

The logo features the word "FORRESTER" in a white, serif font, centered within a dark green oval. The oval is set against a dark blue background with faint, light blue wavy lines radiating from behind it.

FORRESTER®

HITECH Act — Security And Privacy Implications

Khalid Kark

Principal Analyst

Forrester Research

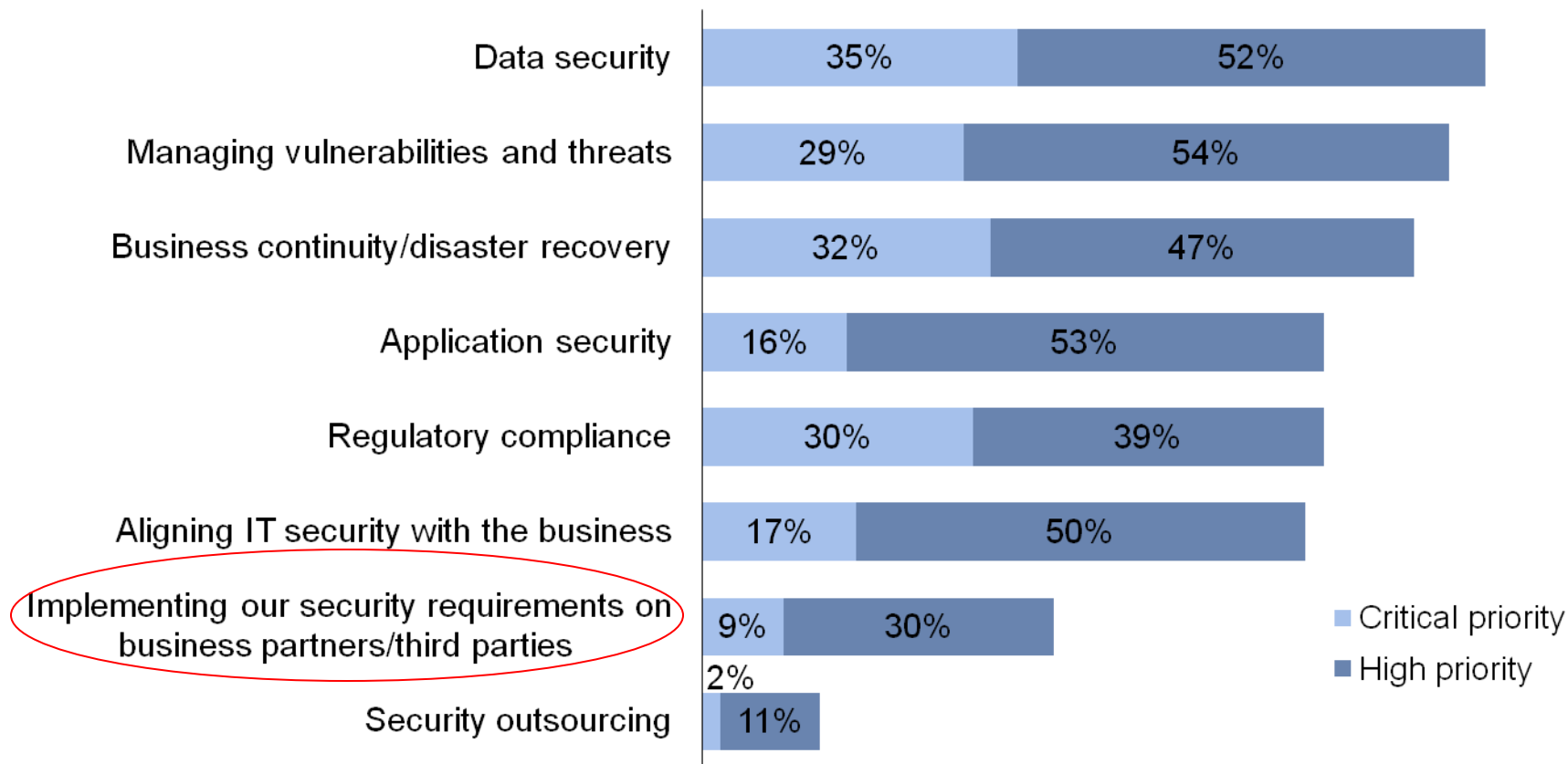
November 5, 2009

Agenda

- Current issues and challenges
- HITECH Act — the basics
- Implications for the healthcare industry
- Recommendations on dealing with the new requirements

Third party security will be the key for healthcare

“Which of the following initiatives are likely to be your firm's/organization's top IT security priorities over the next 12 months?”

