



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

August 12, 2010



ISOAG August 2010 Agenda

- | | | |
|------|-----------------------------------------------------------------------------|---------------------------------------|
| I. | Welcome & Opening Remarks | John Green, VITA |
| II. | Security Inside Out: Protection of Our Databases, Middleware & Applications | Denise Mallin, ORACLE |
| III. | Keystroke Logging & URL Capture: Making Private Information Public | Bob Baskette, VITA
Eric Taylor, NG |
| IV. | 2010 COV Security Annual Report | John Green, VITA |
| V. | Upcoming Events & Other Business | John Green, VITA |
| VI. | Partnership Update | Don Kendrick, VITA |



ORACLE®

Security Inside Out:
Protection for Databases, Middleware, and Applications
An End-to-End Approach to Security Architecture

Denise Mallin, CISSP
Principal Sales Consultant, Oracle Public Sector

Agenda

- What Security Challenges Are Our Customers Facing?
 - Business Drivers
 - Threats
 - Risk Management
 - Sustainable Compliance

- An "End-to-End" Security Architecture
 - Presentation Tier
 - Logical (Application) Tier
 - Data Tier
 - Issues that Span the Tiers

Business Requirements for IT Security



Managing
Security & Risk



Flexible and
Business-Driven



Sustaining
Compliance

How is Data Compromised?

Source: Verizon 2010 Data Breach Investigations Report

WHO IS BEHIND DATA BREACHES?

70% resulted from external agents (-9%)

48% were caused by insiders (+26%)

11% implicated business partners (-23%)

27% involved multiple parties (-12%)

Including the USSS cases in this year's report shook things up a bit but didn't shake our worldview. Driven largely by organized groups, the majority of breaches and almost all data stolen (98%) in 2009 was still the work of criminals outside the victim organization. Insiders, however, were more common in cases worked by the USSS, which boosted this figure in the joint dataset considerably. This year's study has by far improved our visibility into internal crime over any other year. Breaches linked to business partners continued the decline observed in our last report and reached the lowest level since 2004.

Related to the larger proportion of insiders, Misuse sits atop the list of threat actions leading to breaches in 2009. That's not to say that Hacking and Malware have gone the way of the dinosaurs; they ranked #2 and #3 and were responsible for over 95% of all data comprised. Weak or stolen credentials, SQL injection, and data-capturing, customized malware continue to plague organizations trying to protect information assets. Cases involving the use of social tactics more than doubled and physical attacks like theft, tampering, and surveillance ticked up several notches.

HOW DO BREACHES OCCUR?

48% involved privilege misuse (+26%)

40% resulted from hacking (-24%)

38% utilized malware (<>)

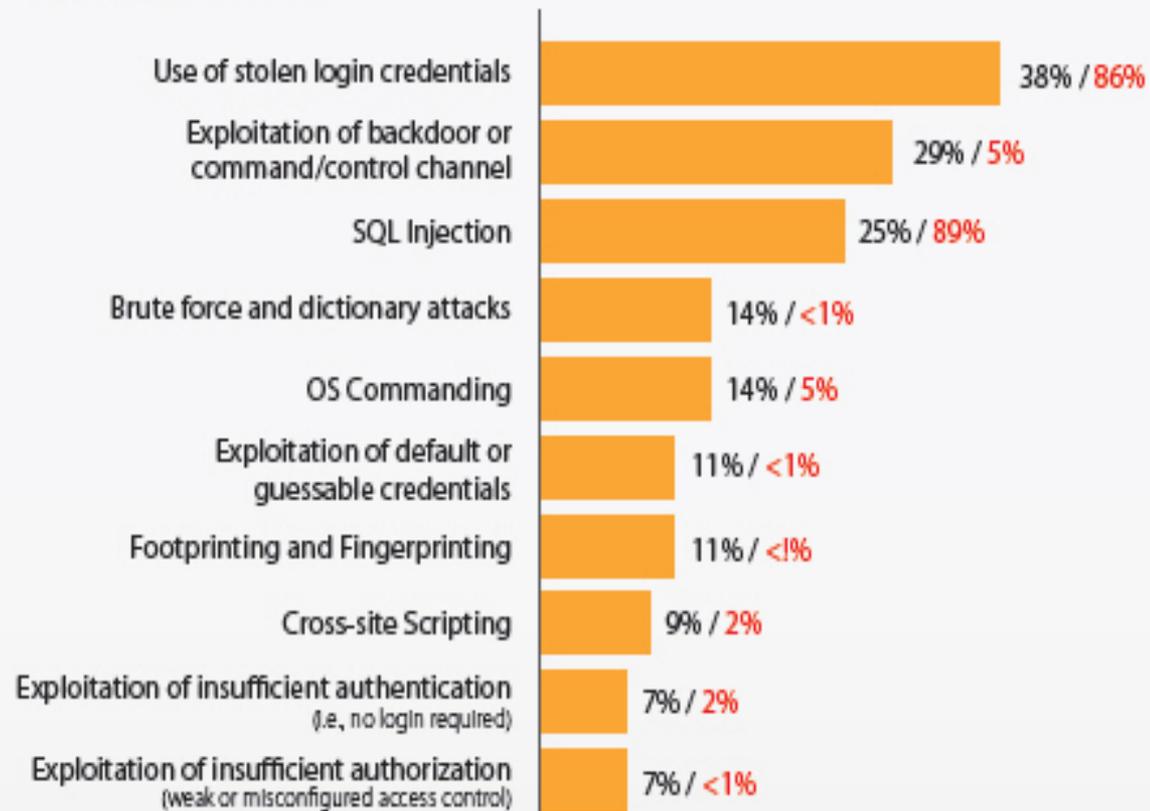
28% employed social tactics (+16%)

15% comprised physical attacks (+6%)

How is Data Compromised?

Source: Verizon 2010 Data Breach Investigations Report

Figure 21. Types of hacking by percent of breaches within Hacking and percent of records



Managing Risk

Threats Faced



- Security Silos
- Orphaned Accounts
- Phishing, Keylogging, MITM
- Insider Threats

Business Impact



- Data breaches
- Fraud
- Remediation Costs
- Headlines
- Citizen Trust

Mitigate with

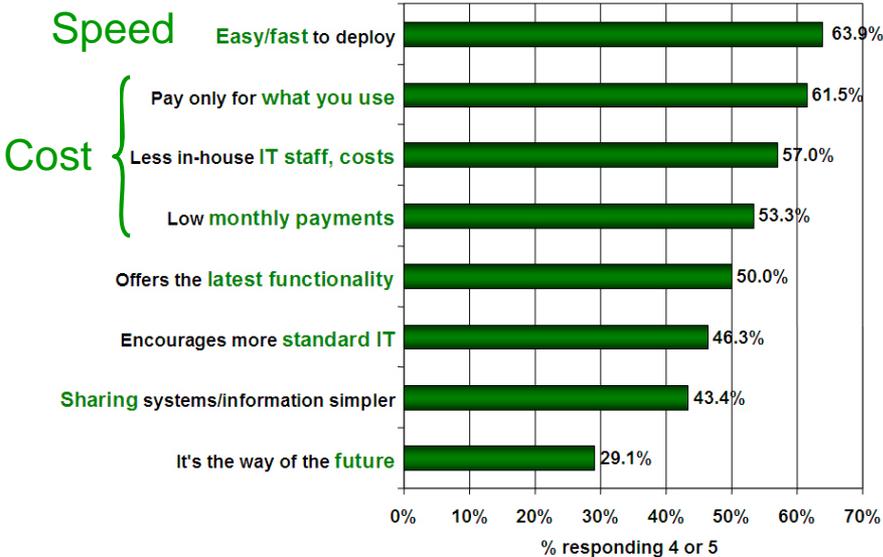


- Controls Management & Enforcement
- Comprehensive Identity and Access Management
- Comprehensive Data Protection
- Boundary Protection

Why Are Enterprises Interested in Cloud? What Are the Challenges Enterprises Face?

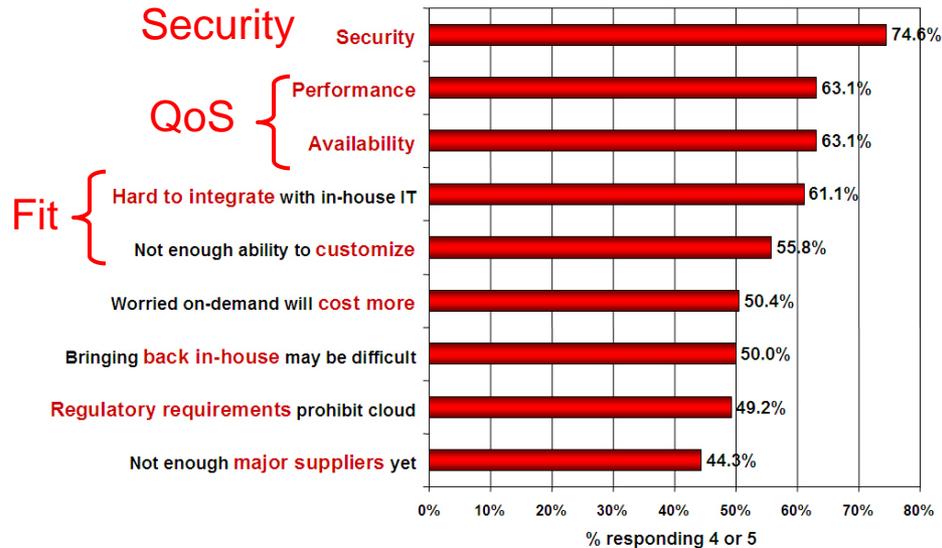
Benefits

Q: Rate the **benefits** commonly ascribed to the 'cloud'/on-demand model
(1=not important, 5=very important)



Challenges/Issues

Q: Rate the **challenges/issues** ascribed to the 'cloud'/on-demand model
(1=not significant, 5=very significant)



Source: IDC eXchange, "IT Cloud Services User Survey, pt. 2: Top Benefits & Challenges," (<http://blogs.idc.com/ie/?p=210>), October 2, 2008

Why Does Compliance Matter?

- More public sector regulations
 - Breach notification laws
 - HIPAA Enforcement Actions
 - PCI as a state standard
- More accountability
 - Credit monitoring
 - Civil restitution
- More attack vectors

More Breach Notification Laws -- 42 States and Counting

Feds finally put teeth into HIPAA enforcement

Three years after the federal law's rules on securing health care data took effect, HHS has issued its first enforcement action plan. And more

House Passes Identity Theft & Restitution Act

Senate to consider bill that addresses data theft, use of keyloggers and spyware

Companies May Be Held Liable for Deals With Terrorists, ID Thieves

New and little-known regulations could mean fines, or even jail time, for comp

FTC Deal Suggests

Enterprises Could Be Liable for Poor Security

ValueClick found negligent when Commission discovers vulnerabilities contrary to privacy policies promising encryption and 'reasonable security measures'

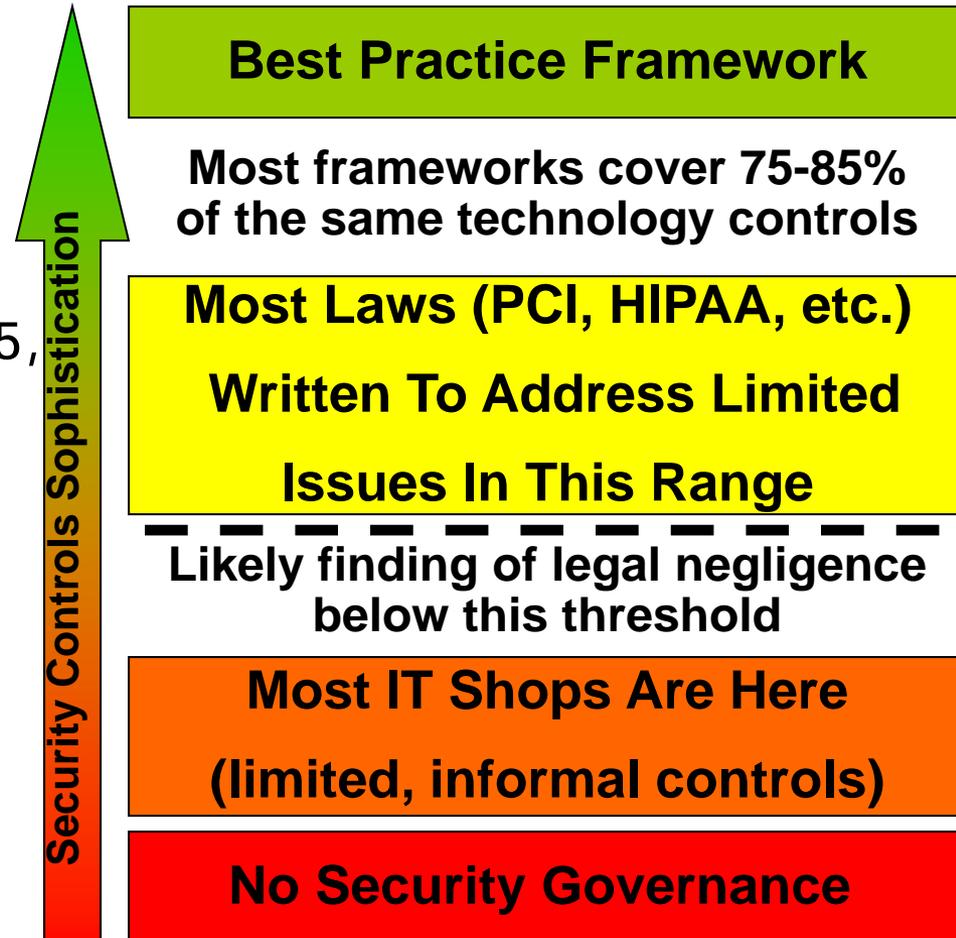
A quarter of US PCs infected with malware: OECD

Report: Website Infection Rate Has Tripled Since 2007

Malicious Web pages now exceed more than 16,000 per day, Sophos says

Overlap in Frameworks & Compliance

- Compliance concerns
 - HIPAA
 - PCI
 - SB 1386 (Breach Notification)
 - Industry Specific (SOX, IRS 1075, FERPA, CFR 28, etc...)
- Frameworks
 - ISO 27001/2
 - ITIL
 - COSO/COBIT
 - FISMA (NIST 800-53)
 - CMMI and others...

