NETSECURE'11

IT SECURITY & FORENSICS CONFERENCE & EXPO • MARCH 24-25, 2011 - WHEATON, IL

INFORMATION SECURITY OF LARGE SYSTEM DEVELOPMENT PROJECTS

James C. Murphy

GSEC, CISSP-ISSMP, CISA, CISM

Information Security Architect

NC DHHS, Office of MMIS Services

james.murphy@dhhs.nc.gov

Information Security of Large System Development Projects

Disclaimer:

This presentation reflects only the presenter's professional and/or personal views. The material presented herein is not intended to represent official statements or positions of the North Carolina Department of Health and Human Services or the Office of Medicaid Management Information Systems Services.

Introduction

Define: **Large System Development Project**

- Significant organizational changes
  - System replacements, process automation, mergers/acquisitions, service/product expansion
- Involves more than one organizational unit
  - Personnel/finance systems, all of "Research", geographic distribution of units
- Multi-year time frame
  - 1 – 3+ years
- External developer
  - Internal resources lacking, vendor with existing system, COTS integration
- Procurement process
  - Request for Proposal, vendor evaluation/selection

Introduction

Challenges!

Project within a project

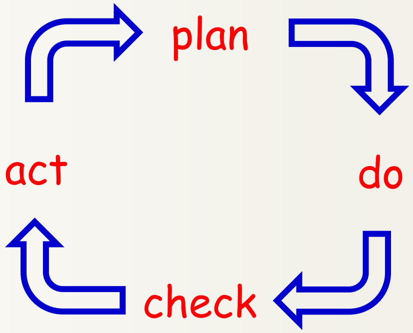
Threaded throughout the larger project

- Data/information
- Regulatory/privacy
- Architecture/infrastructure/software
- Service continuity

Project Management Structure

Deming cycle:

- Plan
- Do
- Check
- Act



Outline

Part I.

Introduction

Before the Beginning

Security Posture

Part II.

PLAN

Organization Characterization

Security Preparation

Security Specification

Part III.

DO

Procurement Participation

Design and Development

Vulnerability Controls

Assessment Instruments

CHECK

System/User Test Reviews

System/User Access Control

ACT

Pre-Operational

Operations and beyond

Part I

Before the Beginning

Security Posture: Knowledge foundation

- Security Background, experience, certification
  - How **Prepared** are you?
- Familiarization with InfoSec Regs, Standards
  - How **Perplexed** are you?
- Understanding of State of "InfoSec Warfare"
  - How **Paranoid** are you?
- Understanding your own industry sector
  - How **Positive** are you?

Know the message

Security Posture: (ISC)^2 Ten Domains of InfoSec CBK

https://www.isc2.org/cissp/default.aspx

- Access Control
- Application Development Security
- Business Continuity & Disaster Recovery Planning
- Cryptography
- Information Security Governance & Risk Management
- Legal, Regulations, Investigations & Compliance
- Operations Security
- Physical (Environmental) Security
- Security Architecture & Design
- Telecommunications & Network Security

Not completely sufficient!!!

Part I

Before the Beginning

No one is listening!

Murphy, James C. 2009. *No one is listening!* p 27-30 *in* ISSA Journal, May 2009.

"The very security professionals who are convinced that we have the answers are the primary barriers preventing the message from being heard. I suggest that there are three main reasons for the barriers."

Know the message

Win the right to be heard

Be always ready to give an answer

Trust – Privacy – Security – Risk

Part I

Know the message

Trust

College Professor, US. Gov't class:

"Do You Trust 'The People?'"

Trust between individuals -- possible

Trust between *groups* ??