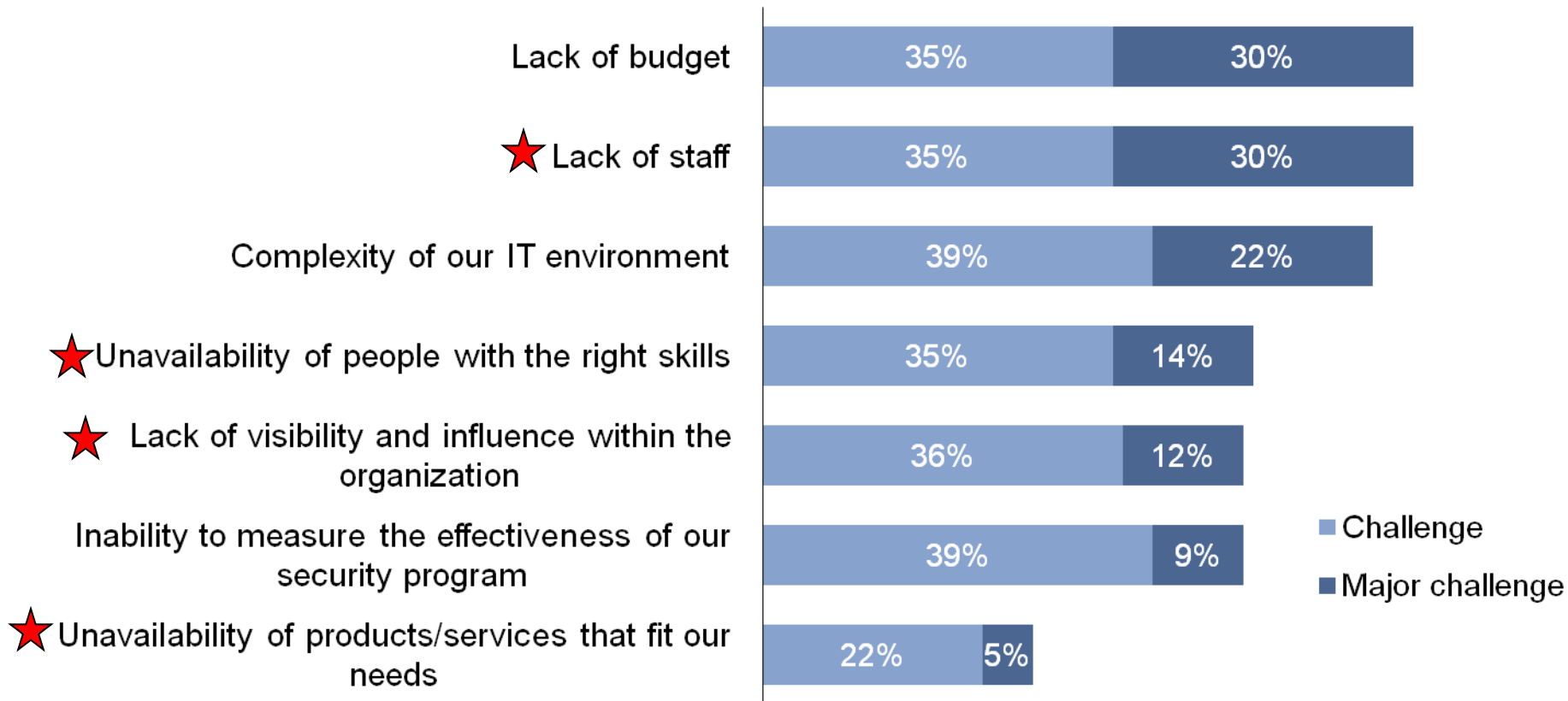


Base: 1,959 North American and European enterprise and SMB decision-makers responsible for IT security

Source: Enterprise And SMB Security Survey, North America And Europe, Q3 2009

Prioritization, people issues dominate challenges

“Please rate the following IT security challenges in your firm.”

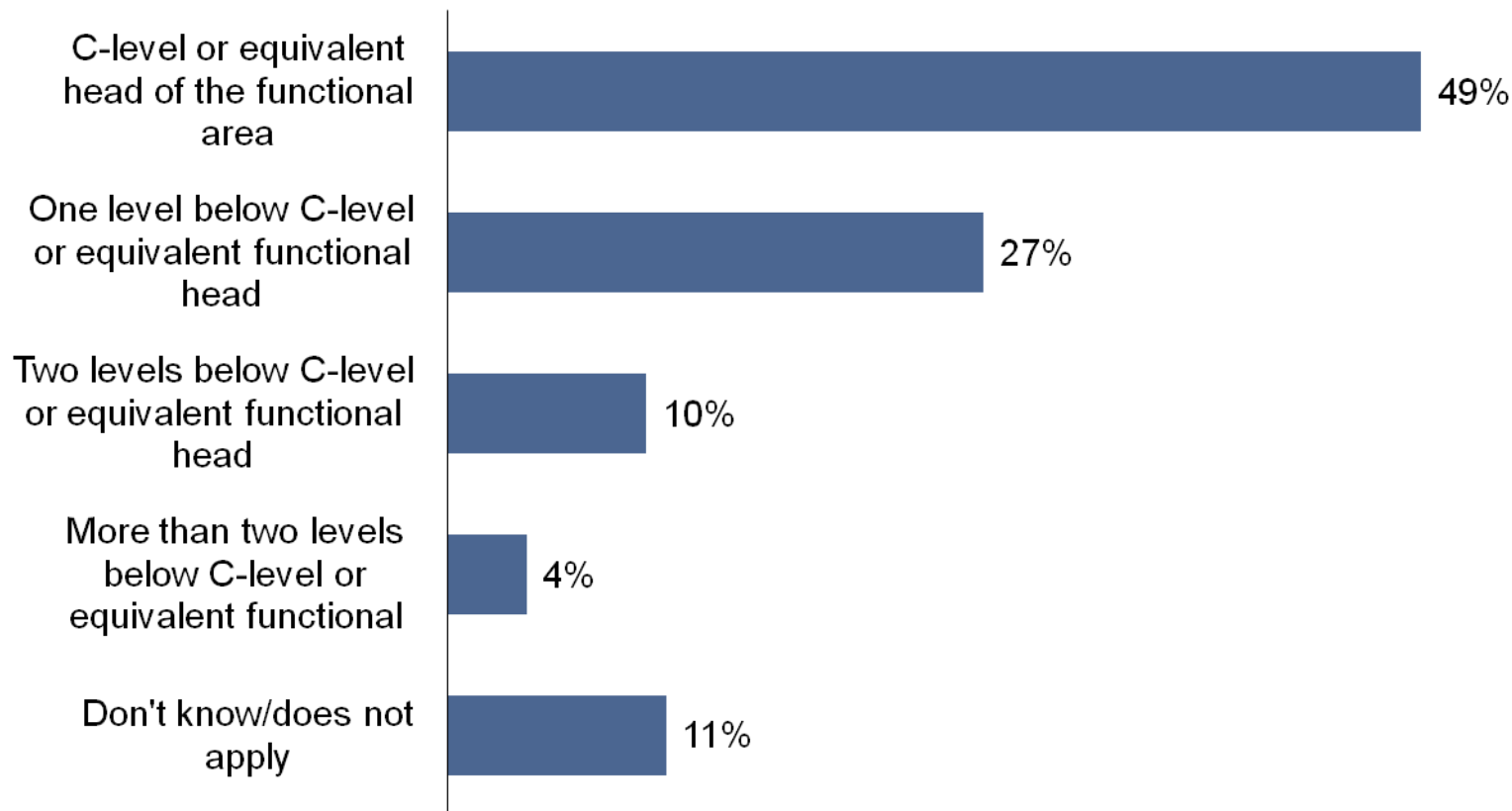


Base: 1,959 North American and European enterprise and SMB decision-makers responsible for IT security

Source: Enterprise And SMB Security Survey, North America And Europe, Q3 2009

Security is getting the visibility it has long sought

“To which level within the organization does the Chief Information Security Officer (CISO) or equivalent directly report?”