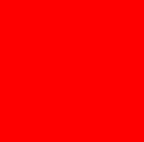


Common Deficiencies Found by Auditors

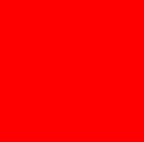
- **Delay in terminating access:**
 - Auditors check how long it takes between when an employee leaves a company and when all his or her access privileges are turned off.
- **Built up privileges over time:**
 - Auditors know that people often change jobs within the company. They also know that it is less common to reduce access than to grant it. Auditors check whether employees have more access than they need to do their current job.
- **Access transactions in conflict:**
 - Auditors are looking for employees who have access to systems that are in conflict with business rules. A classic example of this is when a user can specify vendors for payment in one system, and can issue payment to that same vendor in another.
- **Uncontrolled access authorizations:**
 - Auditors look for a controlled business process for granting and denying access privileges. If your system for provisioning access privileges is a series of random e-mails between business managers and the IT department, auditors see a red flag
- **Lax password policy enforcement:**
 - Auditors want to see that all key systems are guarded by a manageable, enforceable password policy.



5 Questions to ask yourself...



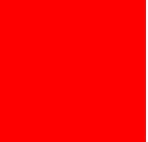
1. Do you always know
when a security breach
has occurred?



2. How many ex-employees
and ex-contractors still
have access to your
systems?



3. Do your DBAs know you got a promotion before you do?

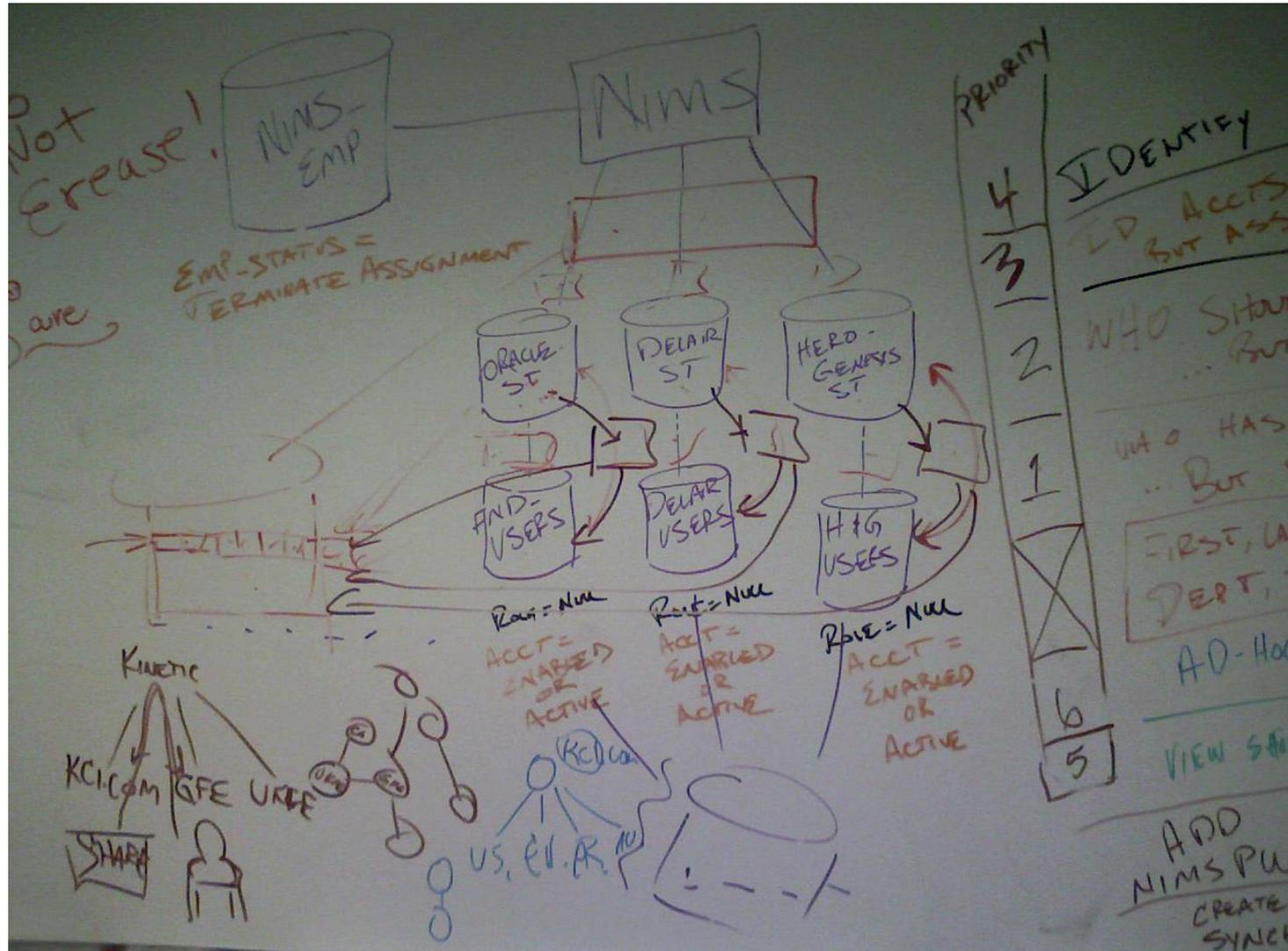


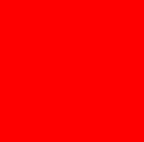
4. Can you guarantee protection of your employee and citizen personal information?



5. How much are manual compliance controls costing your organization?

To fix this problem...We create 'Solutions'





Introduction to A Best Practice, End-to-End Security Strategy

The Goals of a Best Practice Security Strategy

Simplify GRC while Reducing Cost

Safeguard Reputation and Trust

Run Your Organization Better and Prove It

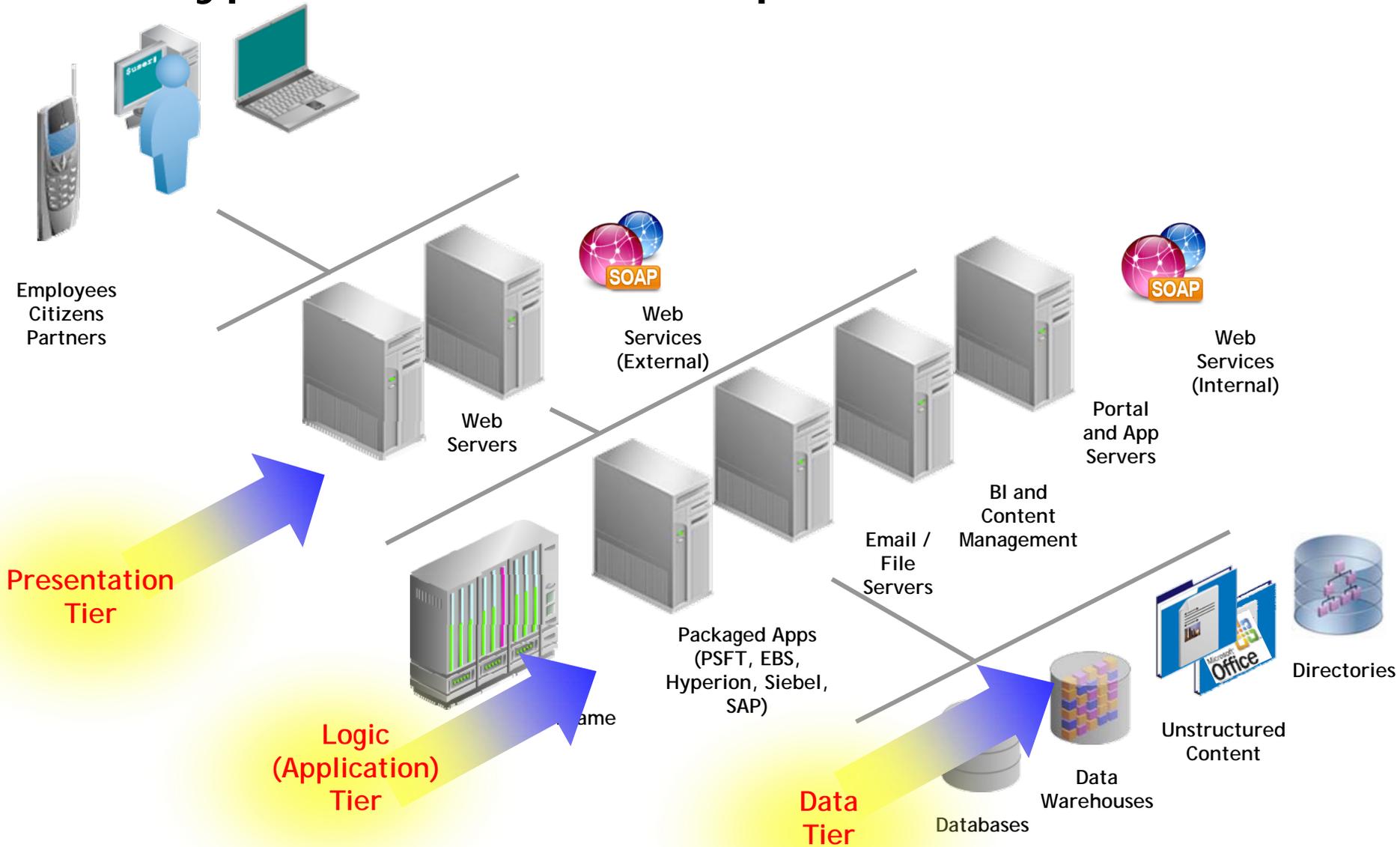
What Have Our Customers Asked For?

Automate and Centralize Security and Compliance



- Simplify the Sign On process for end users
- Manage 'Who has access to What, When, How and Why' for FISMA, SOX, FFIEC, GLBA, HIPAA and PCI compliance
- Automate On-boarding, Termination and Job Transfer processes for tighter security
- Detect and remediate fraudulent activities against both outside and inside threats
- Enforce separation of duties and Chinese Wall regulatory mandates
- Protect Data from compromise

A Typical "3-Tier" Enterprise Environment



A Typical Transaction



Emplo
 Cust
 Part

Pres
 Tier

Logic
 (Application)
 Tier

Mainframe

Packaged Apps
 (PSFT, EBS,
 Hyperion, Siebel,
 SAP)