"…establish *trust* among…"

"…builds *trust* that is essential…"

"…environment of *trust*…"

Understandable intent, but the *reality:*

Trust among complex organizations – *improbable to impossible!!*

Part I

Know the message

Trust

There Is No Universal Security Architecture. Nick Szabo, 1998.
Trusted Third Parties Are Security Holes. Nick Szabo, 2005.
http://szabo.best.vwh.net/index.html

Complete Data Security A Mission Impossible, Study Claims.
Tom's Guide, Wolfgang Gruener, Feb. 11, 2008.
http://www.tomsguide.com/us/data-security,news-563.html

Data Breaches at Arizona Medical Center Makes Case for Zero Trust Security
Fahmida Y. Rashid, Jan. 14, 2011
http://www.eweek.com/c/a/Security/Data-Breaches-at-Arizona-Medical-Center-Makes-Case-for-Zero-Trust-Security-571698/

Trust Agreements/Contracts are *Vital*…

…they don't *provide* Trust or *guarantee* Assurance!

rather *Protection Agreement/Commitment*

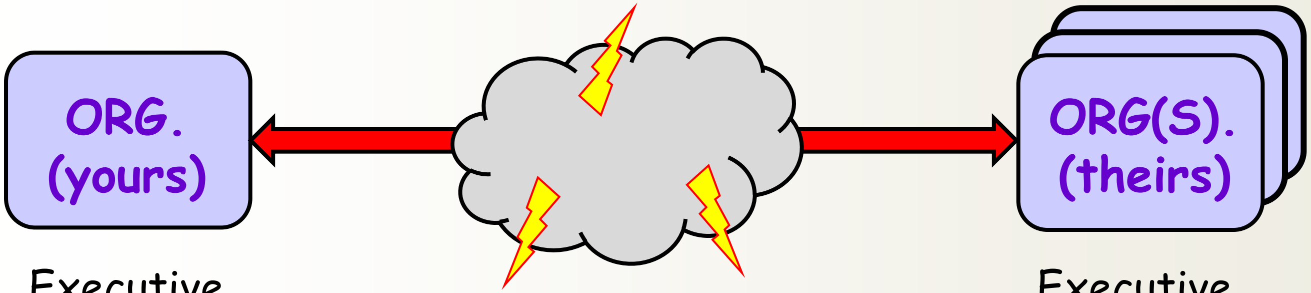
Part I

Know the message

Trust - realistic

Assume NO Trust and plan accordingly!

Too many loose ends!



Executive		Executive
Workforce	Threats	Workforce
Non-workforce	Vulnerabilities	Non-workforce
Software	Attackers	Software
Hardware		Hardware
Buildings		Buildings
?		?

Part I

Know the message

Privacy/Security – clarification needed!

Historic: "…inherent tradeoff between security and usability."

Cranor & Garfinkel. 2005. *Security and Usability.* O'Reilly Media.

security/tech support
privacy
user community

Recent: "…security doesn't equal privacy…."

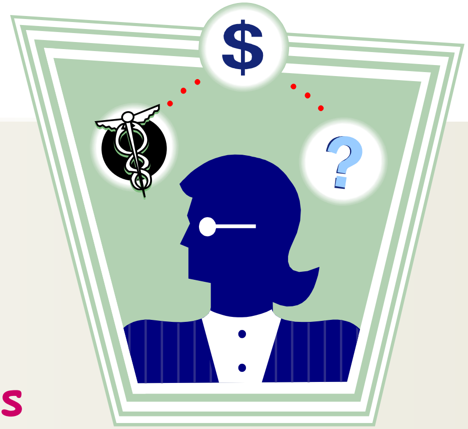
GHIT Notebook. 2/27/2008. *What's more important, privacy or security?*

(Based on interview with Dr. Deborah Peel, Patient Privacy Rights)

http://www.govhealthit.com/blogs/ghitnotebook/350238-1.html

Know the message

Privacy: Two Perspectives



Human-personal

My 'space', my identity, my health record, etc.
Privacy often stated in terms of *person control*

Predominant perspective of legal/compliance efforts

Data/Information

Digitized information *identified/classified as private*
Subset of corporate information

Predominant perspective of IT Security efforts

Necessitates distinction, classification of Information

Part I

Know the message

Security: from the *Information* perspective

Privacy and security are complementary

Privacy

AND

Security!

Protection

AND

Access!

"…security and usability can be [*ARE*] synergistic."

Cranor & Garfinkel. 2005.

Security is the implementation/completion of Privacy

Part I

Know the message

Security is: ***Not Privacy***

Implementation of Privacy requirements

Privacy and Security are Complementary

Security is: ***Not (exclusively) …***

…a Product …a Headcount

…a Checklist …a Budget Item

…a Regulation …an I.T. problem

Security is:

…a Process …a Culture …a Discipline

…an organizational initiative that requires the responsible participation of *all* workforce members – top to bottom!!