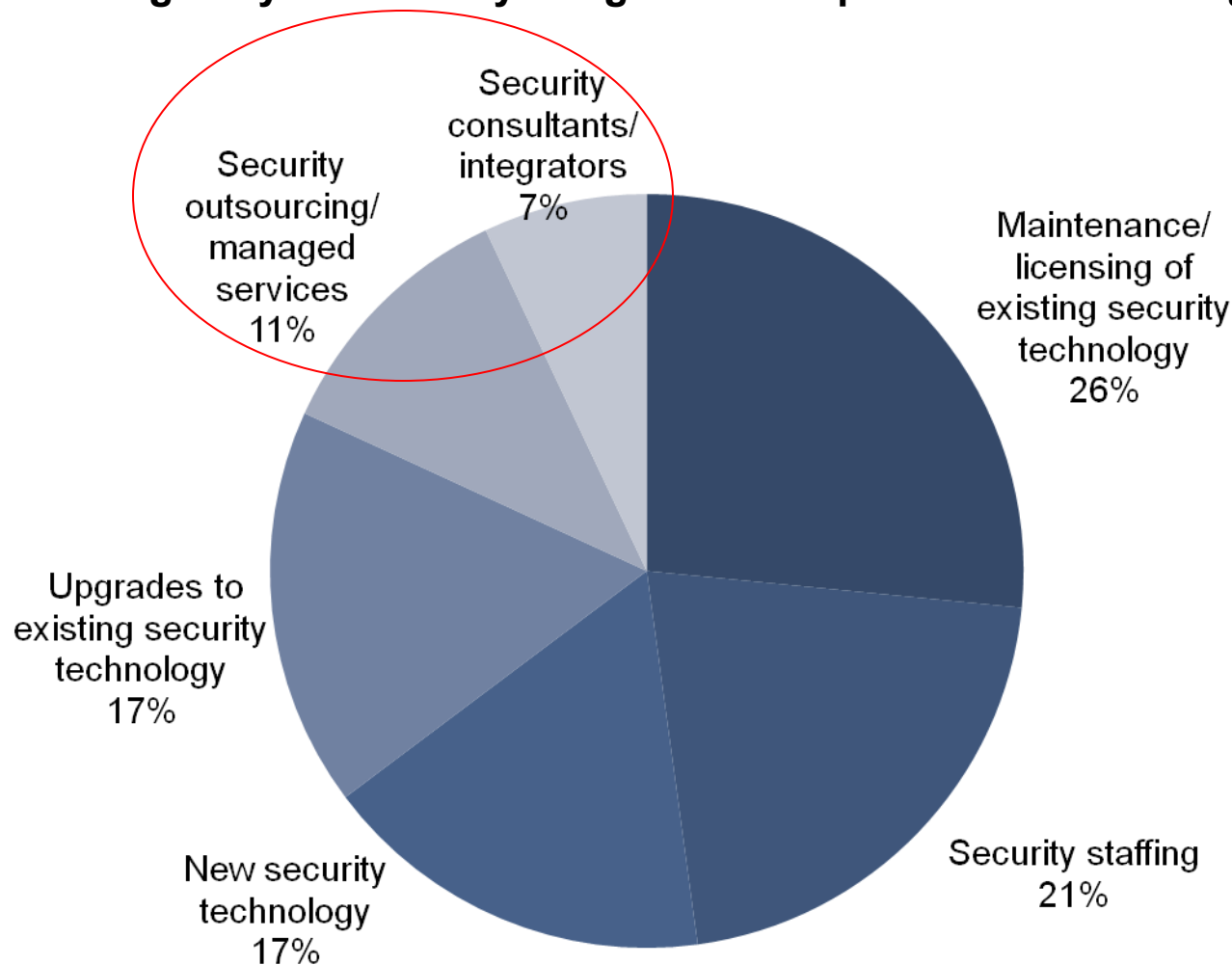


Base: 953 North American and European enterprise decision-makers responsible for IT security who's firm has at least one employee that works on security-related issues at least 75% of their job

Source: Enterprise And SMB Security Survey, North America And Europe, Q3 2009

Services spend is significant and increasing

“In 2009, what percentage of your security budget will be spent on the following categories?”



Base: 1,255 North American and European enterprise and SMB decision-makers responsible for IT security with budget knowledge

