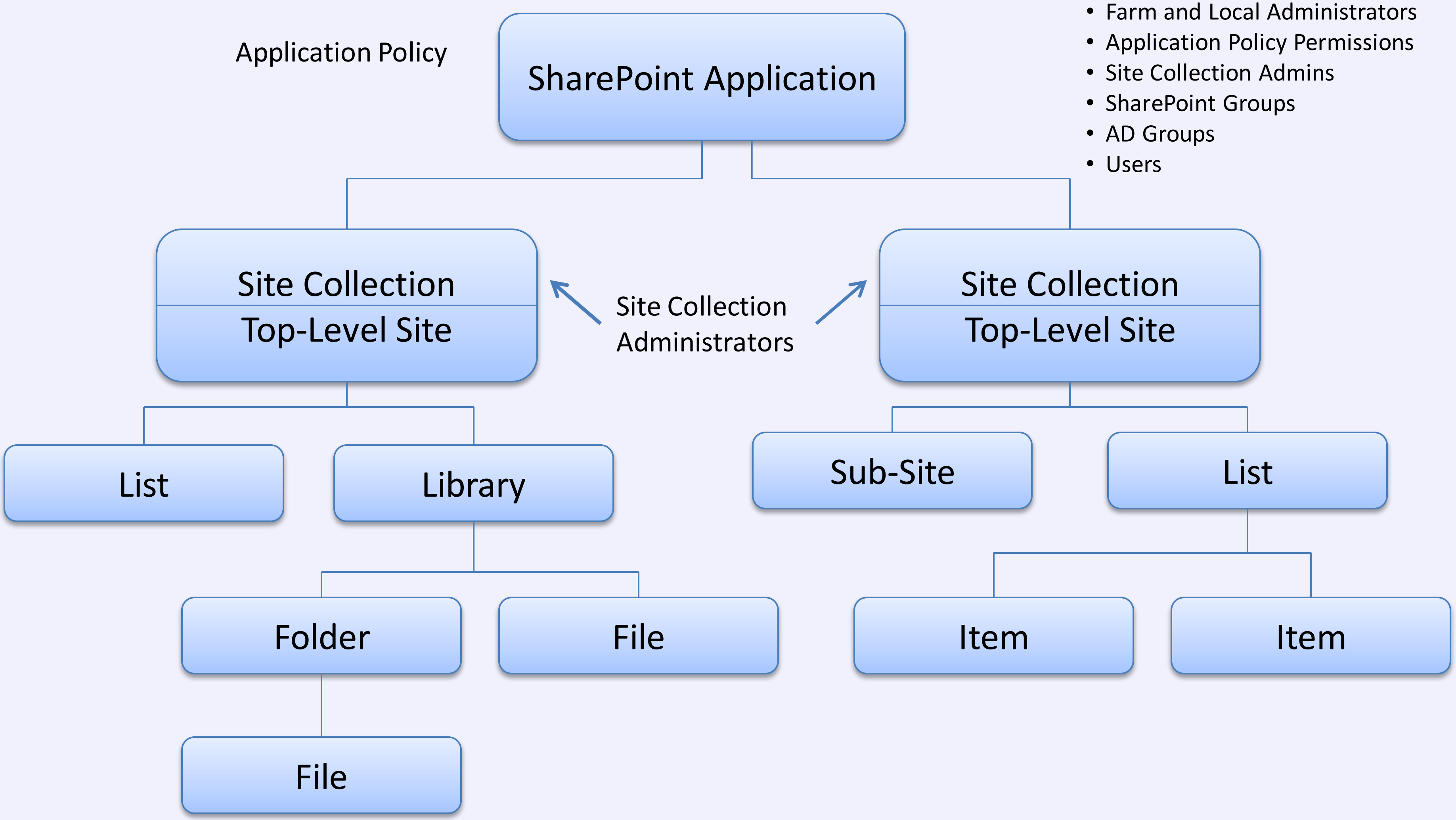
Key SharePoint Security Challenges

#1: Getting Permissions Right

- 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
  - Need to involve data owners.
- What is Required?
  - Automated permissions review tools
  - Baseline and change reports
  - Simplify rights reviews