Know the message

Security **- simplified**

Confidentiality

Integrity Availability

Provides Protection
of Information

Confidentiality, Integrity, Locks, Transmission, Storage, Encryption, Continuity, Backup/Archive, Redundancy, Separation of Duties, Malware Defense, Intrusion Detection/Prevention

Controls Access
to Information

Availability, Accessibility, Usability, Timeliness, Keys, Encryption, Continuity, Display, Input/Output, Identity Management, Account Authorization, Authentication, Provisioning

Process Definition, Documentation,
Training, Monitoring, Auditing

Know the message

Risks – General

- Threats
  - Fairly constant sources
  - Increasing in quantity & varieties
- Vulnerabilities
  - Breakdown in protection structure
  - Actualization of threats
- Asset Value (AV)
  - Value of threat target
  - Costs of successful threat

$$R = P(T) \times V \times AV)$$

Probability of monetary loss

Know the message

Risks - from IT perspective

- Threats
  - *Information is the target*
  - Interruptions to services
  - Unauthorized access → disclosure/loss
- Vulnerabilities
  - Infrastructure – *data storage & movement*
  - Policies/procedures/practices
  - Human omission/commission
- Probability of monetary loss
  - *Value of data/information*
  - Infrastructure replacement
  - Regulatory fines/penalties
  - Disclosure costs: reputation, lawsuits

Part I

Know the message

IT Risk Management: Controlling vulnerabilities

- Infrastructure
  - Reduce complexity
  - Increase redundancy
  - Change management
  - Monitoring/maintenance/audit
- Software Development
  - Planning
  - Testing
- User awareness & training
  - Documentation
  - Communication!!

Part I

Win the right to be heard

Tact & Diplomacy

YOUR Security role:

- Status in organization?
  - Entry level, expert, management
- Personal involvement within organization?
  - Help desk, project planning, policy writing
- Numbers?
  - Solo, small/large team
- Relationship building?
  - Teams, committees, training

Win the right to be heard

Tact & Diplomacy

Opportunities:

- Hallway discussions - *listen*
  - Data users
- Meetings with data owners - *Listen*
  - Current states, changes, access restrictions
- Meet with Subject Matter Experts - *LISTEN*
  - Data usage, data needs
- Hear senior management - *LISTEN*
  - Goals, plans, initiatives

Win the right to be heard

Tact & Diplomacy

Organization targets/needs:

- Organizational profile
  - Industry, products/services, customers
- Nature of data/information
  - External sources, internal stores, outputs
- Basis for changing
  - Legacy systems, opportunities, points of pain
- Desired target state
  - Future system, expectations

Be always ready to give an answer

Professional response

When questioned…

- Informal questions
  - Help desk, email requests, problem solving
- Meeting participation
  - Discussions, suggestions
- Formal presentations
  - Invitations, training, targeted technologies
- Writings
  - Newsletters, blogs, essays, publications

Part I

Be always ready to give an answer

Professional response

Can you identify and present the return on investment (ROI) that information security enhancements can bring to the organization?

Can you break your overall plan into incremental steps that will better fit a budget-managed environment?

Can you recommend standard methods and practices for developing secure software within small or large system development projects?

Have you read (or at least identified) the international, national, and local laws and standards about information privacy and security that directly affect your organization's practices?

Can you participate in organizational discussions about the distribution of responsibilities for personal safety and information security practices?

Will you be able to answer questions about liability of data loss within your organization?

Part I

Be always ready to give an answer

Professional response

Will you be able to initiate (or participate responsibly in) an investigation of data loss or theft?

Do you know how to answer questions about incidents that may lead to emergency response or disaster declaration within your organization?

Can you give answers to questions about numbers and types of successful and unsuccessful attacks on your network?

Can you recommend technology solutions and countermeasures to prevent such activities in the future?

Can you recommend business practices and behaviors that will also mitigate the same activities in the future?

Can you design and lead a security assessment after the project is complete and the system is in production?

Outline

Part I.

Introduction

Before the Beginning

Security Posture

Part II.