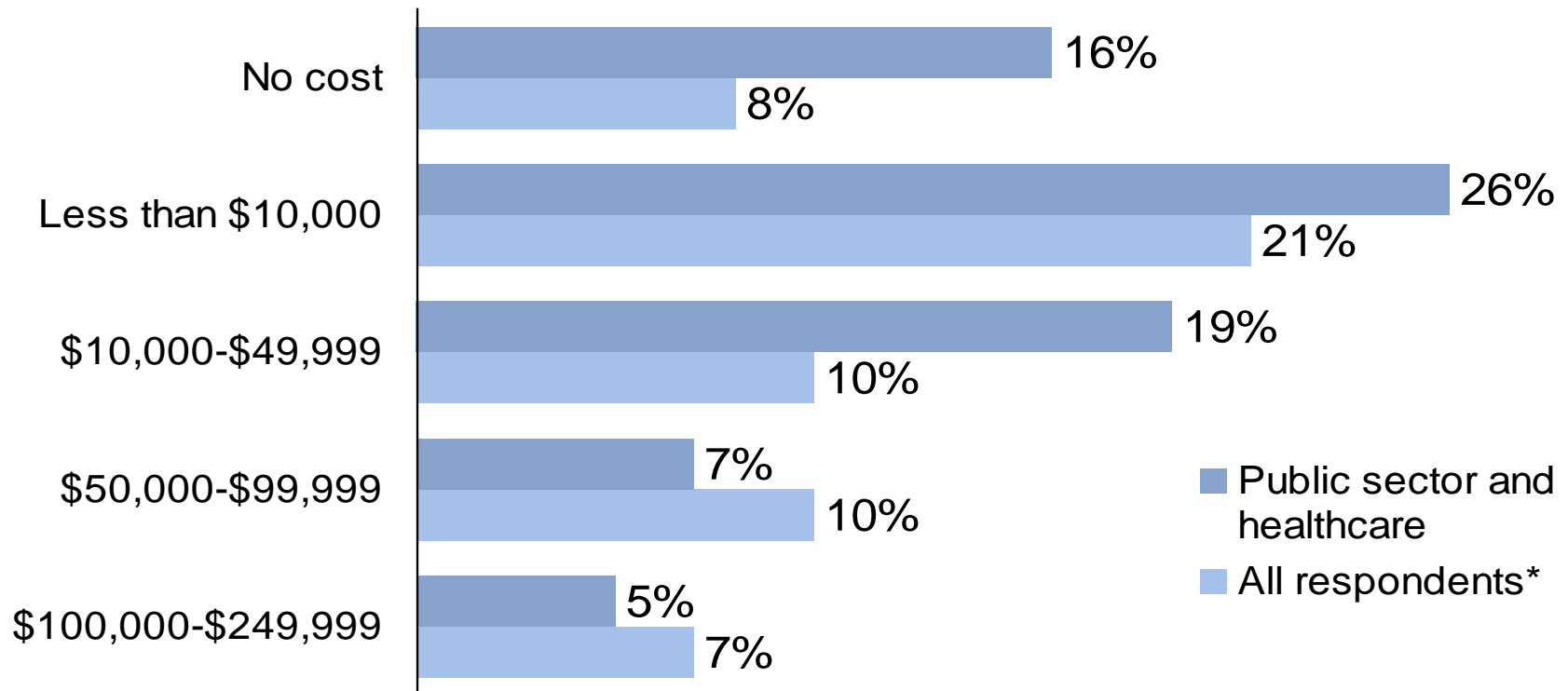
Source: Enterprise And SMB Security Survey, North America And Europe, Q3 2009

Healthcare trends and observations

- Overall spending on security at par with others
 - 10.87% of IT compared to 10.92% overall.
 - Slightly less in services and more in new technologies
- More C level Execs
 - 58% versus 49% overall
- More involved in compliance
 - 50% primarily own it versus 43% overall
- Need to focus more on third parties
 - 34% primarily own it versus 44% overall

Healthcare breaches are smaller typically

“On average, what would you estimate has been the financial impact for a typical security breach in the past 12 months? Include both direct and indirect costs.”



Base: 58 North American enterprise security decision-makers in the public sector or healthcare who's firm has had at least one breach in the past 12 months

*Base: 262 North American enterprise security decision-makers who's firm has had at least one breach in the past 12 months

Source: Enterprise And SMB Security Survey, North America And Europe, Q3 2009

Regulations and compliance quagmire

- HIPAA & HITECH
- NIST 800-53 and FIPS
- ISO 27001 and 27002
- PCI DSS
- FTC regulations
- CMS (Centers for Medicare & Medicaid Services)
- COBIT
- Other standards and guidelines

Agenda

- Current issues and challenges
- HITECH Act — the basics
- Implications for the healthcare industry
- Recommendations on dealing with the new requirements

HITECH Act

- On February 17, 2009, President Obama signed P.L. 111-05, the American Recovery and Reinvestment Act of 2009 (ARRP)
- Title XIII of Division A of ARRP comprise the provisions known as HITECH — the Health Information Technology for Economic and Clinical Health Act



ONC responsibilities under HITECH

- Office of the National Coordinator for Health Information Technology
- Goal: The utilization of an electronic health record for each person in the U.S. by 2014
- Establishing national standards for the exchange of health information
- Coordinating health information technology (HIT) policy and programs, and updating and implementing the Federal Health IT Strategic Plan through collaboration with public and private entities
- Ensuring that privacy and security protections are incorporated in the electronic exchange of health information
- Work with state and regional efforts regarding privacy, security, and data stewardship
- Implementing strategies to enhance the use of HIT and integration of information among healthcare providers, health plans, and government

Security and privacy implications

- HITECH applies the administrative, physical, and technical safeguards of the HIPAA security regulations directly to business associates
- HITECH imposes additional obligations upon business associates regarding policies, procedures, and documentation
- Impact
 - All organizations that support the health care industry as business associates
 - Before HITECH, these entities were required by contract to agree to certain safeguards regarding use or disclosure of protected health information (PHI)
 - After HITECH, required by law to develop and implement written privacy and security policies and procedures regarding handling of PHI

Security and privacy implications

- Upgrade technological capabilities and infrastructure
 - HITECH will specify encryption or other standards
- Revision of HIPAA business associate agreements
 - Differing interpretations — by application of law or amendment required
- Business associates that become aware of a pattern of activity that constitutes a violation of HIPAA must take steps to cure the violation
 - Terminate agreement
 - Report problem to Health and Human Services (HHS)
 - Civil and criminal penalties that apply to covered entities for violations of security and privacy regulations now will apply directly to business associates

Requirements for business associates

- Get involved in HIPAA security compliance
- Develop and implement policies and procedures
- Revise business associate agreements if necessary
- Develop and implement breach notification process



Breach notification requirements

- HITECH requires you to notify individuals or entities when unsecured identifiable PHI or unsecured personal health records (PHR) are breached.
- The definition of “breach” includes:
 - Unauthorized acquisition,
 - Unauthorized access,
 - Unauthorized use, OR
 - Unauthorized disclosure.
- “Breach” does not include an inadvertent disclosure if the information is not further accessed, used, or disclosed.
- HHS must issue guidance specifying the technologies and methodologies that render PHI unusable (i.e. encryption).