SharePoint Permission Hierarchy

OWASP
The Open Web Application Security Project

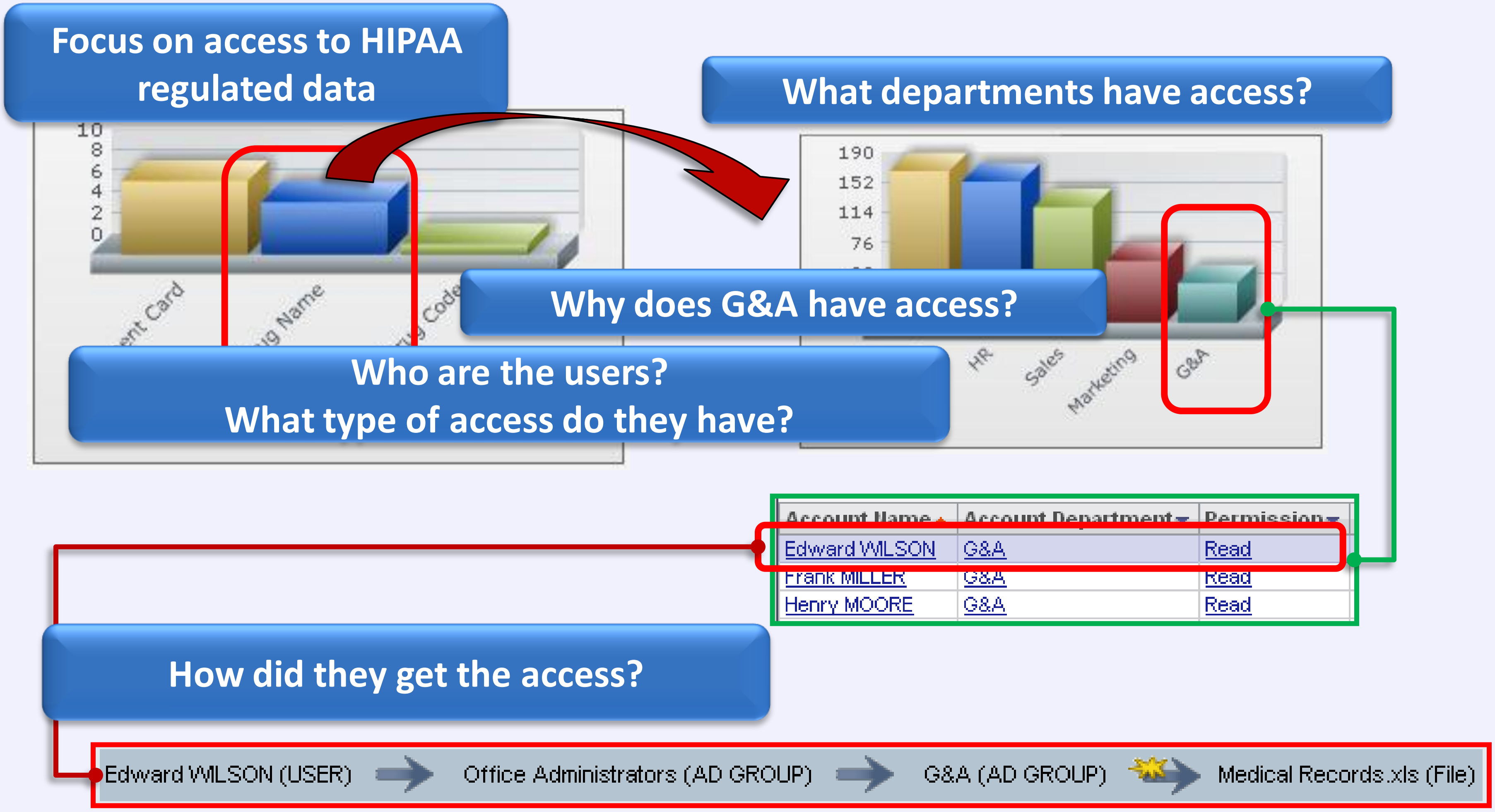


- Farm and Local Administrators
- Application Policy Permissions
- Site Collection Admins
- SharePoint Groups
- AD Groups
- Users

User Rights Management: Doing it Right

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

Finding Excessive Permissions



Focus on access to HIPAA regulated data

What departments have access?

Why does G&A have access?

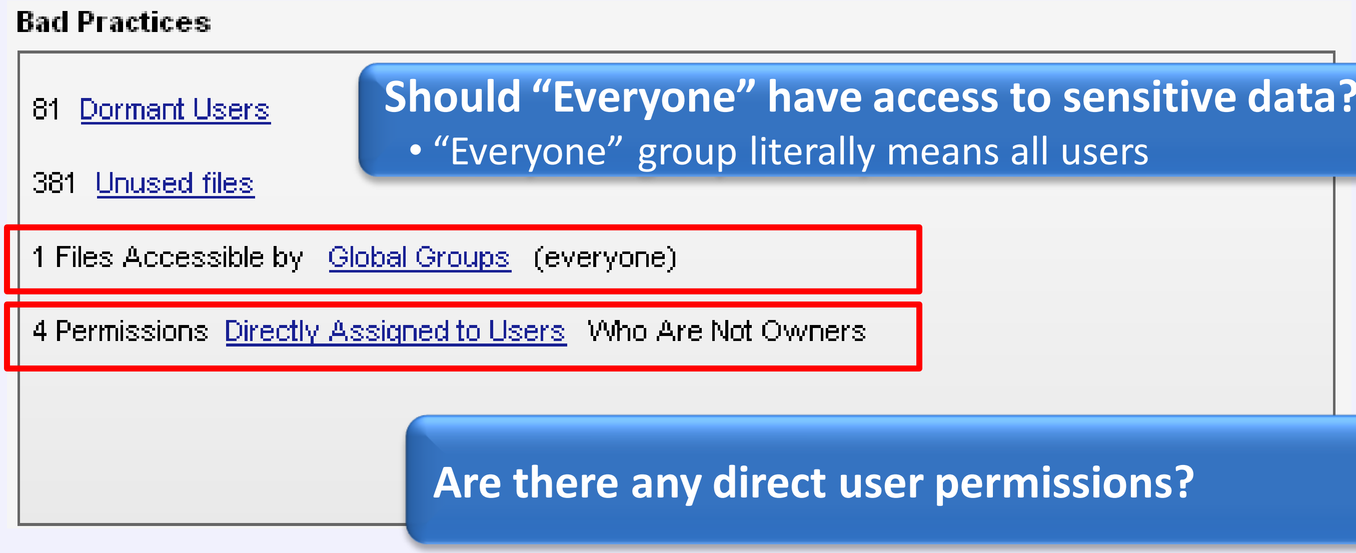
Who are the users?
What type of access do they have?