PLAN

Organization Characterization

Security Preparation

Security Specification

Part III.

DO

Procurement Participation

Design and Development

Vulnerability Controls

Assessment Instruments

CHECK

System/User Test Reviews

System/User Access Control

ACT

Pre-Operational

Operations and beyond

Part II: PLAN

Foundations…

Information Security

Most important asset:
Human Resource (internal)

Greatest source of threats/vulnerabilities:
Human Resource (internal and external)

Most difficult context:
People/Information/Technology/Process

Most important capability:
Personal Communication (all kinds)

Focus!

Provide Protection
Control Access

Information Security

Reviewing design and development…

For InfoSec practices and processes…

Within a future production environment!

In Design and Development…

Evaluating Assertions

In Production…

Confirming Evidence

Preparation

Provide Protection

Control Access

Organizational posture

Public or private

Many differences!

Industry sector

Health Care or State Government?

Regulatory, standards environment

Some quite specific

Size, growth, competition

Cost of new system

Responsibility of SMEs, Business Users

Preparation

Provide
Protection
Control
Access

Business Systems/Processes/Rules

Purpose of new system?

Tied to industry sector

Replacing legacy system?

Or new effort

Subject/services provided?

Target audience, users, customers

In-house or Vendor?

System developer or Fiscal Agent?

Responsibility of SMEs, Business Users

Part II: PLAN

Preparation

Provide
Protection
Control
Access

Business Systems/Processes/Rules

Business systems…

- Umbrella environment
- Defined by business processes…
  - Subsystems, collateral systems, e.g.
  - Described by business rules
    - Functional statements (English)
    - *Undergirded by data/information*
      - Gathered, created, stored, disseminated

Vital for efficient system design

Responsibility of SMEs, Business Users

Preparation

Provide
Protection
Control
Access

Data/information

- Existing
  - Legacy data, reports, volume
  - Conversion, scanning?
- Anticipated
  - Inputs, outputs, volume
  - Reports, searches
- To be created
  - On-line, near-line, archived
  - User community
  - Change management

Preparation

Provide Protection

Control Access

Regulatory Environment

- Industry-specific regulations
  - State and Federal
- Data classification
  - Private vs. non-private
  - Access restrictions
  - Business unit owners
- Audit requirements
  - Frequency, scope
- Reporting requirements
  - Disease registries
  - Breach notification
  - Financial statements

Preparation

Provide
Protection

Control
Access

Security Specification

- Based on previous evaluations/discussions
  - Organizational sector
  - Regulatory environment
  - Privacy expectations
- Descriptive Text
  - Non-technical audience
  - ~ 5-10 pages
- Components of production security plan
  - Enterprise perspective
  - Specifics without details
- Framework – *auditability!!*

Part II: PLAN

Preparation

Provide Protection

Control Access

Security Specification

United States Government Accountability Office (GAO) *Federal Information System Controls Audit Manual* (FISCAM)
GAO-09-232G February 2, 2009
http://www.gao.gov/special.pubs/fiscam.html

SAS 70 (v.II) – AICPA - auditing InfoSec controls in financial systems
http://sas70.com/

Service Organization Controls (SOC) – AICPA – replacing SAS 70 in FY 2012)
http://www.aicpa.org/InterestAreas/AccountingAndAuditing/Resources/SOC/Pages/SORHome.aspx

Procurement

Security Specification

FISCAM: General Controls

Security Management – Enterprise-wide; risk assessment/ control, policies/procedures, awareness/training

Access Controls – physical/logical; identification, authentication, authorization, provisioning

Configuration Management – installation, maintenance, monitoring of hardware/infrastructure; software, systems/applications;

Segregation of Duties – no single point of human failure/ control

Contingency Planning – intrusion detection/prevention, incident response, data backup/recovery, BC/DR plans

Procurement

Security Specification

FISCAM: Business Process Application Controls

Completeness – input, processing, output only once per transaction

Accuracy – correct, timely input, accurate processing, reliable, accurate results

Validity – transactions actually occurred, authentic, approved, authorized, valid output

Confidentiality – data, reports, output protected against unauthorized access

Availability – data, reports, other information readily available when needed

Outline

Part I.

Introduction
Before the Beginning
Security Posture

Part II.