Data
 Tier

Databases

Data
 Warehouses

Unstructured
 Content

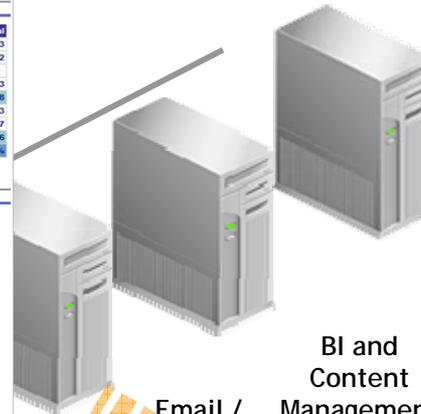
Directories

Portal
 and App
 Servers

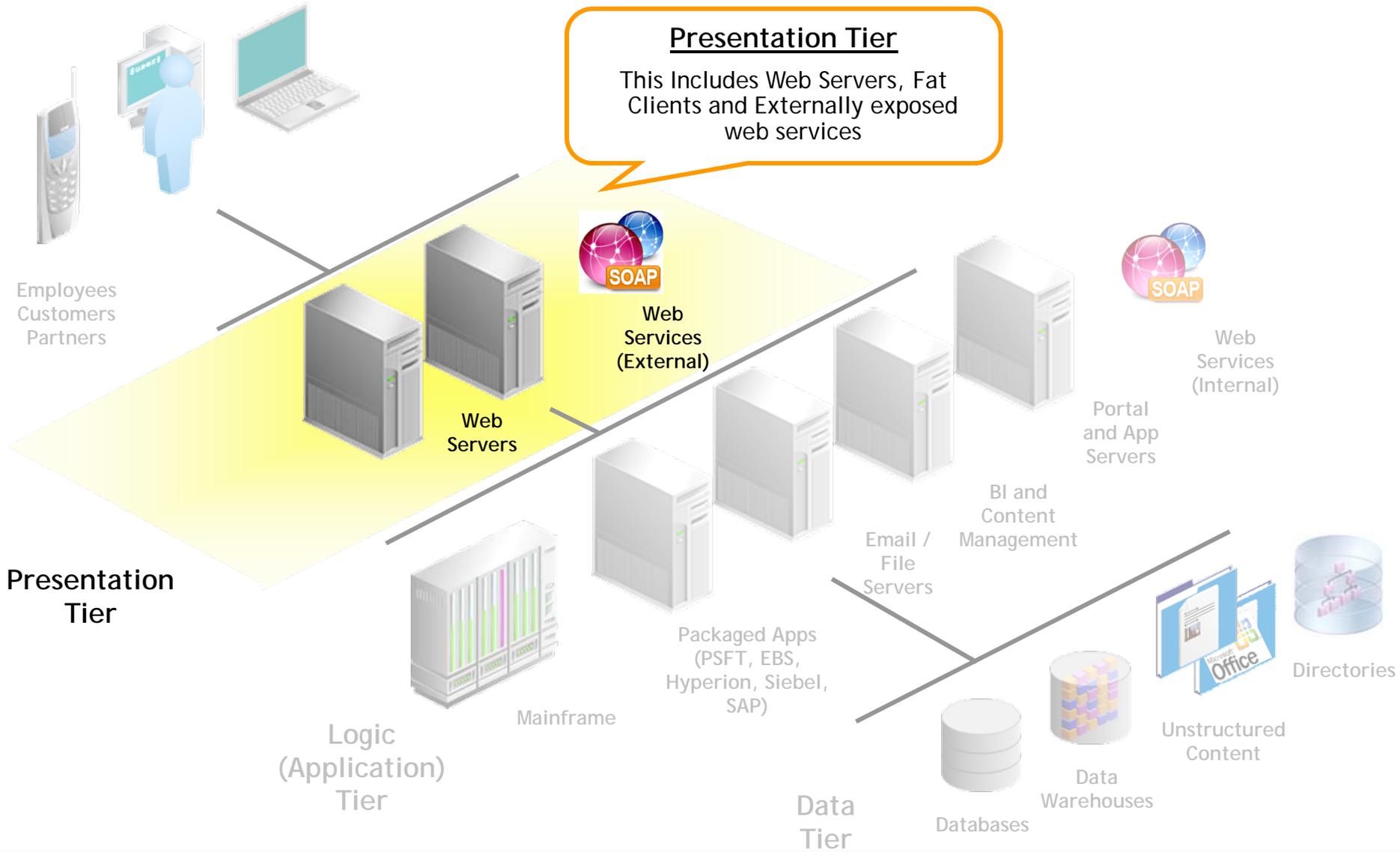
Web
 Services
 (Internal)