How did they get the access?

Account Name	Account Department	Permission
Edward WILSON	G&A	Read
Frank MILLER	G&A	Read
Henry MOORE	G&A	Read

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

Automatic Identification of Excessive Rights



Bad Practices

81 Dormant Users

381 Unused files

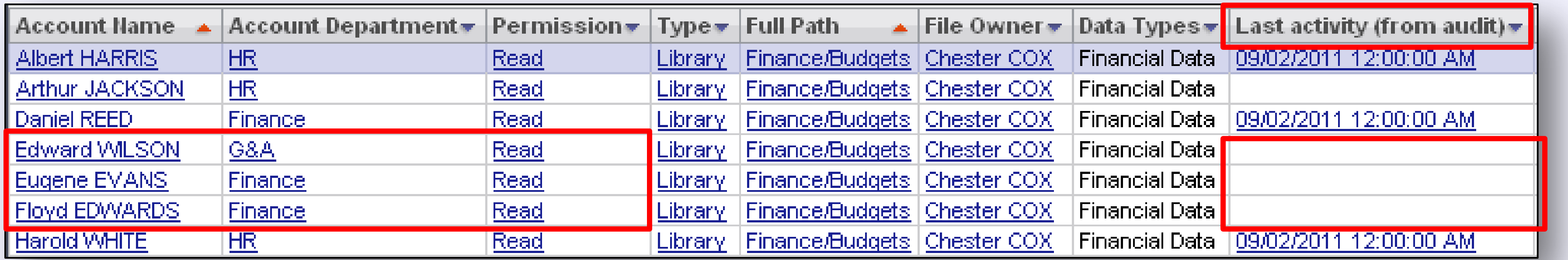
1 Files Accessible by Global Groups (everyone)

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

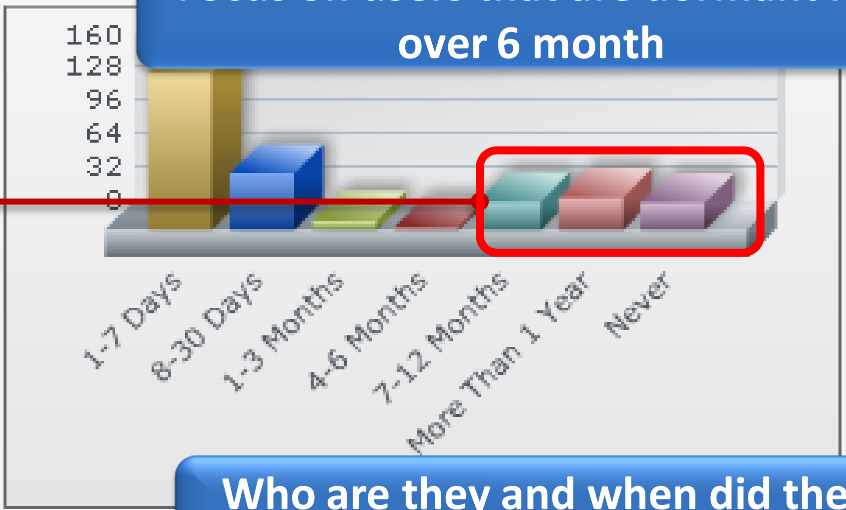
What rights are not used?

- Users with access they appear not to need

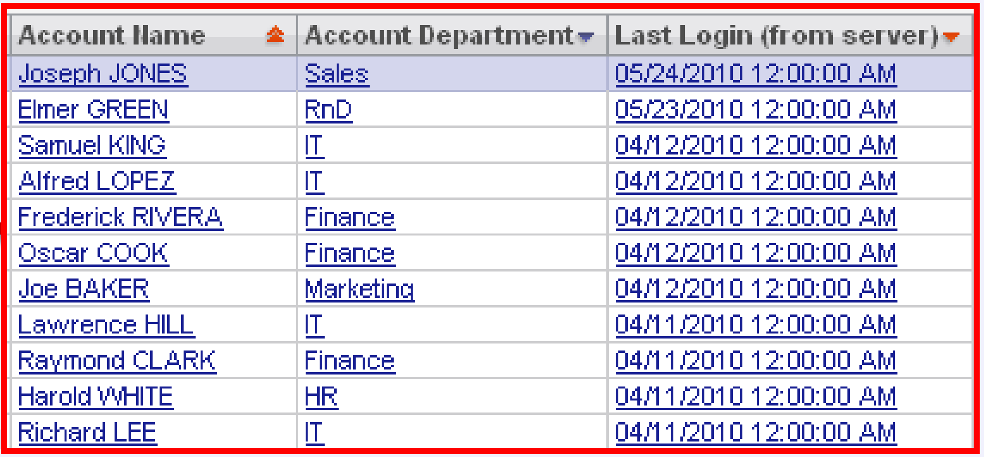
Identifying Dormant Users

Are there dormant users?