PLAN
Organization Characterization
Security Preparation
Security Specification

Part III.

DO
Procurement Participation
Design and Development
Vulnerability Controls
Assessment Instruments

CHECK
System/User Test Reviews
System/User Access Control

ACT
Pre-Operational
Operations and beyond

Procurement

Procurement participation

- Formal, controlled process
- Formal Project Management
- Legal implications
  - Vendor proprietary information
  - Restricted communications
- General sequence
  - Request for Proposal (RFP)
  - Vendor comments, questions
  - Response to comments
  - Proposal Evaluation
  - Final vendor selection
- Private organizations may not engage in formal Procurement!

Part III: DO

Procurement

Request for Proposal (RFP) design

- Introduction/Objectives/Goals
  - Paragraph form
- Legal/contractual requirements
  - Time frame
  - Regulatory requirements
  - Obligations
- General requirements
  - Architecture
  - Security, BC/DR
- Specific requirements
  - Subsystems
  - SME domains
- *Objectives-based requirements*

Note:
RFP is a legally binding document!

Procurement

Proposal Security Requirements

Based on Security Specification

Sentence statements ≠ requirements!

Not this:

…backups performed nightly, using DLT tapes; incrementals 6 nights, full 7th night; tapes archived off-site for 6 months, at least 25 miles from data center, recovery of lost data must be within 24 hours.

Design an incident response plan that… and an incident management plan consisting of….

But this:

…protected backup environment allowing prompt recovery of lost files, backups located sufficiently distant to prevent simultaneous loss with main data center.

Document and implement an incident response and management plan.

Procurement

Proposal Security Requirements

- "Objectives-based" requirements allow vendors to respond creatively
  - Too much detail can be restrictive and costly
- Address all of Security Specification
  - Late requirements are costly
- Eliminate redundancy
  - One requirement covers whole RFP
  - List all pertinent regulations, standards
  - Legal/audit requirements may be addressed in Legal/Contractual section
- Clear wording with Legal/Contracts

Include requirement for pre-op security assessment!

Procurement

Proposal Evaluation

- Led by Sr. Management
- Evaluate satisfaction with proposed solutions to requirements
- Legal tightropes
  - No conflict of interest with vendors
  - No open discussion with outsiders
  - Evaluate vendors separately, no direct vendor comparison
  - Equal time for all vendors
  - Be careful of hand-written notes.
- Vendors may be allowed to revise proposal

Procurement

Vendor selection

- Evaluation based on overall satisfaction of responses to requirements
  - Does vendor have an acceptable concept of enterprise security?
  - Did vendor propose acceptable solutions to specific requirements?
- Evaluators may not be selectors
  - Selection involves final evaluation and final cost/time proposals
- Final decision may be legally challenged!

Design and development

Requirements tracking

Three document sets:

- RFP security requirements
- Final vendor proposal
- System design documents

Vendor is bound to:

- Comply with RFP requirements
- Assert commitments to compliance in proposal
- Detail the compliance and fulfillment in the System Design Documentation

InfoSec Responsibility:

Track security requirements in Design Documents

Design and development

Document review

- Final design documents will be the foundation
  - Changes after "final" will cost
- Separate documents for each subsystem
  - General and Detailed sets
  - Detailed implementation description, screen shots, tables, users, data, etc.
  - Feeds into system analysis documents
- Looking for assertions of compliance with RFP
  - "shall", "will", "intend…"
- Document omissions, errors, unclear statements

Part III: DO

Design and development

Document review

- Additional documents:
  - Security plan
  - Architecture design
  - BC/DR plan
  - Risk management plan
  - Change management plan
- Require Preliminary and Final versions
  - "Preliminary" will have assertions ("will", "shall")
  - "Final" versions to be completed before Operations
  - "Final" versions will be part of Operations documentation.

Part III: DO

Design and development

Documenting vulnerabilities

- Catalog the errors, omissions, etc.
- Clarify with RPF requirements list
  - Check and recheck
- Review corrected documents for resolution (assertions, etc.)
  - May be copy or typo errors
  - Looking for patterns, e.g. no accounting for data protection in transit, contradictions from document to document
- Cataloged list of vulnerabilities can be basis for final (pre-op) security assessment

Final Review

Pre-Ops Security Assessment

Have all the assertions been satisfied?