Email /
 File
 Servers

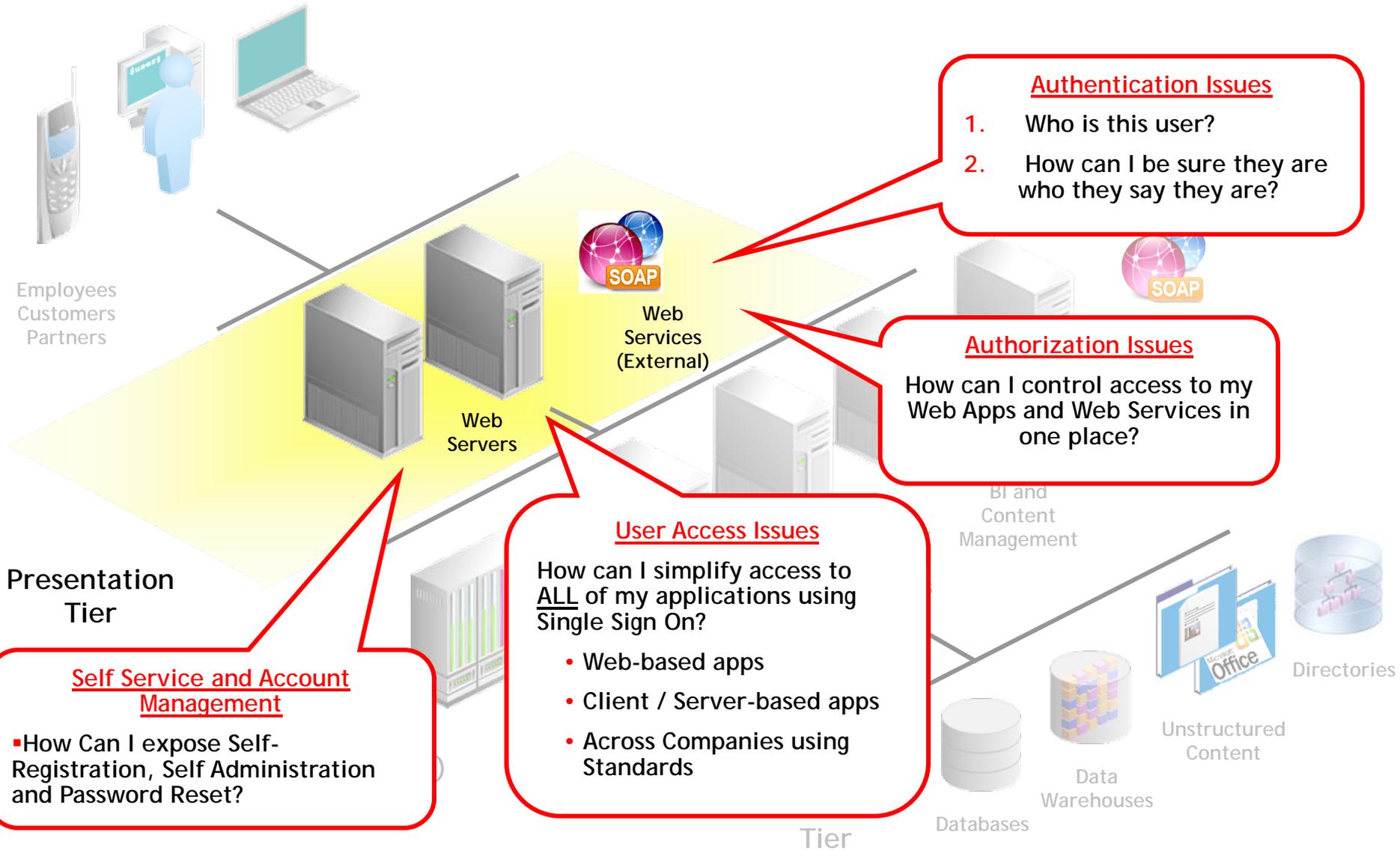
BI and
 Content
 Management



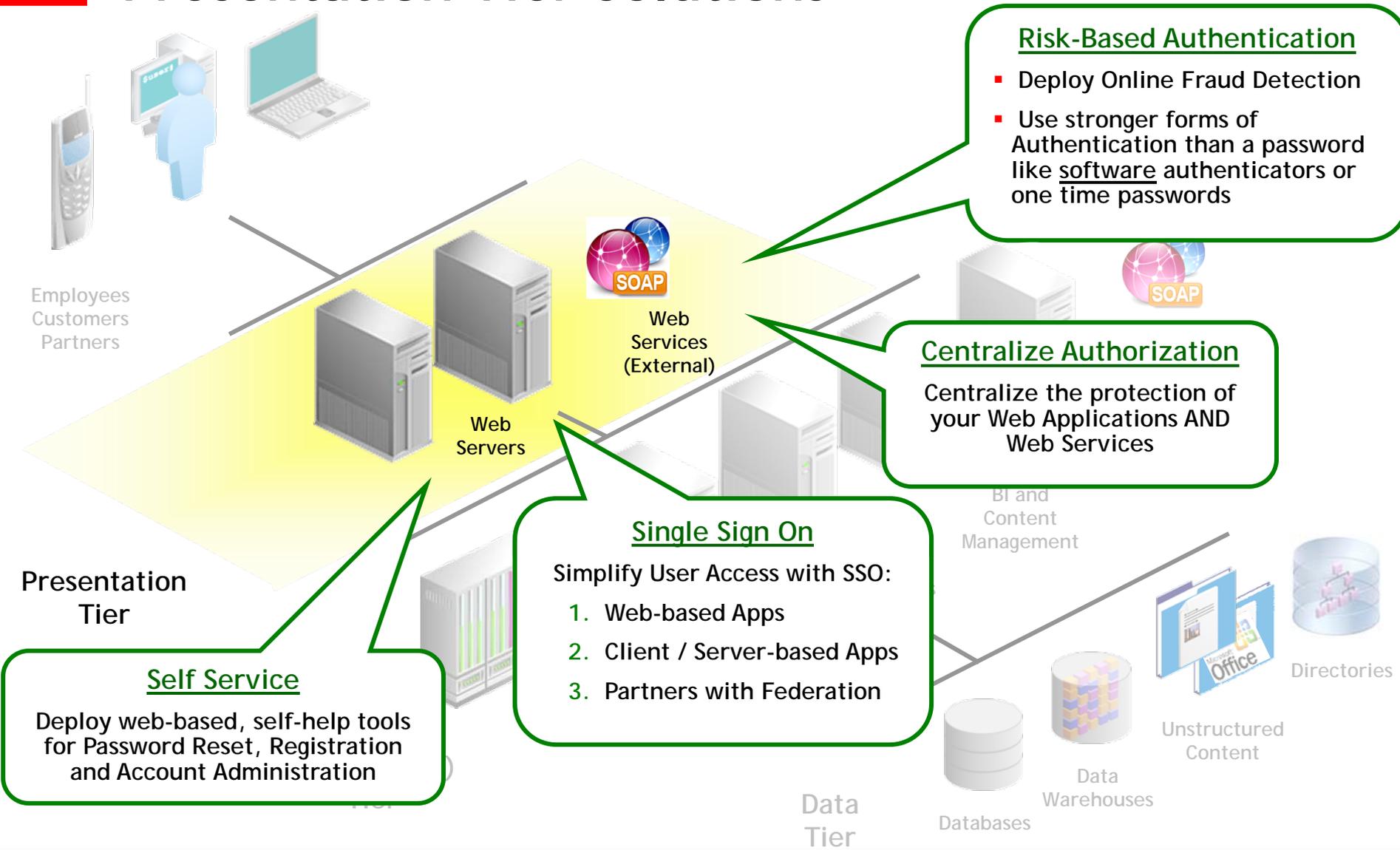
Presentation Tier



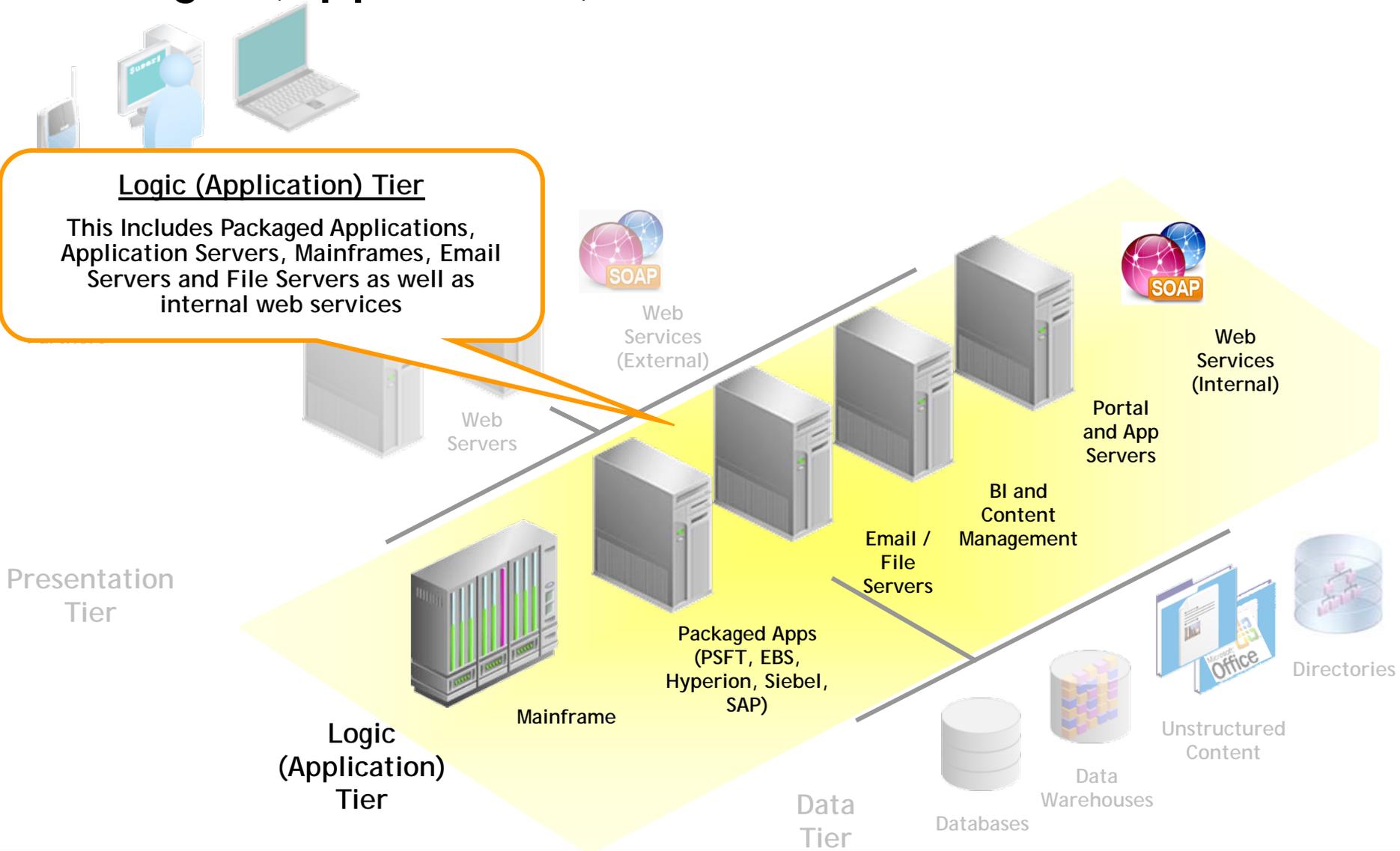
Presentation Tier Issues



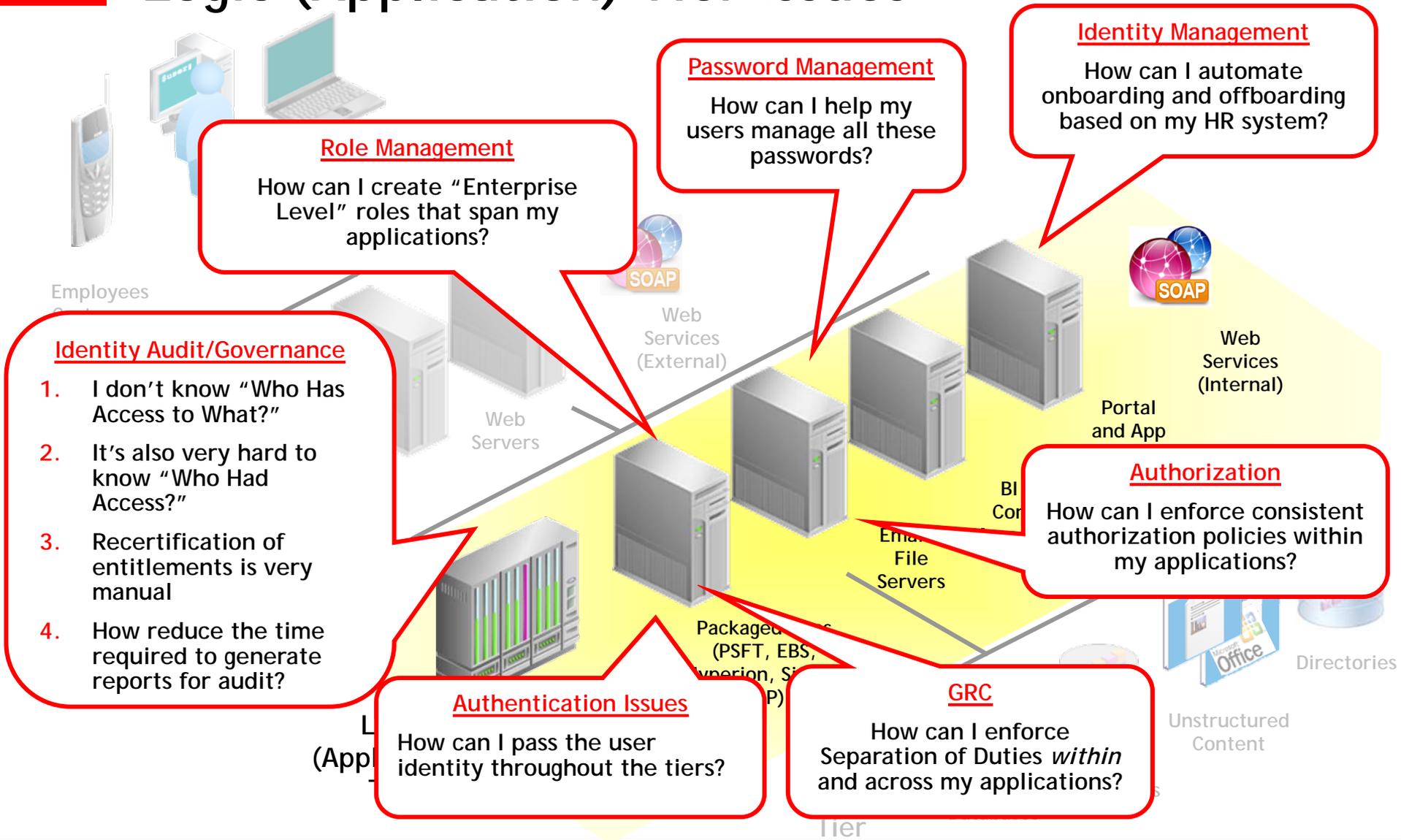
Presentation Tier Solutions



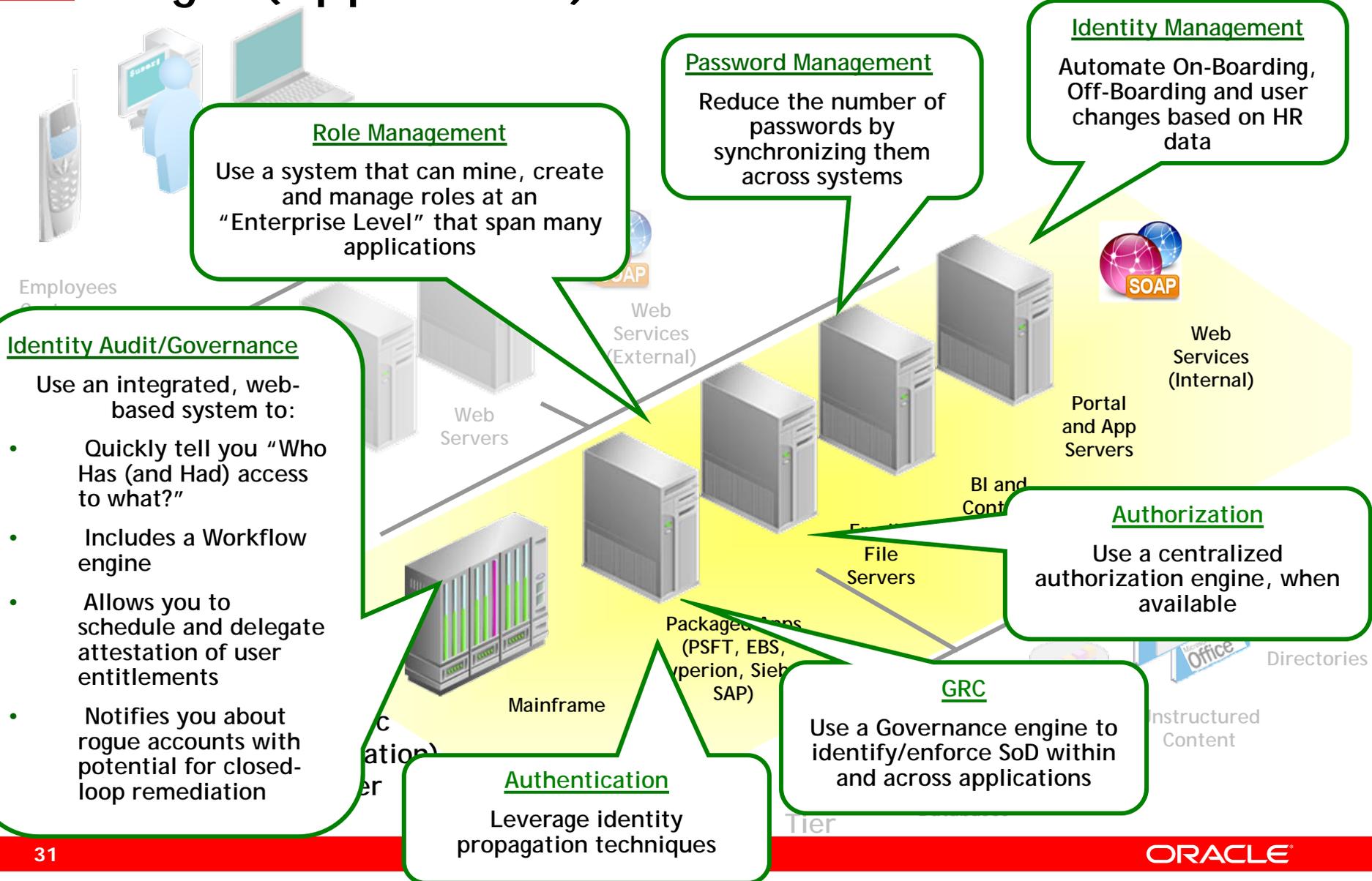
Logic (Application) Tier



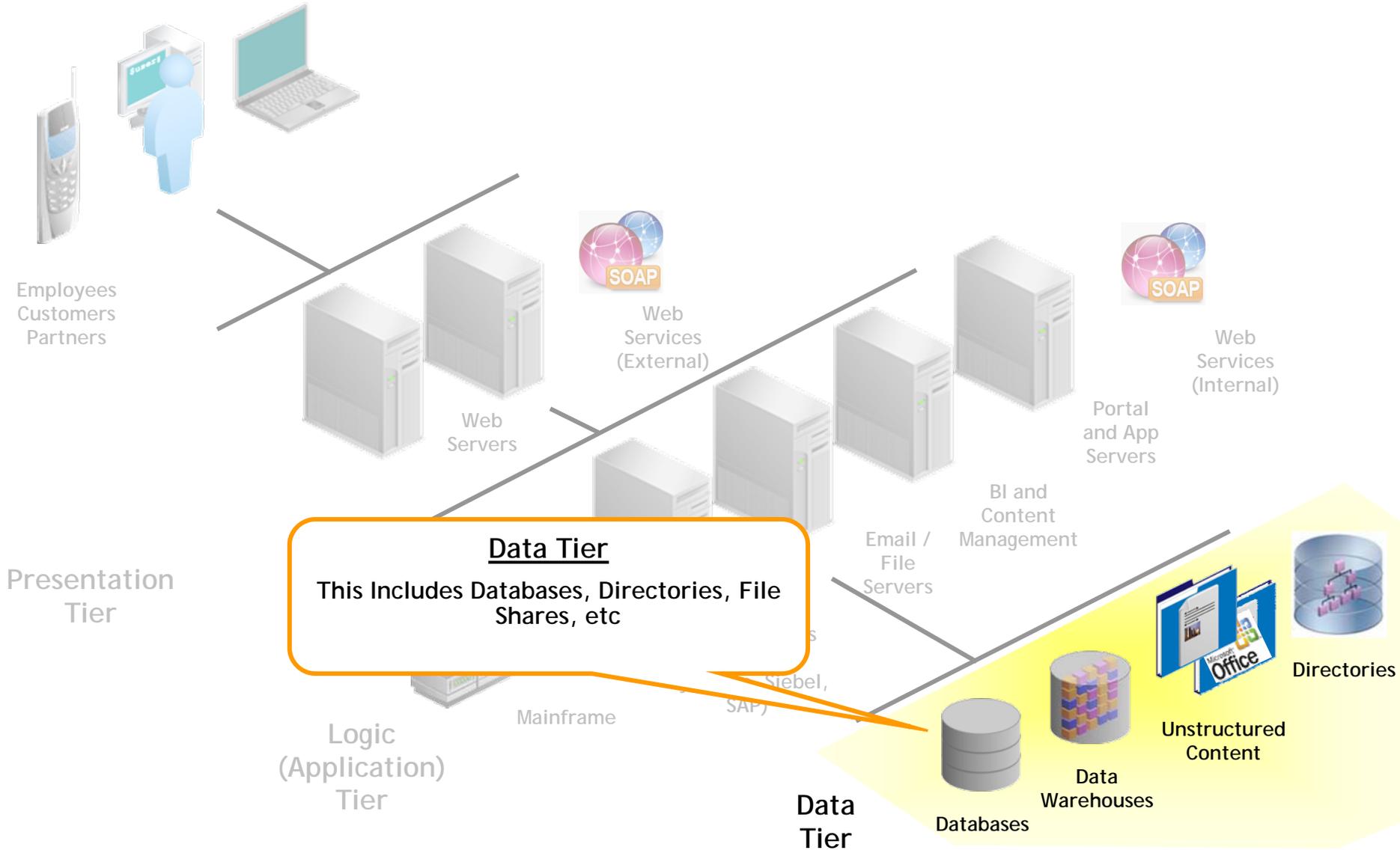
Logic (Application) Tier Issues



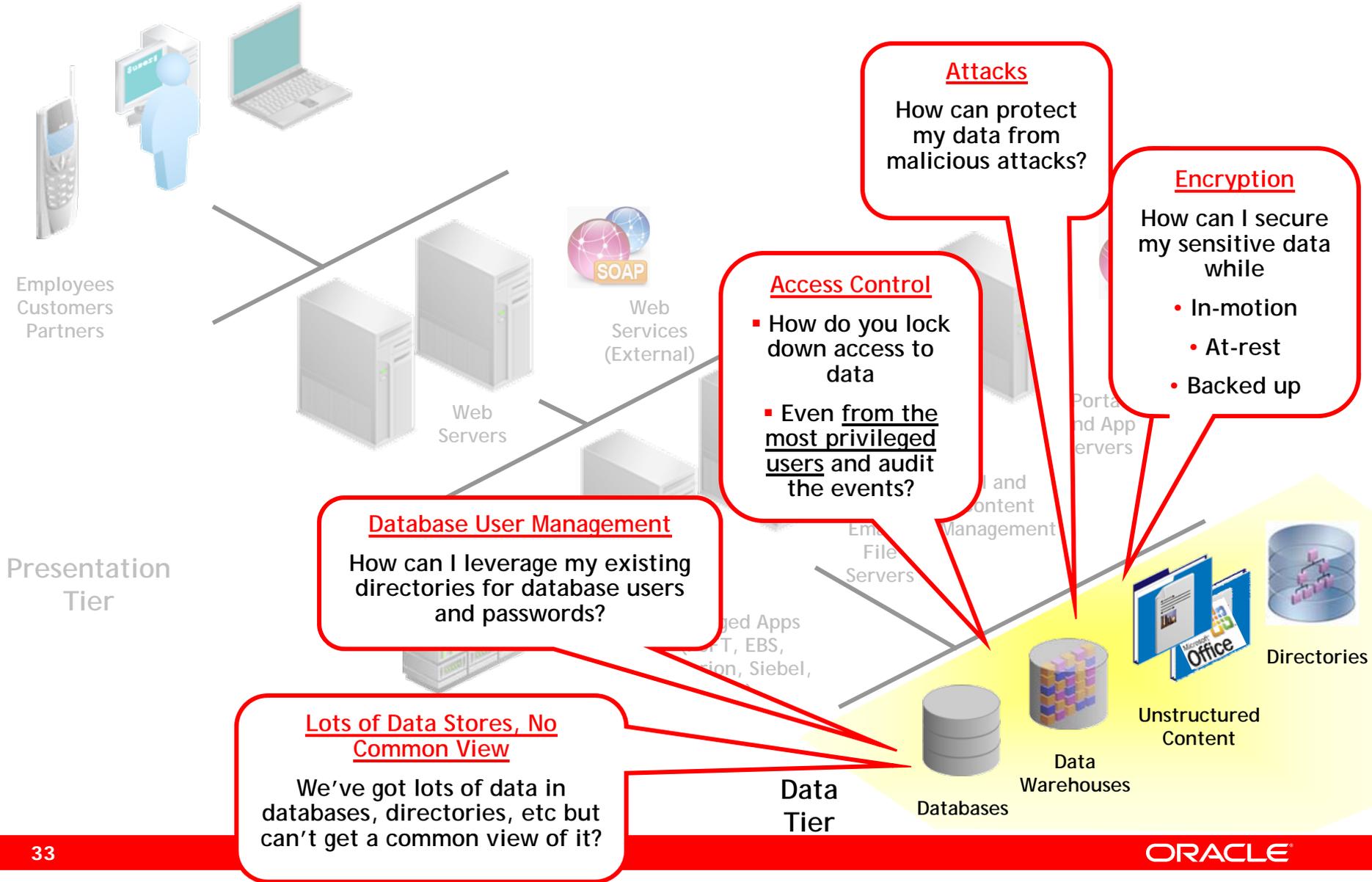
Logic (Application) Tier Solutions



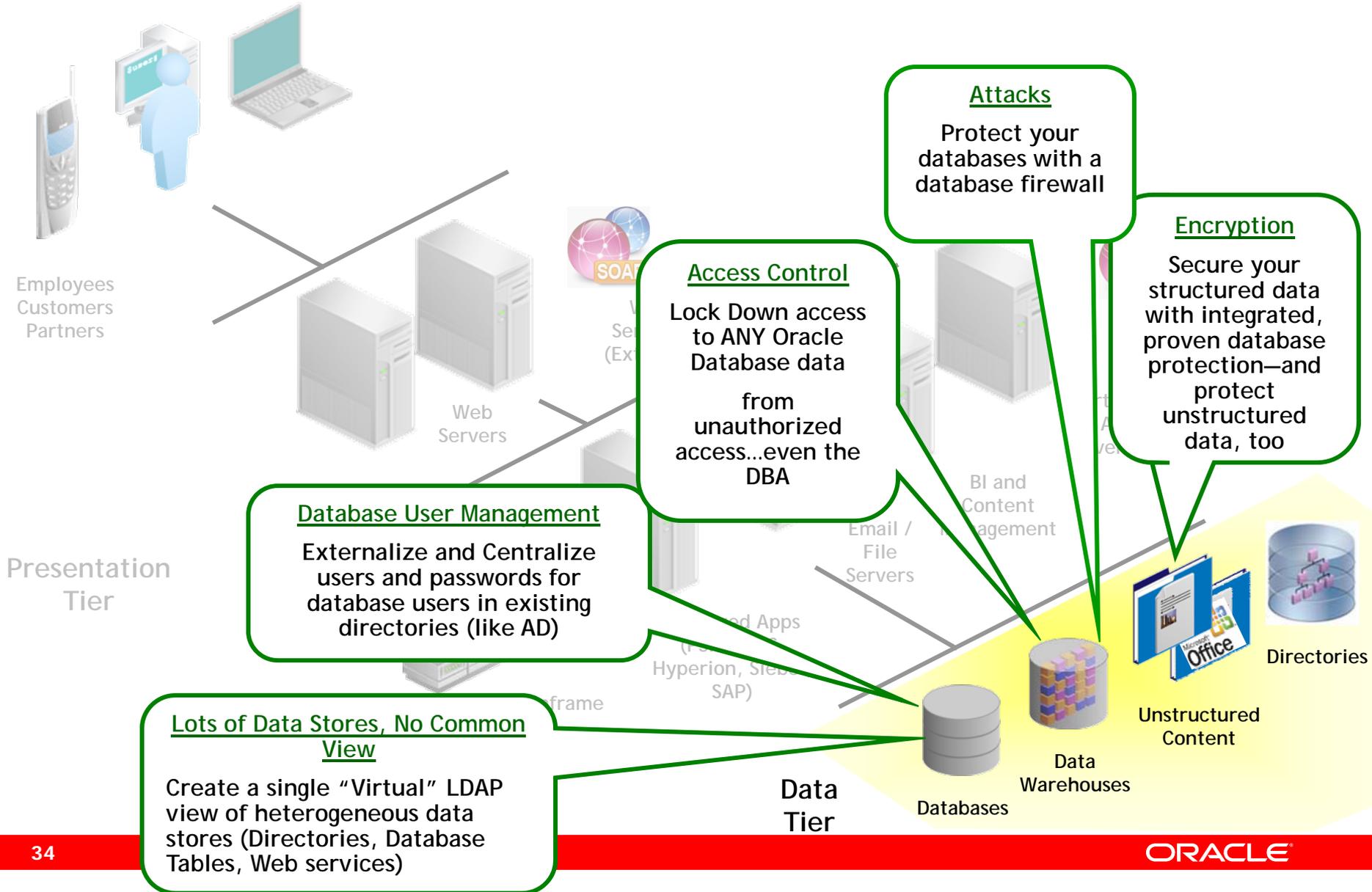
Data Tier



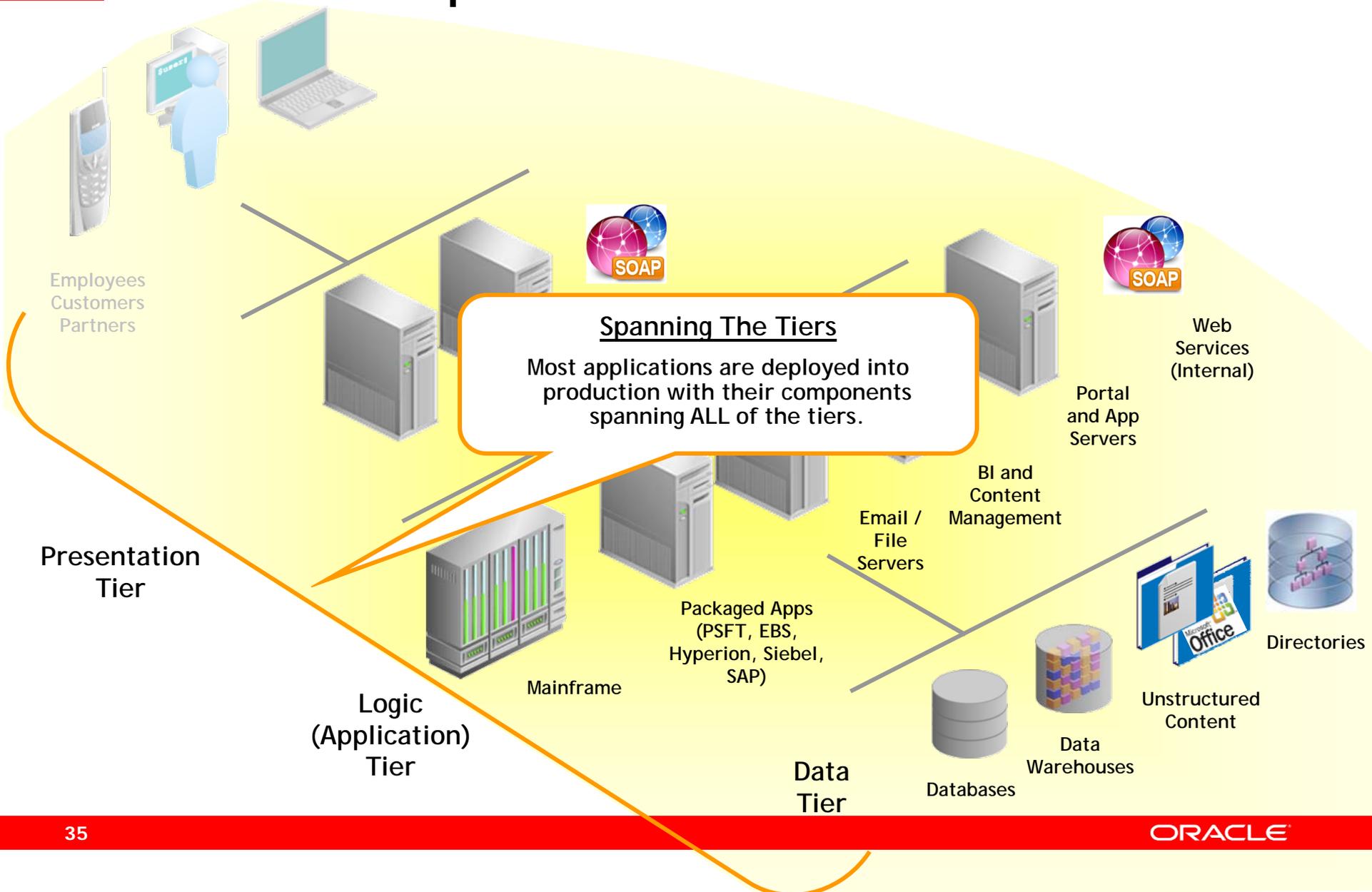
Data Tier Issues



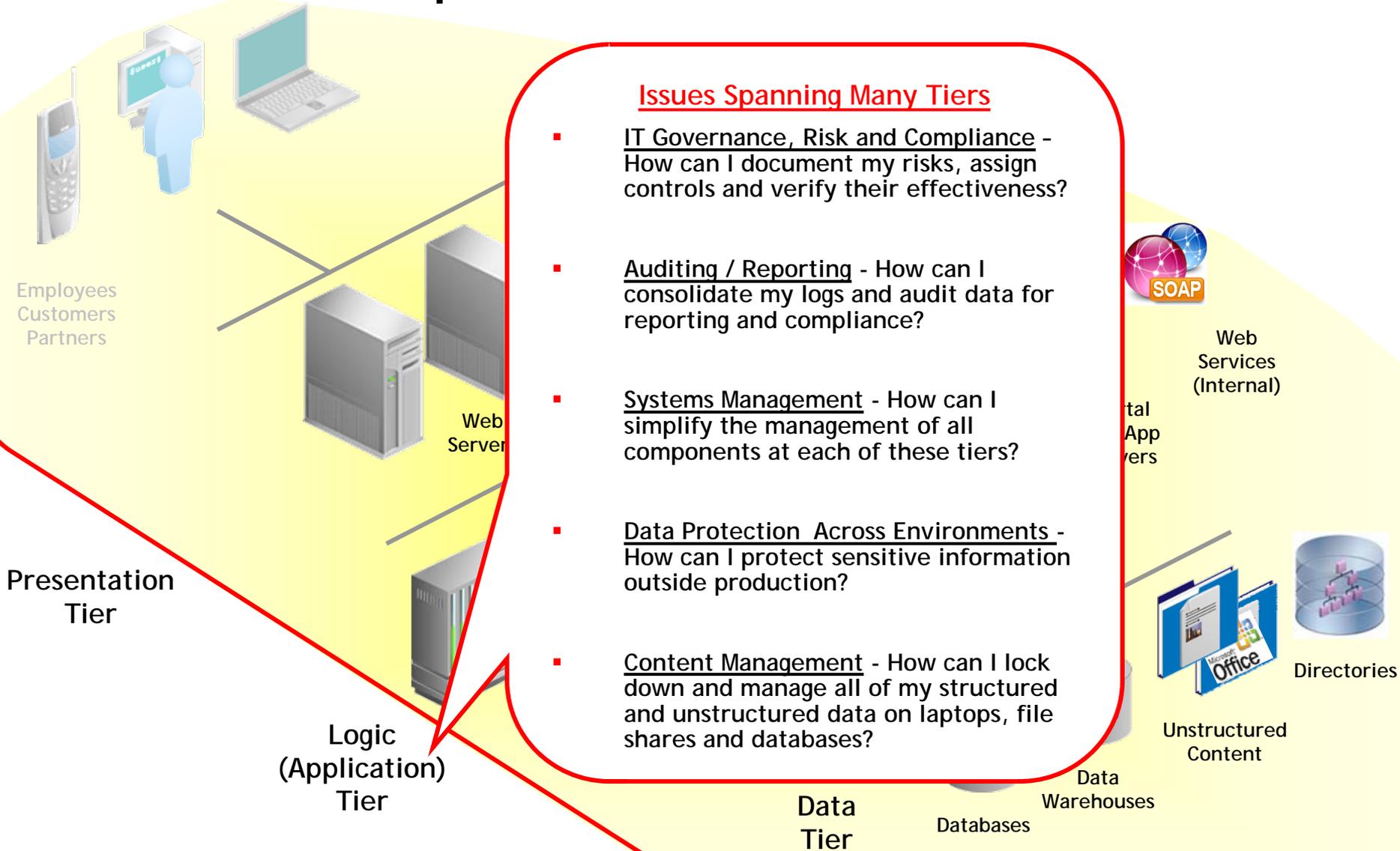
Data Tier Solutions



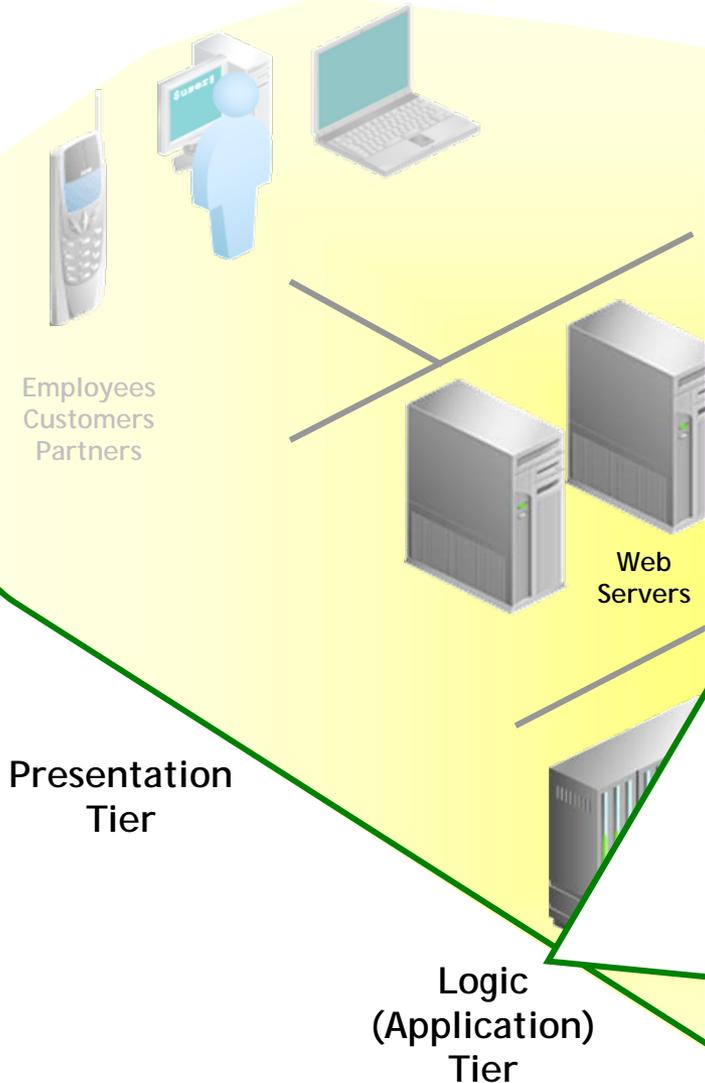
Issues that Span The Tiers



Issues that Span The Tiers



Solutions to Issues that Span



"Monitor and Manage"

- Establish a "Top Down, Risk-based" Approach to Compliance, Risk and Governance using an automated system
- Centralize your log and audit data into a Secure Audit Data Warehouse for reporting and compliance purposes
- Centrally manage and monitor (e.g., performance, availability, configuration, patching) your web servers, application servers, databases, through a "single pane of glass"
- Securely Move Sensitive Data between Production, Dev and Test with data masking
- Manage and assign rights to ALL of your secure unstructured data with Content Management, Data Loss Prevention, and Information Rights Management
- Protect the boundaries and end points

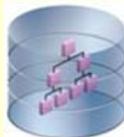


Web Services (Internal)

s
p
s



Unstructured Content

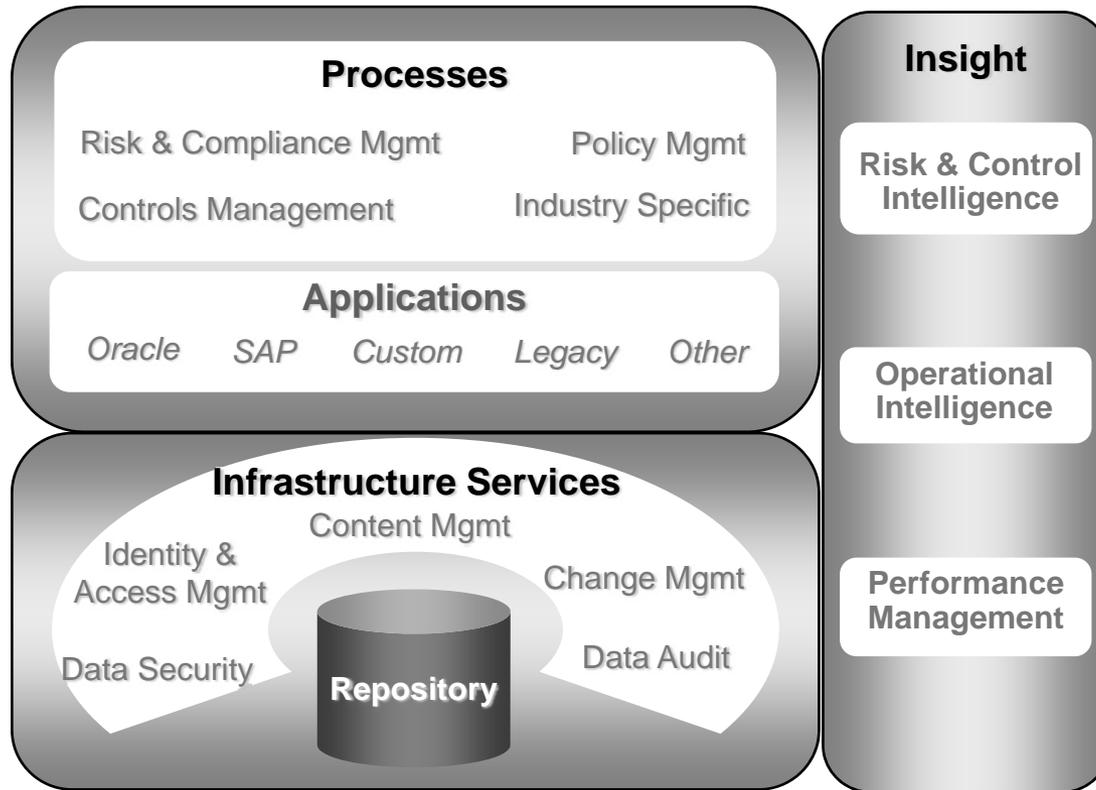


Directories

s

Enterprise-wide GRC Platform

Select a comprehensive platform for Governance,
Risk and Compliance Management



Summary—Apply Best Security Principles

- Defense in Depth: at all tiers, across environments
- Data protection to ensure confidentiality, integrity, and availability
- Apply access control
 - Separation of duties
 - Enforce least privilege
 - Strong authentication
 - Consistent authorization
- When possible, shift from people/process controls to technology for consistency, auditability, and efficiency
- Look for standards-compliant technology that supports a heterogeneous environment

Questions



Denise.Mallin@oracle.com

www.oracle.com



Keystroke Logging and URL Capture: Making Private Information Public

Bob Baskette

CISSP-ISSAP, CCNP/CCDP

Commonwealth Security Architect

Eric Taylor

Northrop Grumman Security Architect



Malicious Software Definitions

- Virus = A computer program that can generate multiple copies of itself as well as infect a computer system without the knowledge of the system owner.
- In order to replicate, a virus must execute malicious code. Much like in nature, a computer virus is inert and cannot perform its malicious mission until it is inserted into a host file (some type of executable code).