Focus on users that are dormant for over 6 month



Who are they and when did they last access?



Account Name	Account Department	Last Login (from server)
Joseph JONES	Sales	05/24/2010 12:00:00 AM
Elmer GREEN	RnD	05/23/2010 12:00:00 AM
Samuel KING	IT	04/12/2010 12:00:00 AM
Alfred LOPEZ	IT	04/12/2010 12:00:00 AM
Frederick RIVERA	Finance	04/12/2010 12:00:00 AM
Oscar COOK	Finance	04/12/2010 12:00:00 AM
Joe BAKER	Marketing	04/12/2010 12:00:00 AM
Lawrence HILL	IT	04/11/2010 12:00:00 AM
Raymond CLARK	Finance	04/11/2010 12:00:00 AM
Harold WHITE	HR	04/11/2010 12:00:00 AM
Richard LEE	IT	04/11/2010 12:00:00 AM

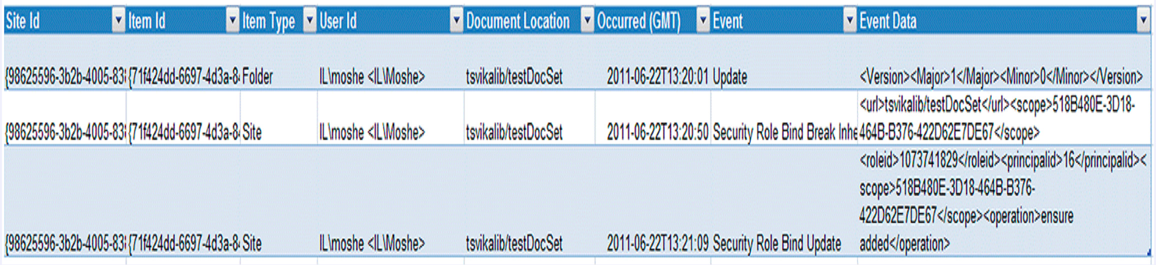
Reviewing User Rights with Data Owners

- Data owners are ultimately responsible for the protection of data
- Data owners have due care responsibility in case of any negligent act
- Data owners should review and manage user rights
  - Review permission changes
  - Revoke unauthorized access permissions
  - Create reports

#2: Compliance Reporting

OWASP
The Open Web Application Security Project

- Summary:
  - If you store business data, you must demonstrate compliance with regulations
- Why challenging?
  - Manual process – minimal inherent data audit capability
  - Native audit trail is not usable/readable
  - No knowledge of the identity of data owners



Site Id	Item Id	Item Type	User Id	Document Location	Occurred (GMT)	Event	Event Data
{98625596-3b2b-4005-83	{71f424dd-6697-4d3a-8	Folder	IL\moshe <IL\Moshe>	tsvikalib/testDocSet	2011-06-22T13:20:01	Update	<Version><Major>1</Major><Minor>0</Minor></Version>
{98625596-3b2b-4005-83	{71f424dd-6697-4d3a-8	Site	IL\moshe <IL\Moshe>	tsvikalib/testDocSet	2011-06-22T13:20:50	Security Role Bind Break Inhe	<url>tsvikalib/testDocSet</url><scope>518B480E-3D18-464B-B376-422D62E7DE67</scope>
{98625596-3b2b-4005-83	{71f424dd-6697-4d3a-8	Site	IL\moshe <IL\Moshe>	tsvikalib/testDocSet	2011-06-22T13:21:09	Security Role Bind Update	<roleid>1073741829</roleid><principalid>16</principalid><scope>518B480E-3D18-464B-B376-422D62E7DE67</scope><operation>ensure added</operation>