- Based on selected standard, e.g., FISCAM
- Internal assessment, not formal audit
    - Employ audit testing methodology
    - Preserve "audit evidence" for future reference
- Advocative, not adversarial
    - Collaboration, not confrontation
- Emphasize vulnerabilities identified in documents
    - Look for final versions of documentation and Operations policies and procedures
- May include BC/DR test
    - Paper/walk-thru or formal full recovery test

Testing

System testing

Does it do what we asked for (functionality)?

- Testing functional system interaction
  - Usually performed by vendor, with oversight of org. representatives
  - May also include stress testing
- InfoSec may not be directly involved
  - Review reports
- Ask about InfoSec test problems
  - Access and data protection
  - System interface exchanges
  - System performance and error logs

Testing

User acceptance testing

Does it operate as we expected (performance)?

- Testing operational service agreements
  - Usually performed by sets of users, targeting specific subsystems
  - Simulates live system, but still pre-op
- Involves transferred/converted data
  - From legacy system
- Look for InfoSec test problems
  - Interface transfers
  - Number/count balances
  - System performance and error logs with large numbers of users

Testing

User interface

Does it restrict appropriately (access control)?

- Provisioning process
  - Identification – user ID, password
  - Authentication – system validation of ID
  - Authorization – permission
  - Deactivation – legal concerns
  - Monitoring – review of active and inactive accounts, login successes and failures
- Testing by attempting to break in
  - Normally and abnormally
  - Local and remote
  - Error messages

Testing

Other tests

- Conversion testing (ETL)
  - *Extraction* – obtain data from legacy system
  - *Transformation* – align legacy terminology to new system
  - *Loading* – formal move of data from legacy to new environment
  - CAREful planning required!
  - Protect private data!!
- Network testing
  - Network node discovery
  - Penetration tests, common vulnerabilities
  - Web interface evaluation
  - *PERMISSION!!*

Wrapping up

Operational Readiness

- "Parallel" system testing
  - Performing same services in legacy and new system
  - Difficult to be exactly "parallel"
- Final load of legacy data
  - Protect private data!
- System functioning as operational
  - Full user, support population
  - All servers/networks active

Wrapping up

Operational Readiness

- Validation
  - Have all requirements been addressed/fulfilled?
- Verification
  - Does the system perform the functionality correctly?
  - Does the system meet the Service Level Agreements?
- Certification/Accreditation
  - Specific federal or industry certifications/ standards
  - Formal approval of security assessment
- Acceptance
  - Formal sign-off, triggers final payment(s)

(Not universally accepted categories!!)

Wrapping up

Go-Live - Operations

The Discipline of Information Security

- Ending, but True Beginning
- Operations InfoSec tracking
  - First-year adjustments
  - Post-op audits
  - Change control
  - Contracted assessments/audits
  - Reports – logs, changes, tests, etc.

"The world is too much with us..."

Wordsworth, 1888

Operations

RSA. 2010. Cybercrime and the Healthcare Industry.
RSA White Paper, RSA Security LLC.
http://www.rsa.com/content_library.aspx
(highlights added)

"With the pervasiveness of information being made available electronically, healthcare organizations are increasingly attracting cybercriminals. As evidence of this, nearly one out of every six data breaches that occurred in 2009 was targeted at the healthcare industry, according to the Open Security Foundation. Certainly, that number is expected to grow."

"The world is too much with us…"

Wordsworth, 1888

Operations

RSA White Paper, continued:

"Why? There are numerous reasons. For one, it pays. The World Privacy Forum has reported that the street cost for stolen medical information is $50, versus $1 for a stolen Social Security number. The average payout for a medical identity theft is $20,000, compared to $2,000 for a regular identity theft. Second, it is harder to detect. Medical information fraud takes more than twice as long to identify as compared to regular identity theft. Simply put, victims can close a compromised bank account, but they can't delete or change their personal information, medical records or history of prescription use."