- A virus can only spread from one computer system to another computer system when its host file is first transferred to the target computer system. The most common methods for virus transmission are via a network connection or removable medium such as a CD/DVD or USB drive.



Virus Types Based on Behavior

- Viruses types based on execution behavior.
 - Nonresident viruses
 - Begin searching for target hosts to infect as soon as the virus is activated.
 - Once the target is infected, the virus will transfer control to the application program it infected.
 - Resident viruses
 - Resident virus loads itself into memory upon execution and transfers control to the host program.
 - The virus will stay active in memory and will infect new host files only when those files are accessed by other programs or the operating system itself.
 - Nonresident viruses have a finder module and a replication module
 - The finder module is responsible for finding new files to infect.
 - The replication module is responsible for actually infecting the file.
 - Resident viruses contain only a replication module
 - Resident viruses contain a replication module, but not a finder module since the replication module is executed each time the operating system is called to perform a certain operation.



Malicious Software Definitions

- Worm = A self-replicating computer program which will exploit security vulnerabilities to spread itself to other computer systems without the need to be transferred as part of a host file.
- A worm can utilize either a network connection or removable media to propagate to other computer systems.
- This propagation can occur as a system background task and usually does not require user interaction.
- Worms almost always cause some disruption to the network (normally consuming bandwidth) whereas a virus will corrupt or destroy files on a targeted computer system.
- Most worms will either carry a "Payload" or download the "Payload" once the worm has taken control of the computer system. A popular payload for a worm is a "Backdoor" program to allow the creation of a "zombie", which will be controlled by the worm author.



Malicious Software Definitions

- Trojan horse (AKA Trojan) = A computer program that appears to perform a desirable function but in fact performs a malicious function.
- Trojan programs allow unauthorized access to the host computer, providing the malicious individual the ability to save files on the compromised computer or capture data processed on the compromised computer.
- The six main types of Trojan horse payloads are:
 - Remote Access
 - Data Destruction
 - Downloader/dropper
 - Server Trojan (Proxy, FTP , IRC, Email, HTTP/HTTPS, etc.)
 - Disable security software
 - Denial-of-service attack (DoS)



Trojan Programs