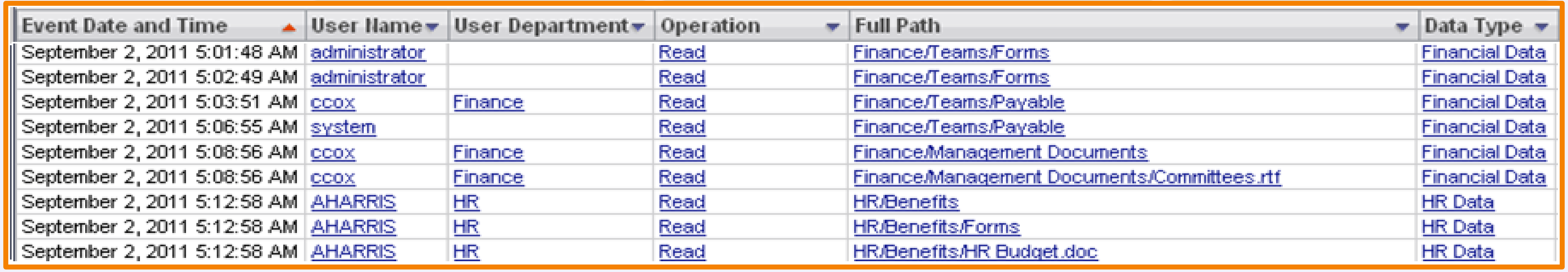
#2: Compliance Reporting

OWASP
The Open Web Application Security Project

- Summary:
  - If you store business data, you must demonstrate compliance with regulations
- Why challenging?
  - Manual process – minimal inherent data audit capability
  - Native audit trail is not usable/readable
  - No knowledge of the identity of data owners
- What is Required?
  - Human-readable activity auditing and reporting
  - Add enrichment data to simplify compliance process
  - Data owner identification
  - Audit Analytics
- 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.