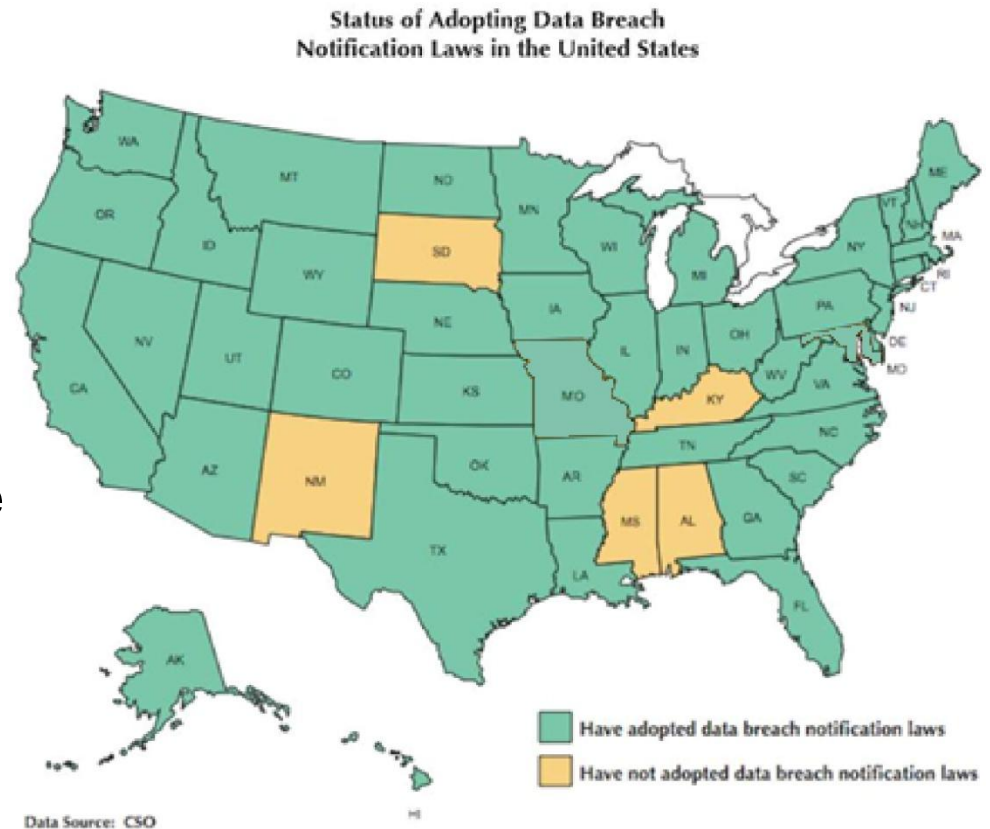


Breach notification responsibilities

- Covered entities and business associates (working through covered entities) must notify each individual whose unsecured PHI has been or is **reasonably believed** to have been accessed, acquired, or disclosed.
- Vendors must notify individuals and the Federal Trade Commission (FTC) and FTC will notify HHS. “Temporary” requirements until Congress enacts new legislation establishing notification requirements for non-covered entities.
- Third party service providers must notify vendor or entity of security breach, including identity of the individual affected.
 - Notification must be within 60 days of discovery unless requested by law enforcement
 - In writing or electronic, posting on Website, or through broadcast media
- If more than 500 people affected, notice must be provided to prominent media
 - Notice must be made to HHS
 - HHS will post on its Website a list of covered entities involved in a breach
 - If less than 500 individuals, covered entity must provide a log to HHS
 - HHS reports results of logs annually to Congress

State breach notification laws

- 45 states have enacted laws
- Most require reasonable belief that information will be used for identity theft (no such requirement in HITECH)
- No specific preemption language in HITECH, although it supersedes any inconsistent standards governing privacy and security of individually identifiable information
- HIPAA does not supersede state law if state law is more stringent
- Need to comply with both state and HITECH if there is a breach



Source: Osterman Research, "Why Your Organization Needs To Implement DLP," October 2008

The cost of a breach

Cost per record

Category	Description	Cost per record		
		Company A: Low-profile breach in a nonregulated industry	Company B: Low-profile breach in a regulated industry	Company C: High-profile breach in a highly regulated industry
Discovery, notification, and response	Outside legal counsel, mail notification, calls, call center, and discounted product offers	\$50	\$50	\$50
Lost employee productivity	Employees diverted from other tasks	\$20	\$25	\$30
Opportunity cost	Customer churn and difficulty in getting new customers	\$20	\$50	\$100
Regulatory fines	FTC, PCI, SOX	\$0	\$25	\$60
Restitution	Civil courts may ask to put this money aside in case breaches are discovered.	\$0	\$0	\$30
Additional security and audit requirements	The security and audit requirements levied as a result of a breach	\$0	\$5	\$10
Other liabilities	Credit card replacement costs. Civil penalties if specific fraud can be traced to the breach.	\$0	\$0	\$25
Total cost per record		\$90	\$155	\$305

Source: April 10, 2007, "Calculating The Cost Of A Security Breach," Forrester report

Agenda

- Current issues and challenges
- HITECH Act — the basics
- Implications for the healthcare industry
- Recommendations on dealing with the new requirements