Data from Javelin Strategy & Research, 2010

Part III: ACT

"The world is too much with us…"

Wordsworth, 1888

Civil money penalty

HHS.gov

HHS Imposes a $4.3 Million Civil Money Penalty for HIPAA Privacy Rule Violations

http://www.hhs.gov/ocr/privacy/hipaa/news/cignetnews.html

The HHS Office for Civil Rights (OCR) has issued a Notice of Final Determination finding … Cignet Health of Prince George's County, MD (Cignet), violated the Privacy Rule of … (HIPAA). HHS has imposed a civil money penalty (CMP) of **$4.3 million** … representing the first CMP issued by the Department for violations of the HIPAA Privacy Rule. The CMP is … authorized by Section 13410(d) of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Press release: http://www.hhs.gov/news/press/2011pres/02/20110222a.html

Part III: ACT

"The world is too much with us..."

Wordsworth, 1888

Marcus Ranum

Chief of Security
Tenable Network Security, Inc.
mjr@tenablesecurity.com

Information Systems Security Association
The Global Voice of Information Security

6th Annual Triangle (NC)
InfoSeCon; October 21, 2010.

"Advanced Persistent Threats:

Coping with the truth behind the hype"

Advanced: Technical skills/tools we (most of us) haven't seen
Persistent: Extreme patience, slow, careful, difficult to detect
Threats: Harmful intent - capture of valuable data

Paraphrased quotes:

If organizations do not have a strong technical support staff, they have lost the battle.

How can we make attackers' costs go up??

[heavy sigh]

Health Net, Inc. Investigating Unaccounted-for Server Drives
03/14/2011
http://healthnet.tekgroup.com/article_display.cfm?article_id=5529
(highlights added)

"…follows notification by IBM, Health Net's vendor…that it could not locate several server drives.…Health Net has determined that personal information … is on the drives, and may include names, addresses, health information, Social Security numbers and/or financial information."

IBM says it can't find hard drives with 2M health records
03/15/2011
http://wraltechwire.com/business/tech_wire/news/blogpost/9270864/

"…the California Department of Managed Health Care placed the number [of people affected] at 1.9 million.… "Obviously something went wrong, but we don't know," … spokeswoman … said. Health Net…would not say whether the drives were stolen."

[heavy sigh]

N.J. state computers nearly sold with sensitive data 03/10/2011

http://www.reuters.com/article/2011/03/10/us-computer-snafu-idUSTRE7296KC20110310

"Child abuse reports, Social Security numbers and other highly sensitive data were discovered on a batch of government computers headed for the auction block to be sold by the State of New Jersey….
State workers preparing the equipment for sale had opted not to use a device designed to magnetically erase sensitive data from hard drives because it was noisy, the comptroller's office said in a news release.

Part III: ACT

Gauntlet down!

IT Is Too Darn Slow - 02/26/2011

http://www.informationweek.com/news/global-cio/interviews/showArticle.jhtml?articleID=229218781

"….security and regulatory compliance make business IT more complicated than consumer IT, but security can't be the overriding excuse for not moving faster.

CISOs must bring more of a business point of view to their security judgments…. CISOs must weigh a delay against the risk and decide if the app can be rolled out and any problems resolved along the way.

Again, it's velocity over perfection--and it's heresy to some security pros. "CISOs need to get comfortable with that,"….

CISOs also need to … [automate] more security testing….

"Reserve these really good security people for the really difficult security problems,"…. Too often, the interpretation of a law or regulation gets debated anew with every security problem.

Operations

Redefining InfoSec role

- Current view of ISO
  - Part of IT technical support
  - *Operational/tactical* planning
  - User account management
  - User training, testing
  - Policy/procedure documentation
  - BC/DR planning, testing
  - Log review, incident response
    - Interrupt driven
    - Fire-fighting
    - *Detection/Response oriented*

Operations

Redefining InfoSec role

- New view of ISO
  - Independent of IT (conflicts)
  - InfoSec *strategic* planning, management
    - Information life cycle protection
    - Technology change management
    - Development project planning
    - *Anticipation oriented!*
  - Collaborator, coordinator, bridge-builder
    - Privacy/Risk/Audit
    - Service continuity
    - IT Tech Support
    - Safety/physical security
  - ***The Discipline of Information Security***

Tough Challenge!

Is it a losing battle?

Questions?

Answers?