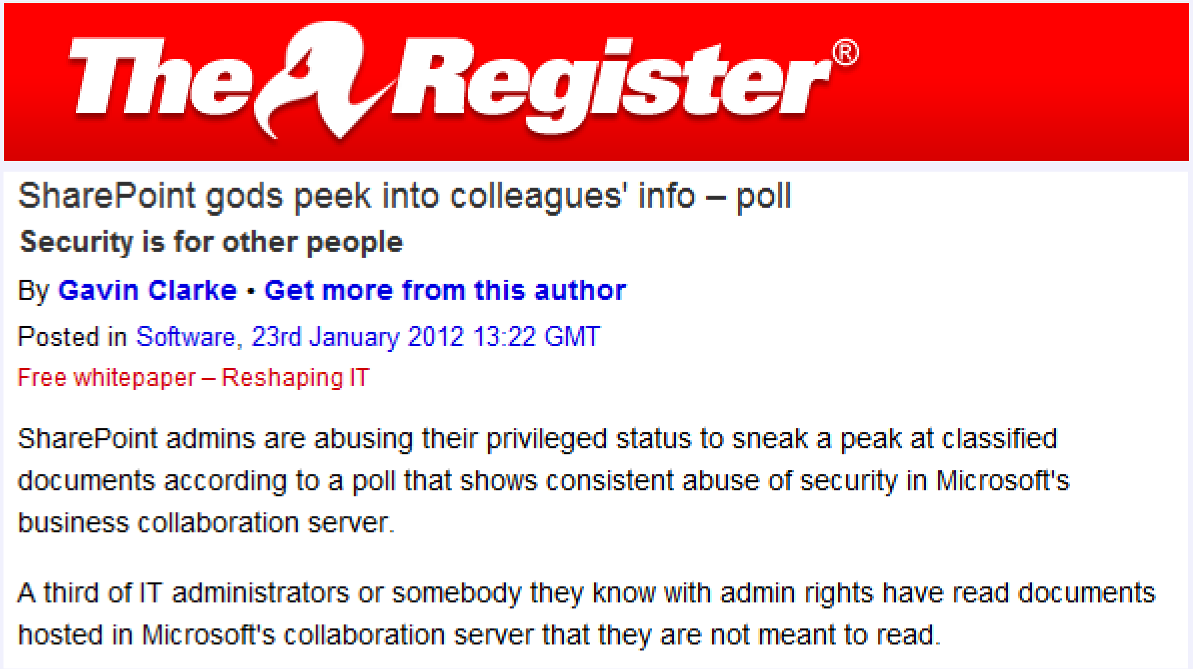
Full Audit Trail

When | Who | Where | 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

SharePoint Admins Gone Wild



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

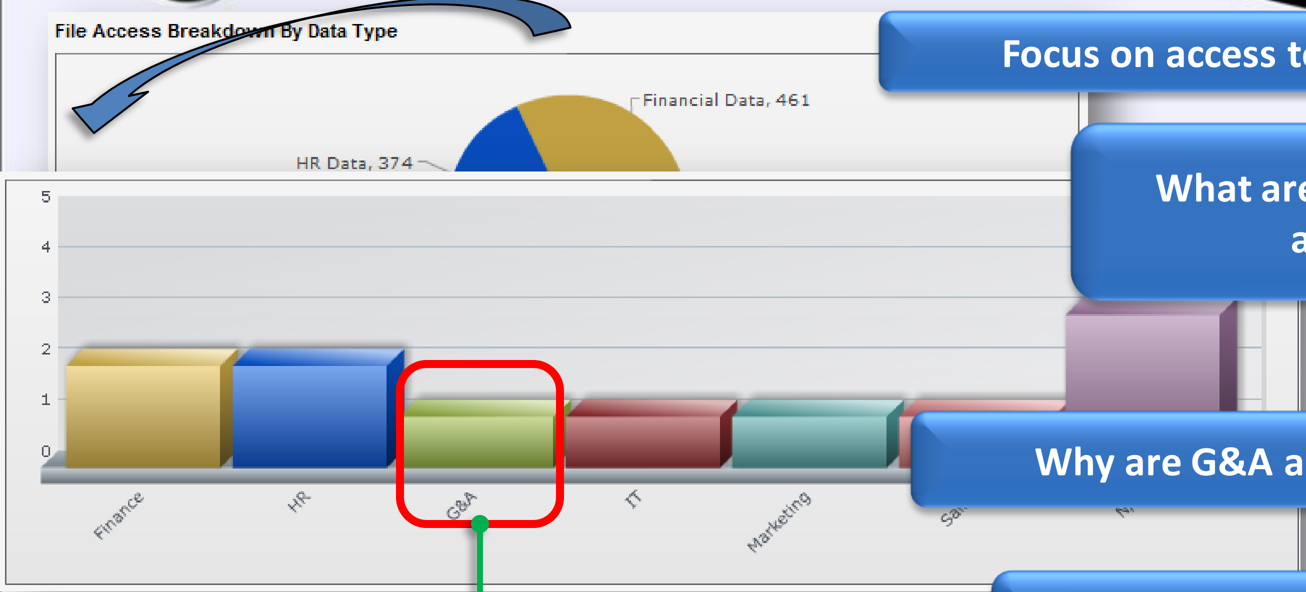
SharePoint admins are abusing their privileged status to sneak a peak at classified documents according to a poll that shows consistent abuse of security in Microsoft's business collaboration server.

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."

Detailed Analytics for Forensics

OWASP
The Open Web Application Security Project

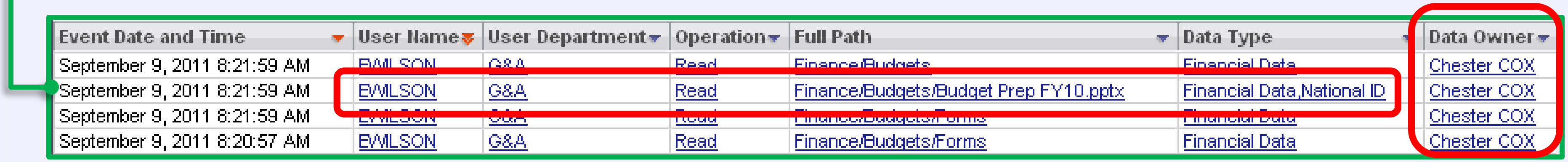


Focus on access to financial data

What are the primary departments accessing this data?

Why are G&A accessing financial data?

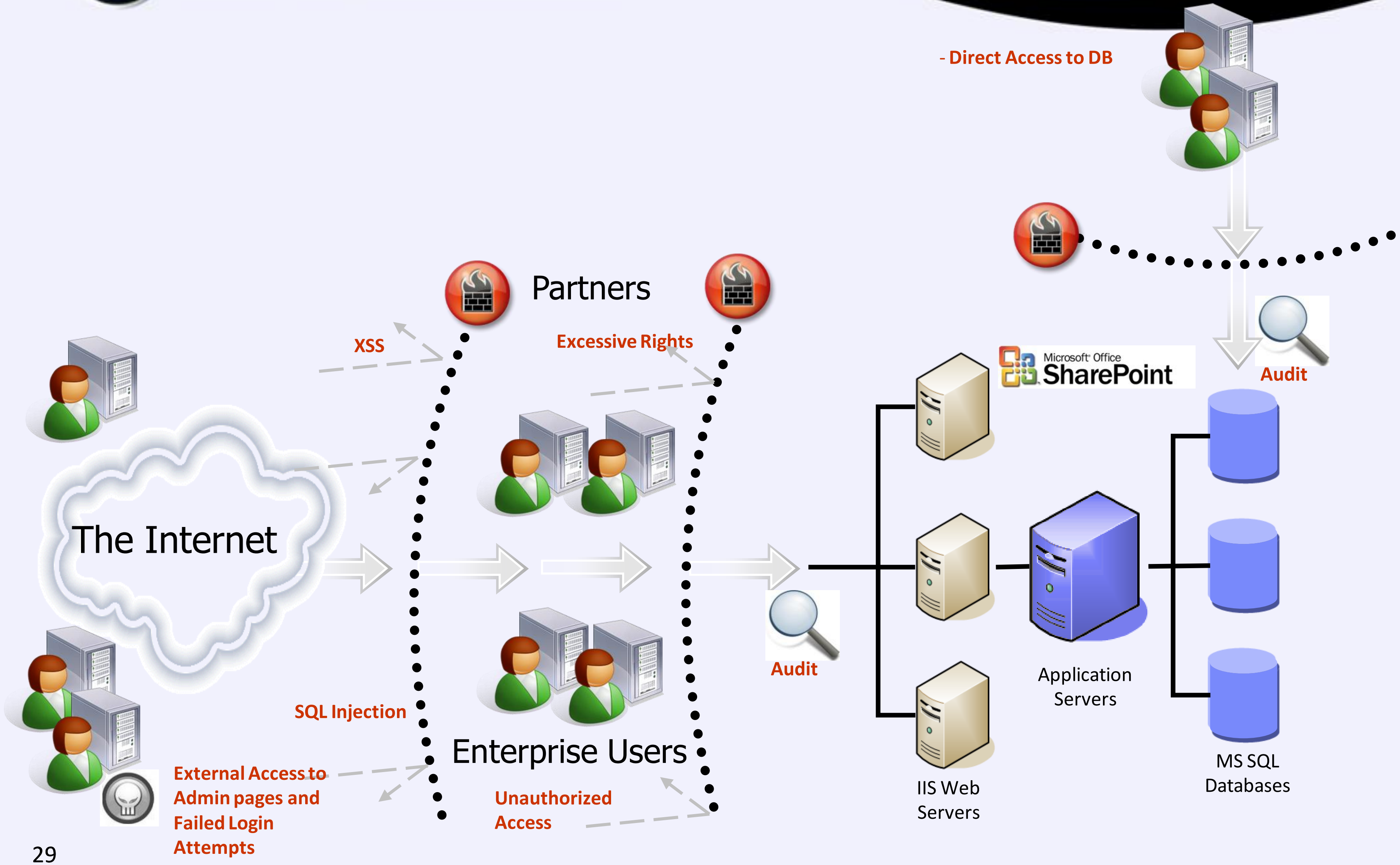
Who accessed this data?
When & what did they access?