Incentives & penalties



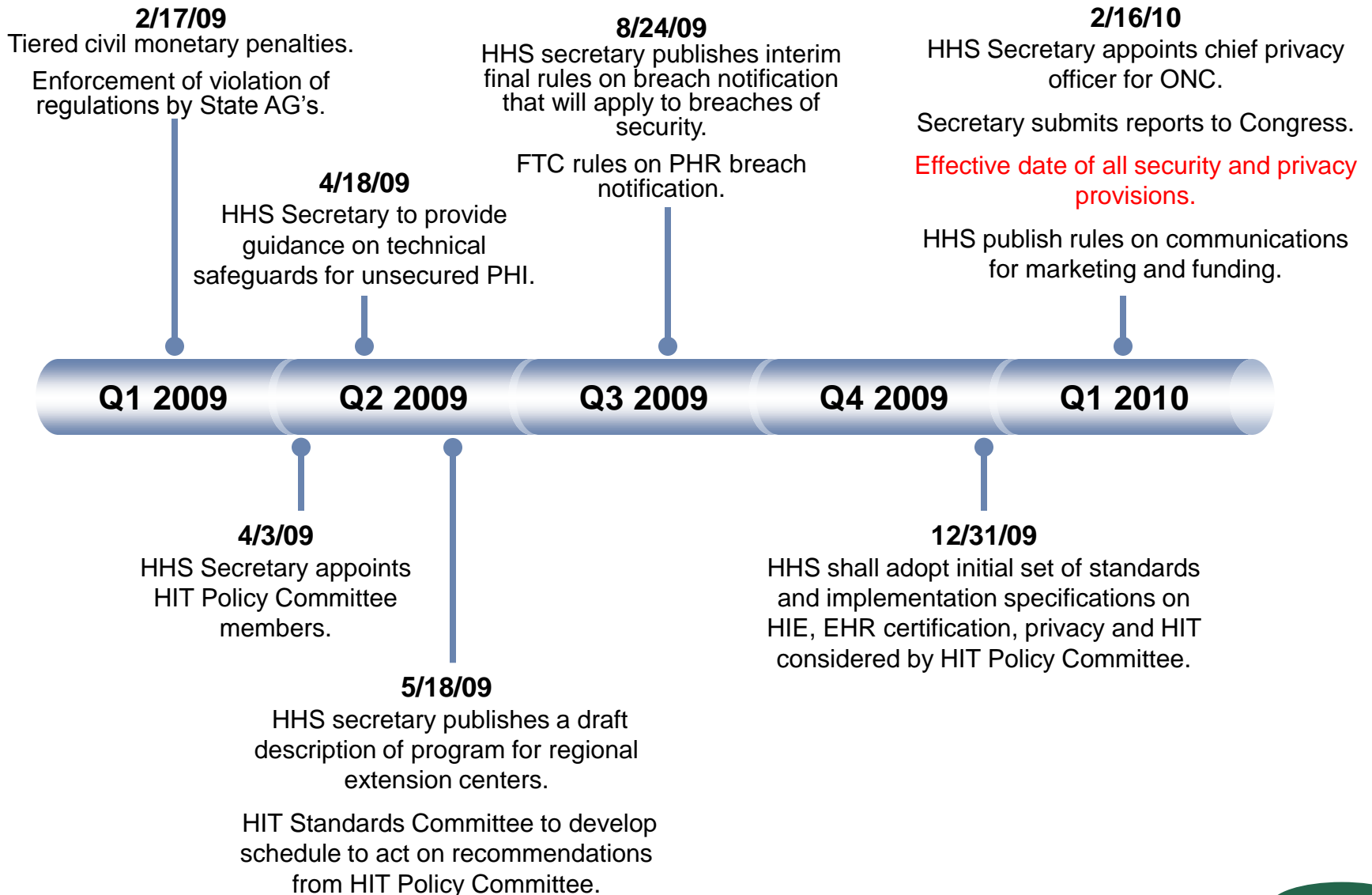
- Incentives worth \$17 billion
 - Front loaded incentives
 - Majority of incentives in the first 2 years
 - 75% of allowable expenses for Medicare
- Penalties are tiered, depending on conduct
 - Unknown — \$100 per violation, up to \$25,000 for all identical violations in a calendar year, with a cap of \$1.5 million
 - Reasonable cause that is not willful neglect — \$1,000 for each violation, up to \$100,000 for all identical violations in a calendar year, with a cap of \$1.5 million for all violations of this type in a calendar year
 - Willful neglect — If violation corrected within 30 days of knowledge: \$10,000 for each identical violation, up to \$250,000 for all identical violations in a calendar year, with a cap of \$1.5 million for all violations of this type in a calendar year. If violation not corrected: \$50,000 for each violation, up to \$1.5million for all identical or non-identical violations in a calendar year

Audit and enforcement

- Secretary of HHS required to conduct periodic audits of covered entities and business associates
- Secretary of HHS is required to report the number of audits and a summary of audit findings to Congress starting in 2010
- Reports will be made available on HHS website



Timeline



Agenda

- Current issues and challenges
- HITECH Act — the basics
- Implications for the healthcare industry
- Recommendations on dealing with the new requirements

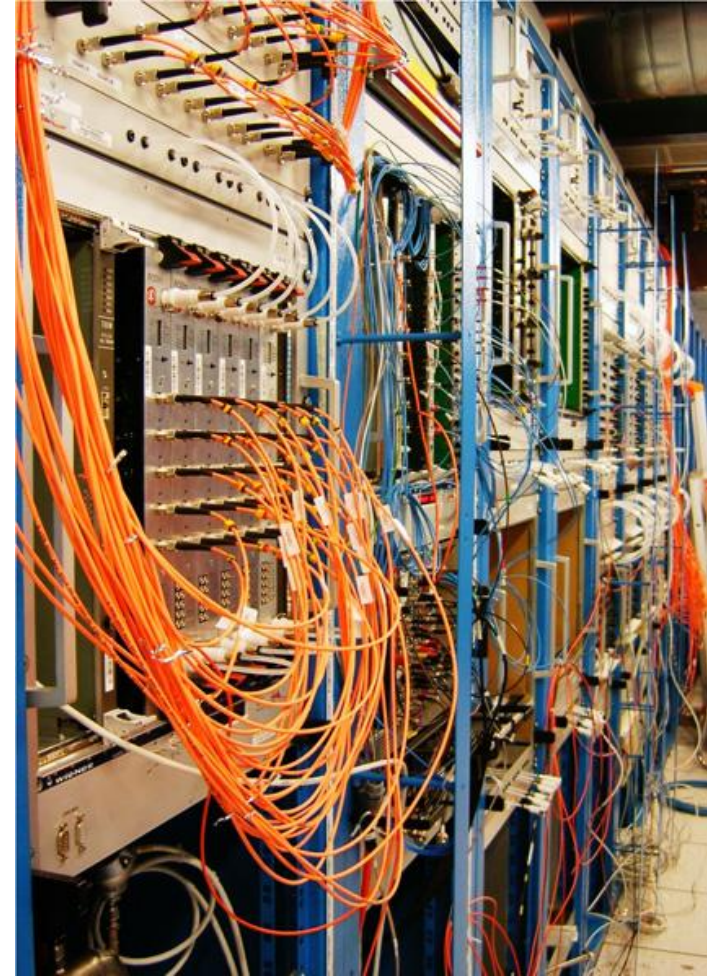
Rule 1: Take a risk-based approach

- Look beyond regulatory compliance.
- Go beyond PHI and HIPAA in performing a risk assessment.
- Use a standard security framework for your risk assessment.
- Apply once, use multiple times.