- Trojans can communicate via overt or covert channels
- Trojans that communicate via covert channels are classified as Backdoor programs
- Backdoor program is any type of program that will allow an attacker to connect to a computer without going through the normal authentication process



Trojan infection mechanisms

- **Peer-to-Peer Networks (P2P)**
 - Kazaa
 - Imesh
 - Aimster
 - gnutella
- **Instant Messaging (IM)**
- **Internet Relay Chat (IRC)**
- **Email Attachments**
- **Physical access**
- **Software Vulnerabilities**



Trojan's in action

- Let's take a look at a Trojan program in action
 - Delivery – email social engineering
 - Communication – Port 443
 - Run in users context



Keystroke Logging

- Also known as key-logging
- The action of tracking and recording the keys pressed on a keyboard
- Normally performed in a covert manner so that the person using the keyboard is unaware that their keystrokes are being recorded



Keystroke Logging Methods

- Software programs to capture keyboard interrupts
- Hardware devices to capture electronic impulses
- Electromagnetic radiation and Acoustic waveform analysis



Software Keystroke Logging Categories

- Hypervisor-based
- Kernel based
- Hook based
- Passive Method
- Form grabber / URL scraping



Software Keystroke Logging Categories

- Kernel based keystroke logging programs reside at the kernel level
- Operating at the kernel level makes the keystroke logging program difficult to detect and therefore difficult to remove since most anti-virus programs also operate at the Kernel level
- Usually implemented as rootkit keyboard driver to subvert the operating system kernel and gain unauthorized access to the underlying hardware



Software Keystroke Logging Categories

- Hypervisor-based keystroke logging programs reside within a malicious software hypervisor running below the client operating system
- The client operating system is not altered by the malicious software hypervisor since the malicious software remains strictly within the hypervisor
- It effectively becomes a virtual machine



Software Keystroke Logging Categories

- Hook based keystroke logging programs hook or replace the APIs used by applications to subscribe to the keyboard events monitored by the operating system
- Does not replace the kernel level driver but alters the operating system library routines
- The operating system will notify the keystroke logging program each time a key is pressed



Software Keystroke Logging Categories

- Passive method keystroke logging make use of existing API calls such as `GetAsyncKeyState()` and `GetForegroundWindow()` to poll the state of the keyboard or subscribe to keyboard events
- Passive method keystroke logging programs are simple to create and simple to detect since the constant polling of each key can increase the CPU utilization