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

Who owns this data?

SharePoint Architecture



#3: Protect Web Applications

OWASP
The Open Web Application Security Project

- Summary:
  - Web attacks are a common threat
  - 30% of organizations have external-facing SharePoint sites
- Why challenging?
  - Need to patch the system frequently
  - 3rd party add-ons
- What is Required?
  - Real-time attack protection
  - Reputation based protection: malicious IPs, anonymous proxies
  - Prevent access to the admin pages by external users

- Example: According to CVE details, XSS is the most commonly reported vulnerability in SharePoint.

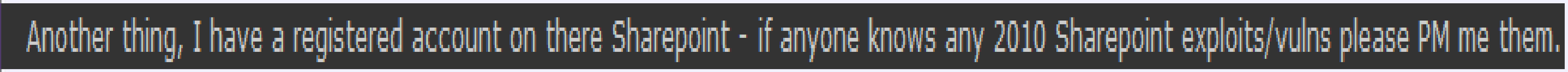
Patch Protection

InfoWorld (2010):

“Admins report that a new Microsoft patch is causing SharePoint servers to fall over – and getting them back up isn’t easy”

http://www.infoworld.com/t/application-security/june-black-tuesday-patch-causes-sharepoint-woes-510

What Do Hackers Think?



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

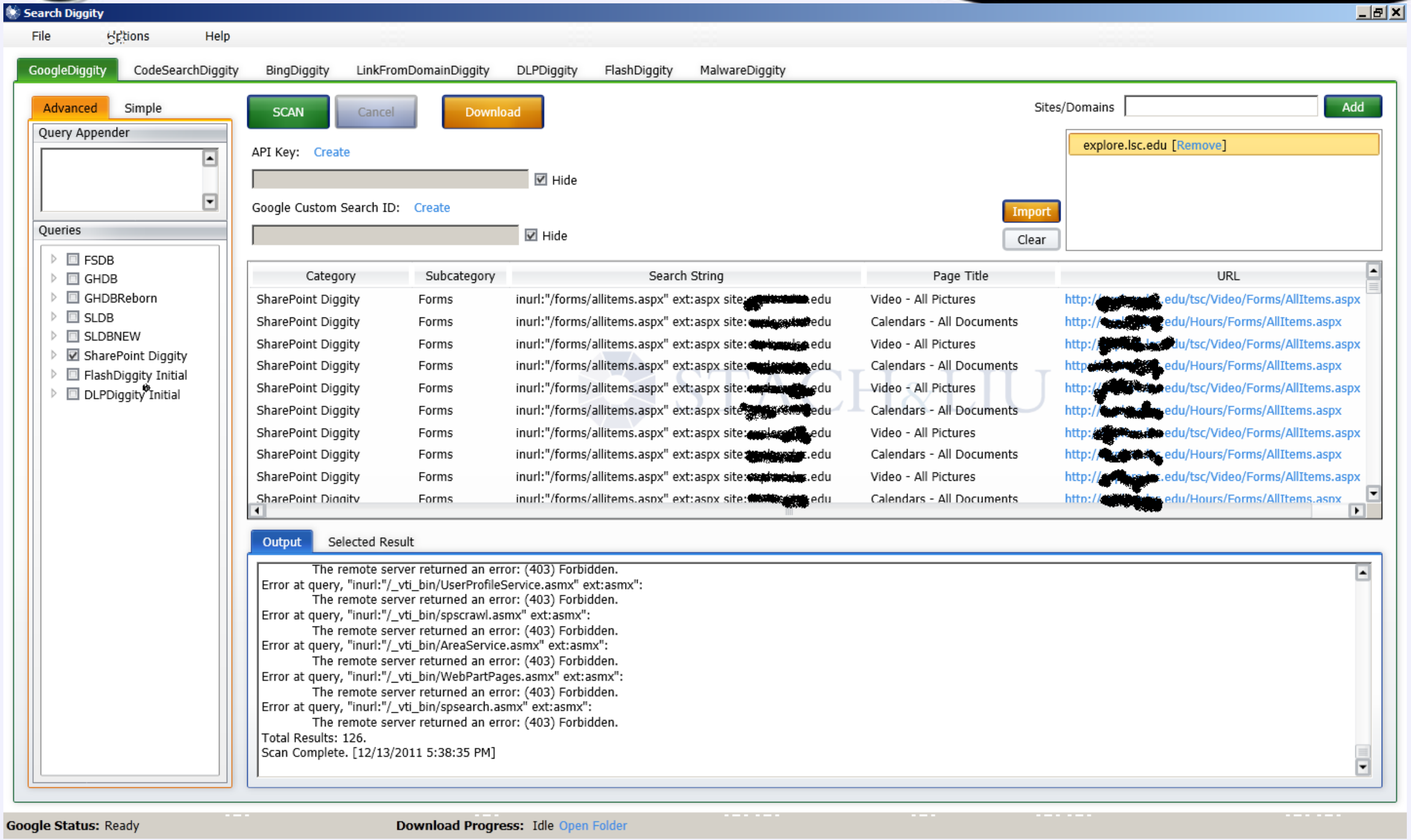
Example: April 2010, Microsoft reveals a SharePoint issue