Rule 2: Follow the data through its life cycle

- Take a pragmatic approach to data classification.
- Track disclosure of ePHI.
- Monitor and log access to sensitive data.
- Dispose of data properly.
- Focus on the security of all devices that house sensitive data.



Rule 3: Equip yourself to monitor and respond to security incidents

- Proactive monitoring and detection capabilities
- Incident management processes
- Well-rounded response capabilities



Rule 4: Focus on third parties and business associates

- Perform risk assessments of your critical business partners.
- Implement service levels with proper escalation processes.
- Re-do new contracts.
- Review existing contracts to add security language or addendums.



Rule 5: Be prepared to respond to the changing technology and threat landscape

- Responding to the ever-changing external threat paradigm
- Ensuring proper security and privacy tools for new Web 2.0 and virtualized environments
- Dealing with consumer demands around managing their data privacy
- Changing legislation and regulatory requirements



Concluding thoughts

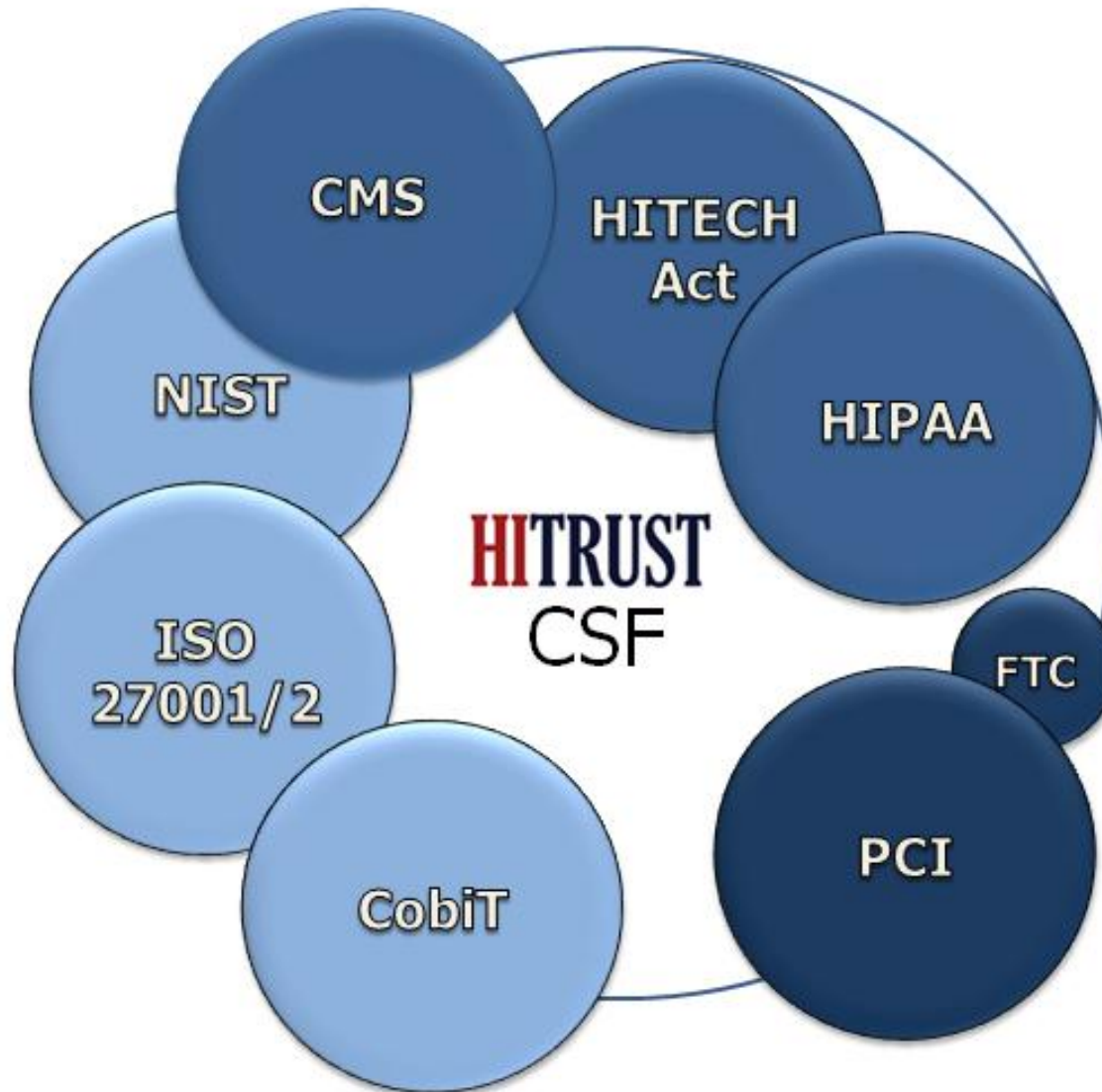
- Additional competency may be crucial for your success
 - Services versus in-house resources
- Third party security will be the biggest challenge
 - Industry in general is behind the curve on this
- Justification and spending
 - Higher visibility means business-centric view





HITRUST, HITECH, HIPAA: How Solutionary Can Help

Presented by Don Gray, Chief Security Strategist



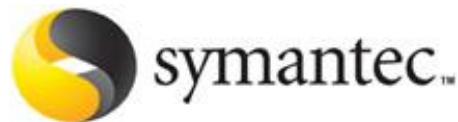
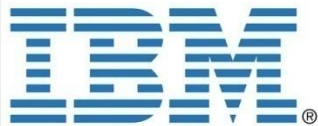
- Risk based – organization size, capabilities, systems
- Very broad (all PHI not just ePHI)
- Unifying – tying multiple standards together
- Very proscriptive (you must use XXX encryption, password strength, etc.)
- Wide community support
- For now the “easy button” for showing HITECH compliance