Software Keystroke Logging Categories

- Form grabber/URL scraping keystroke logging programs capture the information in a form submission by recording the web browsing onSubmit event functions
- The information retrieved from onSubmit event functions is not encrypted since the SSL encryption process occurs at a later stage of the HTTPS protocol



Keystroke Log Transmission

- The collected keystrokes can be transmitted using one of the following four methods:
 - Keystrokes are uploaded to a malicious web server, database server, or FTP server
 - Keystrokes are periodically emailed to a pre-defined email address.
 - Keystrokes are wirelessly transmitted through the use of an attached hardware system.
 - The keystroke logging software contains a remote login shell



Additional Keystroke Logging Techniques

- Clipboard logging
- Screen logging
- Microphone and Webcam recording



Screen Logging / Capture

- Screenshots are taken at regular intervals to capture graphics-based information
- The screenshot can record the entire screen, a specific application window, or the area of mouse focus
- Focusing on the area of mouse control can be used to defeat a web-based keyboard



Acoustic Keystroke Logging

- Acoustic cryptanalysis can be utilized to determine which key was depressed based on the sound created during typing
- Each character on the keyboard will generate a subtly different acoustic signature when depressed
- The keystroke signature to keyboard character mapping can be determined using statistical frequency analysis

Acoustic Keystroke Logging

- The statistical frequency analysis is based upon the repetition frequency of similar acoustic keystroke signatures, the timing differential between different keyboard strokes, and contextual information such as the probable language in use
- The typical sample size required for analysis is 1000 or more keystrokes



Electromagnetic Emission Recording

- Electromagnetic emissions from a wired keyboard can be recorded from up to 66 feet away
- In 2009, a Swiss research team tested 11 different USB, PS/2 and laptop keyboards in a semi-Anechoic chamber and found all 11 keyboard types susceptible to electromagnetic emission recording due to lack of shielding

Electromagnetic Emission Recording

- The Swiss research team utilized a wide-band receiver to monitor the specific frequency of the emissions radiated from the 11 keyboards
- A anechoic chamber is an insulated room designed to stop reflections of either sound or electromagnetic waves.



Keystroke Logging Countermeasures

- Live CD/USB
 - CD/USB drive must be free of malicious software and the live operating system fully patched so that the operating system cannot become compromised during use
 - Booting from a Live CD/USB drive will not affect a hardware keystroke logging device

Keystroke Logging Countermeasures

- Anti-virus/ Anti-spyware software
 - Can detect software-based keystroke logging software operating at a lower privilege level based on patterns in executable code, heuristics, and software behavior
 - Cannot detect non-software keystroke logging devices such as hardware keystroke logging devices and waveform capture devices



Keystroke Logging Countermeasures

- On-screen keyboards
 - Can defeat hardware-based keystroke logging devices and some software-based keystroke logging programs
- Network monitors
 - Also known as reverse-firewalls
 - Will generate an alert whenever an application attempts to make a network connection
 - Will detect when the keystroke logging device attempts to transmit the captured data to the malicious individual or malicious system



Keystroke Logging Countermeasures

- One-time passwords/Secure Tokens
 - Can be used to protect an interactive session since each password is invalidated as soon as it's used
 - One-time passwords prevent replay attacks where a malicious individual uses the old information to impersonate the victim
 - Cannot prevent unauthorized transactions if the malicious individual has remote control over the system since the victim will use the OTP to initiate the session



Zeus Information

- AKA Zbot, Wsnpoem, and Gorhax
- Trojan horse that performs keystroke logging
- Primary infection method is via drive-by downloads and phishing schemes
- First documented in July 2007 after the theft of information from the United States Department of Transportation



Zeus Information

- Since 2007 Zeus has compromised accounts on websites utilized by Bank of America, NASA, Monster, ABC, Oracle, Cisco, Amazon, and BusinessWeek
- Zeus has sent out over 1.5 million phishing messages on Facebook
- The Zeus Botnet has control over systems in 196 countries including Egypt, Mexico, Saudi Arabia, Turkey and the United States



Zeus Information

- Zeus targets only Microsoft Windows systems
- Computers running Microsoft Windows XP Professional SP2 constitute the majority of the Botnet
- The Zeus Botnet targets login credentials for online social networks, e-mail accounts and online financial services



Zeus Information

- Current Anti-Virus software cannot consistently detect the presence of Zeus
- The best defense is security awareness and security awareness training related to suspicious URLs and emails
- An additional measure is to limit Local Administrative Rights



MS-ISAC Examples / VSP

Agency: vsp

Workgroup-Name: XXXXXXXXXXXXXXX

Client-Name: XXXXXXXXXXXXXXX

Client-ID: XXXXXXXXXXXXXXX

Client-IP-Addr: XXXXXXXXXXXXXXX

Malware: zeus2

Client-OS:

Client-Application: \Program Files\Internet Explorer\iexplore.exe

Date: 2010-07-01T16



MS-ISAC Examples / VSP

Key-Log Payload:

<https://apps.vsp.virginia.gov/ncjis/publicformrequest.do>

Data:

formName=SP167

methodToCall=submitRequest

requestId=

lastName= XXXXXXXXXXXXX

firstName= XXXXXXXXXXXXX

middleName= XXXXXXXXXXXXX



MS-ISAC Examples / VSP

maidenName=

nameSuffix=

sex= XXXXXXXXXXXXX

race= XXXXXXXXXXXXX

dob= XXXXXXXXXXXXX

soc=

searchtype=OTHER

specify=employment

countryName=



MS-ISAC Examples / VSP

requesttype= XXXXXXXXXXXXXXXX
requesterName= XXXXXXXXXXXXXXXX
requesterAttention= XXXXXXXXXXXXXXXX
requesterAddress= XXXXXXXXXXXXXXXX
requesterCity= XXXXXXXXXXXXXXXX
requesterState= XXXXXXXXXXXXXXXX
requesterZipCode= XXXXXXXXXXXXXXXX
paymentMethodCode= XXXXXXXXXXXXXXXX



MS-ISAC Examples / Tax

Agency: tax

Workgroup-Name: XXXXXXXXXXXXXXX

Client-Name: XXXXXXXXXXXXXXX

Client-ID: XXXXXXXXXXX

Client-IP-Addr: XXXXXXXXXXXXXXX

Malware: zeus2

Client-OS:

Client-Application: \Program Files\Internet
Explorer\iexplore.exe

Date: 2010-07-02T12



MS-ISAC Examples / Tax

Key-Log Payload:

https://www.irms.tax.virginia.gov/VTOL_ARWeb/maintain_claim.do

Data:

findMethod=ssn

externalID=SSN-XXXXXXXXXXXXXX

agencyNumber= XXXXXXXXXXXXXXX

claimNumber= XXXXXXXXXXXXXXX



MS-ISAC Examples / Tax

customerName= XXXXXXXXXXXXXXX

street1= XXXXXXXXXXXXXXX

street2=

city= XXXXXXXXXXXXXXX

state= XXXXXXXXXXXXXXX

zip= XXXXXXXXXXXXXXX

agencyName= XXXXXXXXXXXXXXX

claimName= XXXXXXXXXXXXXXX

claimAmount= XXXXXXXXXXXXXXX



MS-ISAC Examples / Tax

agencyInfo=

claimYear=2010

claimBalance= XXXXXXXXXXXXX

claimNumberVal= XXXXXXXXXXXXX

totalClaimReleasedAmount=
XXXXXXXXXXXXXX

claimStatusStr=Matched

totalClaimMatchedAmount=
XXXXXXXXXXXXXX



MS-ISAC Examples / Tax

agencyId= XXXXXXXXXXXXXXX

agencyPartnerStatus= XXXXXXXXXXXXXXX

claimStatus= XXXXXXXXXXXXXXX

claimStatusBeforeDelete=

previousClaimAmount= XXXXXXXXXXXXXXX

submittedDate= XXXXXXXXXXXXXXX

createTmstamp= XXXXXXXXXXXXXXX

lastUpdUserId= XXXXXXXXXXXXXXX

lastUpdTmstamp= XXXXXXXXXXXXXXX



MS-ISAC Examples / VSP

Agency: VSP

Malware: wsnpoem_v6

Original-

SHA1:bbc4e3a0c0e0a8566643f6d5aec774
16085c7530

Download-Date: 2010-01-26T223745

Client-Side-ID: XXXXXXXXXXXXX

Client-Side-Date: 2009-05-11T20



MS-ISAC Examples / VSP

[https://apps.vsp.virginia.gov/firearmdealers
/queryGunBuyer.do](https://apps.vsp.virginia.gov/firearmdealers/queryGunBuyer.do)

Data:

methodToCall=insertQueryGunBuyerSave

transactionId=0

attention=XXXXXXXXXXXXXX

sellerId=XXXXXXXXXXXXXX

documentNumber=XXXXXXXXXXXXXX



MS-ISAC Examples / VSP

lastName= XXXXXXXXXXXXX

firstName= XXXXXXXXXXXXX

middleName= XXXXXXXXXXXXX

sex= XXXXXXXXXXXXX

race= XXXXXXXXXXXXX

dateOfBirth= XXXXXXXXXXXXX

soc1= XXXXXXXXXXXXX

soc2= XXXXXXXXXXXXX

soc3= XXXXXXXXXXXXX



MS-ISAC Examples / VSP

usCitizen=Y

insNumber=

vaResident=Y

noOfPistol=

noOfRevolver=

noOfRifle=

noOfShotgun= XXXXXXXXXXXXX

transactionType=New Gun Purchase



2010 Key-Log Summary

Agency	Unique IP	Total URLs	Unique IDs
• Total	621	15164	1786
• BOA	2	8	1
• DBHDS	1	2	0
• DCJS	4	19	3
• DCR	4	6	0
• DEQ	3	12	2
• DGS	2	10	1
• DHCD	3	17	1



2010 Key-Log Summary

Agency	Unique IP	Total URLs	Unique IDs
• DHP	14	75	14
• DHRM	56	749	30
• DJJ	1	1	0
• DMAS	2	29	6
• DMBE	1	1	0
• DMV	125	2868	126
• DOA	14	154	15
• DOE	8	102	2
• DPOR	12	66	5



2010 Key-Log Summary

Agency	Unique IP	Total URLs	Unique IDs	
• DSS	34	129	36	
• LVA	9	16	0	
• SBE	3	4	0	
• SCC	33	353	23	
• Tax	87	1426	227	***
• TRS	14	164	5	
• VADOC	8	18	1	
• VAWC	123	7084	692	
• VDACS	1	10	1	



2010 Key-Log Summary

Agency	Unique IP	Total URLs	Unique IDs	
• VDFP	4	20	7	
• VDH	7	169	51	
• VDOT	4	58	5	
• VEC	17	34	1	
• VITA	7	186	93	
• VSP	18	1374	438	***



2009 Key-Log Summary

Agency	Unique IP	Total URLs	Unique IDs
• Total	618	11035	711
• ABC	2	4	0
• BOA	3	33	2
• DBHDS	1	7	1
• DCJS	2	2	0
• DFS	2	6	1
• DGIF	3	48	1
• DGS	2	5	0
• DHCD	1	11	0



2009 Key-Log Summary

Agency	Unique IP	Total URLs	Unique IDs
• DHP	5	39	6
• DHRM	78	1109	35
• DJJ	3	27	3
• DMBE	6	28	0
• DMV	146	2615	75
• DOA	20	124	32
• DOE	6	159	8
• DPOR	9	44	0
• DSS	51	364	106



2009 Key-Log Summary

Agency	Unique IP	Total URLs	Unique IDs
• FSTRS	1	3	1
• JYF	1	1	0
• LVA	22	33	1
• Mail	2	3	2
• SBE	5	30	0
• SCC	4	8	0
• TAX	49	569	69
• TRS	19	147	1
• VADOC	9	369	5



2009 Key-Log Summary

Agency	Unique IP	Total URLs	Unique IDs
• VAWC	116	3102	80
• VDEM	1	3	0
• VDH	7	23	1
• VEC	23	83	1
• VITA	8	160	4
• VSP	7	1821	272



Remediation / Web-based Banners

- Malicious software informational banner
 - http://www.vita.virginia.gov/uploadedFiles/Security/Toolkit/Citizens_Awareness_Banner_code.txt
- Password management banner



Final Thoughts

- Keep Anti-Virus software up to date
- Limit Local Administrative Rights
- Limit information collected on web forms
- Agent agreements



Questions???

For more information, please contact:
CommonwealthSecurity@VITA.Virginia.Gov

Thank You!



Virginia Information Technologies Agency

2010 Commonwealth Security Annual Report

John Green
Chief Information Security Officer



§ 2.2-2009

§ 2.2-2009. (Effective until July 1, 2010) Additional duties of the CIO relating to security of government information.

C. The CIO shall annually report to the Governor, the Secretary, and General Assembly those executive branch and independent agencies and institutions of higher education that have not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions, or other security threats. For any executive branch or independent agency or institution of higher education whose security audit results and plans for corrective action are unacceptable, the CIO shall report such results to (i) the Secretary, (ii) any other affected cabinet secretary, (iii) the Governor, and (iv) the Auditor of Public Accounts. Upon review of the security audit results in question, the CIO may take action to suspend the public body's information technology projects pursuant to § 2.2-2015, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor and Secretary any other appropriate actions.