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/

Google Diggity Project

OWASP
The Open Web Application Security Project



API Key: Create

☑ Hide

Google Custom Search ID: Create

☑ Hide

Sites/Domains

explore.lsc.edu [Remove]

- □ FSDB
- □ GHDB
- □ GHDBReborn
- □ SLDB
- □ SLDBNEW
- ☑ SharePoint Diggity
- □ FlashDiggity Initial
- □ DLPDiggity Initial

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]u/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

```
          The remote server returned an error: (403) Forbidden.
Error at query, "inurl:"/_vti_bin/UserProfileService.asmx" ext:asmx":
          The remote server returned an error: (403) Forbidden.
Error at query, "inurl:"/_vti_bin/spscrawl.asmx" ext:asmx":
          The remote server returned an error: (403) Forbidden.
Error at query, "inurl:"/_vti_bin/AreaService.asmx" ext:asmx":
          The remote server returned an error: (403) Forbidden.
Error at query, "inurl:"/_vti_bin/WebPartPages.asmx" ext:asmx":
          The remote server returned an error: (403) Forbidden.
Error at query, "inurl:"/_vti_bin/spsearch.asmx" 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

#4: Monitor and Protect the SharePoint Database

- Summary:
  - The SharePoint database holds all configuration and content information
  - SharePoint administrators have full access to all SharePoint content
  - Whoever gains direct access to the database have full control on SharePoint
- Why challenging?
  - *The SQL Server database isn't properly secured.*
  - *No activity monitoring and audit capabilities*
  - *No built-in database policy prevention*
- What is Required?
  - Full audit trail of all activity originated from sources other than the application servers.
  - Protection from direct manipulation to the SharePoint internal database

Database Protection

Microsoft Support:
"Database modifications may results in a unsupported database state"
http://support.microsoft.com/kb/841057

Gartner (Securing SharePoint, February 2009):
"Fully audit all SQL Server administrative activities"
Security Considerations and Best Practices for Securing SharePoint

#5: Respond to Suspicious Activity

- Summary:
  - SharePoint is used as a place to share information
  - Access is granted to internal and external users
  - 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
- What is Required?
  - Policy framework to identify suspicious behavior

- Example: In the Wikileaks scenario, Manning used an automated process to crawl the SharePoint system and to siphon out available files. A simple policy on ***occurrences*** would have alerted if a certain number of files were touched in a short timeframe.

A Checklist to Securing SharePoint

Get ahead of all SharePoint deployments

- Implement a SharePoint governance policy.
- Define security requirements before deployment
- 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.
- Secure sensitive data held in files

A Checklist to Securing SharePoint

Manage User Rights

- Manage permissions on a need-to-know basis.
- Identify and delete dormant users
- Prevent the use of direct permissions to users
- Avoid managing permissions at the item level
- Use claims authentication for external users for better control
- Involve data owners in the review process.

Protect Web sites

- Protect your SharePoint applications from web attacks
- Log all failed login attempts.
- Identify suspicious activity
- Prevent access to admin pages by external users

Monitor and Protect the Database

- Audit all administrative activity.
- Prevent access from external sources
- Prevent direct manipulation of the content
- Check for data leakage

Enable auditing for compliance and forensics

- Review who accessed data, when and what they accessed
- Identify who owns the data
- Report on repeated failed login attempts
- Create compliance reports

Questions

https://www.surveymonkey.com/s/Research12_TsvikaKlein