HITRUST certified

- **MSSP Services**
 - Log Monitoring & Management
 - Vulnerability Lifecycle Management
- **Security / Compliance Consulting**
 - Assessor

Experience w/multiple compliance standards

- HIPAA, ISO 27001/2, NIST, PCI, CobiT



More than 100 devices supported – highest in the industry

- ✓ Epic
- ✓ Mysis
- ✓ Centricity RIS
- ✓ Centricity PACS
- ✓ Carecast
- ✓ CARE
- ✓ Onbase
- ✓ Hospital Badge System
- ✓ Nurse Call

- ✓ Teletracking
- ✓ Transchart
- ✓ Pyxis
- ✓ SMS
- ✓ IDX
- ✓ Lawson
- ✓ MSO
- ✓ PeopleSoft

Forensics – activity by user for all logs, sorted by time

Patient – activity by patient for all logs, sorted by time

Same Name – activity on a patient account where the user has the exact same name

Family – activity on a patient account where the users last name is the same

Same Address – activity on a patient account where the users home address is the same as the patient

Print – where a user prints more than one report from an application

Demographics – activity where a user accesses more than two patients and only views demographic data

Wrong Location – where an IP user accesses the system from an OP/Clinic terminal and list all activity where an OP/Clinic user accesses the system from an IP terminal

Wrong Time –users who are signing in at a time that is abnormal for their pattern

Gender Based –users who over the period of a week access over 80% of the same gender patient records (male or female)

High Risk Users –activities of users not found in the Lawson or MSO IDM

Wrong Department –activities of individuals who are signed in to one department and access client information in a different department

VIP –activities associated with a certain group of VIP patients and whitelist / blacklist / other notation for each user

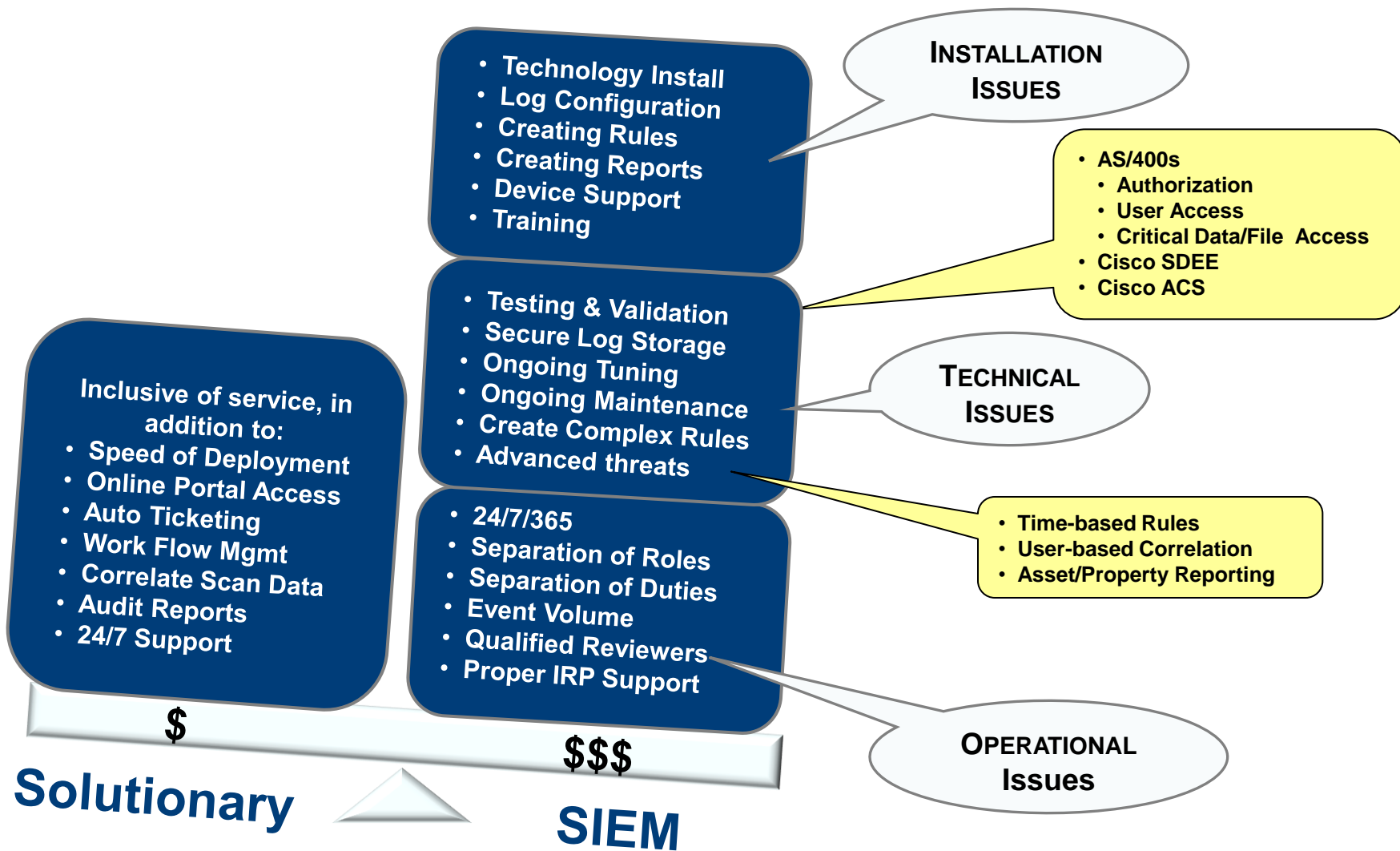
Excessive log-in Time – users logged in for more than 16 hours on any one application

Multiple Log-in – users who are logged into a single application in more than one location

Employee – activity where an employee accesses another employee's patient record

NOTE: Reports listed here can only be produced if the applications, systems, and devices sending logs to Solutionary provide the log data listed above.

Let Us Do The Heavy Lifting



Khalid Kark
617.613.6433
kkark@forrester.com
www.forrester.com

Don Gray
402.361.3000
dgray@solutionary.com
www.solutionary.com

Thank You