The CIO shall also include in this report (a) results of security audits, including those state agencies, independent agencies, and institutions of higher education that have not implemented acceptable regulations, standards, policies, and guidelines to control unauthorized uses, intrusions, or other security threats and (b) the extent to which security standards and guidelines have been adopted by state agencies.



Explanation

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	Yes	Yes	100%

Acronyms:

- ISO:** Information Security Officer
- IS:** Information Security
- CAP:** Corrective Action Plan
- CISO:** Chief Information Security Officer of the Commonwealth

ISO Designated: The Agency Head has

Yes - designated an ISO with the agency within the past two years

No – not designated an ISO for the agency since 2006

Expired –designated an ISO more than 2 years ago or the designated ISO is no longer with the agency

Attended IS Orientation:

The number indicates agency personnel that have attended the optional Information Security Orientation sessions within the last 2 years. Their attendance indicates they are taking additional, voluntary action to improve security at their agency akin to “Extra Credit!”



Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	Yes	Yes	100%

Security Audit Plan Received: The Agency Head has

Yes - submitted a Security Audit Plan for the period of fiscal year (FY) [2010-2012 or 2011-2013](#) for systems classified as sensitive based on confidentiality, integrity or availability (Note: after July 1, 2010, Audit Plans submitted shall reflect FY 2011-2013)

No - not submitted a Security Audit Plan since 2006

Exception – submitted an exception on file with VITA to allow time for developing the Security Audit Plan & the CISO has approved

Expired –submitted a Security Audit Plan on file that does not contain the current three year period FY [FY 2010-2012 or FY 2011-2013](#)

Pending –submitted a Security Audit Plan that is currently under review

Corrective Action Plans Received: The Agency Head or designee has

Yes - submitted an adequate Corrective Action Plan or notification of no findings for Security Audits scheduled to have been completed

Some - submitted an adequate Corrective Action Plan or notification of no findings for some, but NOT all Security Audits scheduled to have been completed

No – not submitted any adequate Corrective Action Plans or notification of no findings for Security Audits scheduled to have been completed

Not Due - not had Security Audits scheduled to be completed

N/A - not submitted a Security Audit Plan so not applicable

Pending –submitted a Corrective Action Plan that is currently under review



Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	Yes	Yes	100%

Quarterly Updates: The Agency Head or designee has

Yes - submitted adequate quarterly status updates for all corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

Some - submitted adequate quarterly status updates for some corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

No - not submitted ANY quarterly status updates for some corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

Not Due - no open Security Audit findings

N/A - not submitted a Security Audit Plan or a Corrective Action Plan that was due

Pending - submitted quarterly status update that is currently under review



Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	Yes	Yes	100%

Percentage of Audit Obligation Completed:

Percent of sensitive systems reported in 2007 (according to IT Security Audit Plans) that have been audited to date. This datapoint is based on the IT Security Audit Standard requirement: *“At a minimum, databases that contain sensitive data, or reside in a system with a sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall be assessed at least once every three years.”*

Agencies that did not submit an IT Security Audit Plan in 2007 were not in compliance and therefore there is no data to report on for 2010.

Systems that have been removed from audit plans within the three year period due to retirement of the system or reclassification to non-sensitive are not counted.

N/C – agency not in compliance in 2007, agency did not submit an IT Security Audit Plan in 2007

N/R – agency not required to submit an IT Security Audit Plan until 2008

Pending – currently under review

Exception – submitted an exception on file with VITA to allow time for developing the Security Audit Plan & the CISO has approved



FAQ!

What should an agency do if they conduct a Security Audit that results in no findings?

In the event that a Security Audit was performed and there were no findings and, therefore, no Corrective Action Plan is due, the Agency Head should notify Commonwealth Security via email or letter stating what audit was conducted and that there were no findings.

What is the cutoff date to submit documentation for the Commonwealth Security Annual Report?

October 31, 2010



Secretariat: Administration

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Compensation Board	Yes	1	Yes	No	N/A	0%
Dept. of General Services	Yes	3	Yes	Not Due	Not Due	0%
Dept. of Human Res. Mgmt	Yes	1	Yes	No	N/A	0%
Dept. Min. Bus. Enterprise	Yes	0	Yes	Not Due	Not Due	N/C
Employee Dispute Resolution	Yes	0	Exception	Exception	Exception	0%
Human Rights Council	Yes	0	Yes	Not Due	Not Due	N/C
State Board of Elections	Yes	0	Expired	Some	No	50%

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Agriculture & Forestry

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Forestry	Yes	0	Yes	Not Due	Not Due	0%
Va. Dept. of Ag. & Cons. Serv.	Yes	27	Yes	Yes	Yes	66%

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Commerce & Trade

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Board of Accountancy	Yes	0	Yes	Yes	Not Due	100%
Dept of Business Assistance	Yes	0	Yes	Yes	Not Due	N/C
Dept. of Housing & Community Development	Yes	1	Yes	Yes	Yes	14%
Dept. of Labor & Industry	Yes	0	Yes	No	N/A	N/C
Dept. of Mines, Minerals & Energy	Yes	0	Yes	Yes	Yes	80%
Dept. of Professional & Occupational Regulation	Yes	1	Yes	Yes	Not Due	100%
Tobacco Indemnification Commission	Yes	1	Yes	No	N/A	N/C
Va. Economic Development Partnership	Yes	1	Yes	Not Due	Not Due	N/C
Va. Employment Commission	Yes	1	Yes	Yes	Yes	4%
Va. National Defense Industrial Authority	Yes	0	Yes	Not Due	Not Due	N/C
Va. Racing Commission	Yes	1	Yes	Yes	Not Due	N/C
Va. Resources Authority	No	0	No	N/A	N/A	N/C

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Education

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Christopher Newport University	Yes	0	Yes	Not Due	Not Due	0%
Dept. of Education	Yes	1	Yes	Not Due	Not Due	0%
Frontier Culture Museum of Va.	Yes	0	Yes	Not Due	Not Due	N/C
Gunston Hall	Yes	1	Yes	Not Due	Not Due	N/C
Jamestown - Yorktown Foundation	Yes	2	Yes	Pending	Not Due	29%
Library of Va.	Yes	0	Yes	Not Due	Not Due	100%
Norfolk State University	Yes	0	Yes	No	N/A	N/C
Richard Bland College	Yes	0	Yes	Not Due	Not Due	100%
Science Museum of Va.	Yes	1	Yes	Not Due	Not Due	N/C
State Council of Higher Education for Va.	Yes	0	Yes	Not Due	Not Due	N/C
University of Mary Washington	Yes	1	Yes	Yes	Yes	67%
Va. Commission for the Arts	Yes	0	Yes	Not Due	Not Due	N/C
Va. Museum of Fine Arts	Yes	0	Yes	Yes	Some	Exception
Va. School for the Deaf and Blind	Yes	2	Yes	Not Due	Not Due	N/R
Virginia State University	Yes	1	Yes	Yes	Yes	Exception

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact

CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Finance

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Accounts	Yes	0	Yes	Yes	Not Due	N/C
Dept. of Planning & Budget	Yes	0	Yes	Yes	Not Due	N/C
Dept. of Taxation	Yes	1	Yes	Yes	Not Due	53%
Dept. of Treasury	Yes	1	Yes	No	N/A	0%

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Health & Human Resources

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Health Professions	Yes	4	Yes	Not Due	Not Due	0%
Dept. of Medical Assistance Services	Yes	4	Yes	Yes	Yes	100%
Department of Behavioral Health and Developmental Services	Yes	12	Yes	Some	Some	N/C
Dept. of Rehabilitative Services	Yes	0	Yes	Yes	Not Due	0%
Dept. of Social Services	Yes	0	Yes	Not due	Not Due	0%
Virginia Foundation for Healthy Youth FSF	Yes	1	Yes	Not due	Not Due	N/C
Va. Dept. for the Aging	Yes	0	Yes	Yes	Not Due	Exception
Va. Dept. of Health	Yes	2	Yes	Some	Some	20%

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Natural Resources

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Conservation & Recreation	Yes	1	Yes	Some	No	0%
Dept. of Environmental Quality	Yes	2	Yes	Some	Some	60%
Dept of Game & Inland Fisheries	Yes	3	Expired	Some	No	N/C
Dept. of Historic Resources	Yes	1	Expired	No	No	0%
Marine Resources Commission	Yes	1	Yes	Yes	Yes	100%
Va. Museum of Natural History	Yes	2	Yes	Not Due	Not Due	N/C

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Public Safety

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Alcoholic Beverage Control	Yes	5	Yes	Yes	Yes	100%
Commonwealth's Attorney's Services Council	Yes	0	Yes	Not Due	Not Due	N/C
Dept. of Correctional Education	Yes	1	Pending	Yes	Pending	N/C
Dept. of Corrections	Yes	3	Yes	Pending	Yes	50%
Dept. of Criminal Justice Services	Yes	2	Pending	Pending	Pending	20%
Dept. of Fire Programs	Yes	2	Pending	Yes	Yes	N/C
Dept. of Forensic Science	Yes	0	Yes	Not Due	Not Due	N/C
Dept. of Juvenile Justice	Yes	0	Yes	Yes	Not Due	33%
Dept. of Military Affairs	Expired	1	No	N/A	N/A	N/C
Dept. of Veterans Services	Yes	0	Yes	Not Due	Not Due	N/C
Va. Dept. of Emergency Management	Yes	1	No	N/A	N/A	N/C
Va. State Police	Yes	1	Yes	Some	Yes	67%

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Technology

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
The Ctr for Innovative Tech.	Yes	0	Yes	Not Due	Not Due	N/C
Va. Info. Technologies Agency	Yes	14	Yes	Yes	Yes	70%

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Secretariat: Transportation

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Motor Vehicles	Yes	1	Yes	Yes	No	N/C
Dept. of Aviation	Yes	1	Expired	Not Due	Not Due	N/C
Dept. of Rail & Public Trans.	Yes	0	Yes	Not Due	Not Due	0%
Motor Vehicle Dealers Board	Yes	0	Yes	Not Due	Not Due	N/C
Va. Dept. Of Transportation	Yes	5	Yes	Yes	Yes	66%

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Independent Branch Agencies

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Indigent Defense Commission	Yes	3	Yes	Yes	Not Due	N/R
State Lottery Dept.	Yes	2	Yes	Not Due	Not Due	N/R
State Corporation Commission	Yes	4	Yes	No	No	N/R
Va. College Savings Plan	Yes	2	Yes	Yes	Not Due	N/R
Va. Office for Protection & Advocacy	Yes	1	Exception	Exception	Exception	N/R
Va. Retirement System	Yes	1	Yes	Some	Some	N/R
Va. Workers' Compensation Commission	Yes	3	Exception	Exception	Exception	N/R

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Others

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Office of the Governor	No	0	No	N/A	N/A	N/C
Office of the Attorney General	Yes	0	Yes	Not Due	Not Due	N/C

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov



Virginia Information Technologies Agency

Upcoming Events





Future ISOAG's

From 1:00 – 4:00 pm at CESC

Wednesday - September 15, 2010

Thursday - October 14, 2010

Tuesday - November 9, 2010



Future IS Orientation Sessions

Tuesday - September 14, 2010 1:00 – 3:30 (CESC)

Monday - November 1, 2010 1:00 – 3:30 (CESC)

IS Orientation is now available via webinar!



AITR Meeting

AITR Meeting:

Tuesday, August 17

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

Location: CESC



Information Security System Association

ISSA meets on the second Wednesday of every month

DATE: Wednesday, September 8, 2010

LOCATION: Maggiano's Little Italy, 11800 W. Broad St.,
#2204, Richmond/Short Pump Mall

TIME: 11:30 - 1:30pm. Presentation starts at 11:45 &
Lunch served at 12.

COST: ISSA Members: \$10 & Non-Members: \$20

PRESENTATION: *National Cyber Security Update*



MS-ISAC Webcast

National Webcast!

Wednesday, August 25, 2010, 2:00 to 3:00 p.m.

Topic: Social Networking/Web 2.0

The National Webcast Initiative is a collaborative effort between government and the private sector to help strengthen our Nation's cyber readiness and resilience. A number of vendors have offered their services at no cost, to help develop and deliver the webcasts.

Register @: <http://www.msisac.org/webcast/>



Identity Theft Red Flags Rules Extended Until December 31, 2010

The Red Flags Rule requires many businesses and organizations to implement a written Identify Theft Prevention Program designed to detect the warning signs – or “red flags” – of identity theft in their day-to-day operations.

At the request of members of Congress, the Federal Trade Commission is delaying enforcement of the “Red Flags” Rule until December 31, 2010. Read the FAQ at:

<http://www.ftc.gov/bcp/edu/microsites/redflagesrule/index.shtml>



Virginia Information Technologies Agency

Any Other Business ???????





ISOAG-Partnership Update

Don Kendrick

IT Infrastructure Partnership Team

August 12, 2010



NORTHROP GRUMMAN

Section Agenda

- Windows Patching Effort
- Server Patching Cycle: Dave Matthews
- Product Roadmaps: Tony Shoot
- Partnership Q & A

ADJOURN

THANK YOU FOR ATTENDING

