FORRESTER®

Chenxi Wang, Ph.D.
Forrester Research

- Principal Analyst, Security and Risk Mgmt
- Responsible for covering
  - Application Security
  - Content Security
  - Emerging technologies and threats
- Prior roles include Associate Professor at Carnegie Mellon university, Chief Scientist for KSR, Inc.

FORRESTER®

Addressing compliance with automatic vulnerability management

Chenxi Wang

Qualys Webinar

December 6, 2007

Agenda

- Regulatory compliance
  - PCI
  - Sarbanes-Oxley
  - HIPAA
  - Others
- Best practices for vulnerability management for compliance

PCI compliance

- PCI DSS requires you to main a vulnerability management program
  - 2.2: Develop configuration standards for all system components
  - 6.1: Ensure all system components and software have the latest vendor-issued patches
  - 11.2 Run internal and external system scans at least quarterly and after any significant changes (external by PCI certified scanning vendors)

Reality

- Changes happen often on the network
  - » New devices
  - » New applications
  - » New components
  - » New partners
- Ensuring all systems conform to policies is a non-trivial task

Price of non-compliant

- A monthly fine of $25,000 for non-compliant level 1 merchant
- A monthly fine of $5,000 for non-compliant level 2 merchant

Sarbanes-Oxley

- Governs operations of public companies, strengthens corporate accountability
- Section 404 has specific requirements on security
  - » “secure operating systems, database, network, firewalls and infrastructure”
  - » Demonstrate appropriate internal controls to safeguard financial processes

Steps to achieve SoX 404 compliance

- Establish an audit and self-assessment processes
- Establish “gold standards” for device security
- Access current state of the system
- Identify & remediate significant deficiencies in IT competency
- Product reports for auditors
- Repeat above three steps

HIPAA compliance

- Governs the protection of personal health information (PHI)
- Who must comply to HIPAA
  - » Health care provider, health insurance, hospitals, and any organizations that handle electronic personal health information

HIPAA compliance

- PHI must be kept confidential and secure
- Must have security measures to enforce the confidentiality of PHI (administrative, technical, physical safeguards)
- "…assess potential risks and vulnerabilities to such information in its possession in electronic form, and develop, implement, and maintain appropriate security measures to protect that information. Importantly, these measures are required to be documented and kept current."

OCR statistics

- 26,000 complaints of privacy breaches since 2003
- 4,100 have been determined to be actual violations of federal rules

- How many more are unreported?…

What does all this mean?

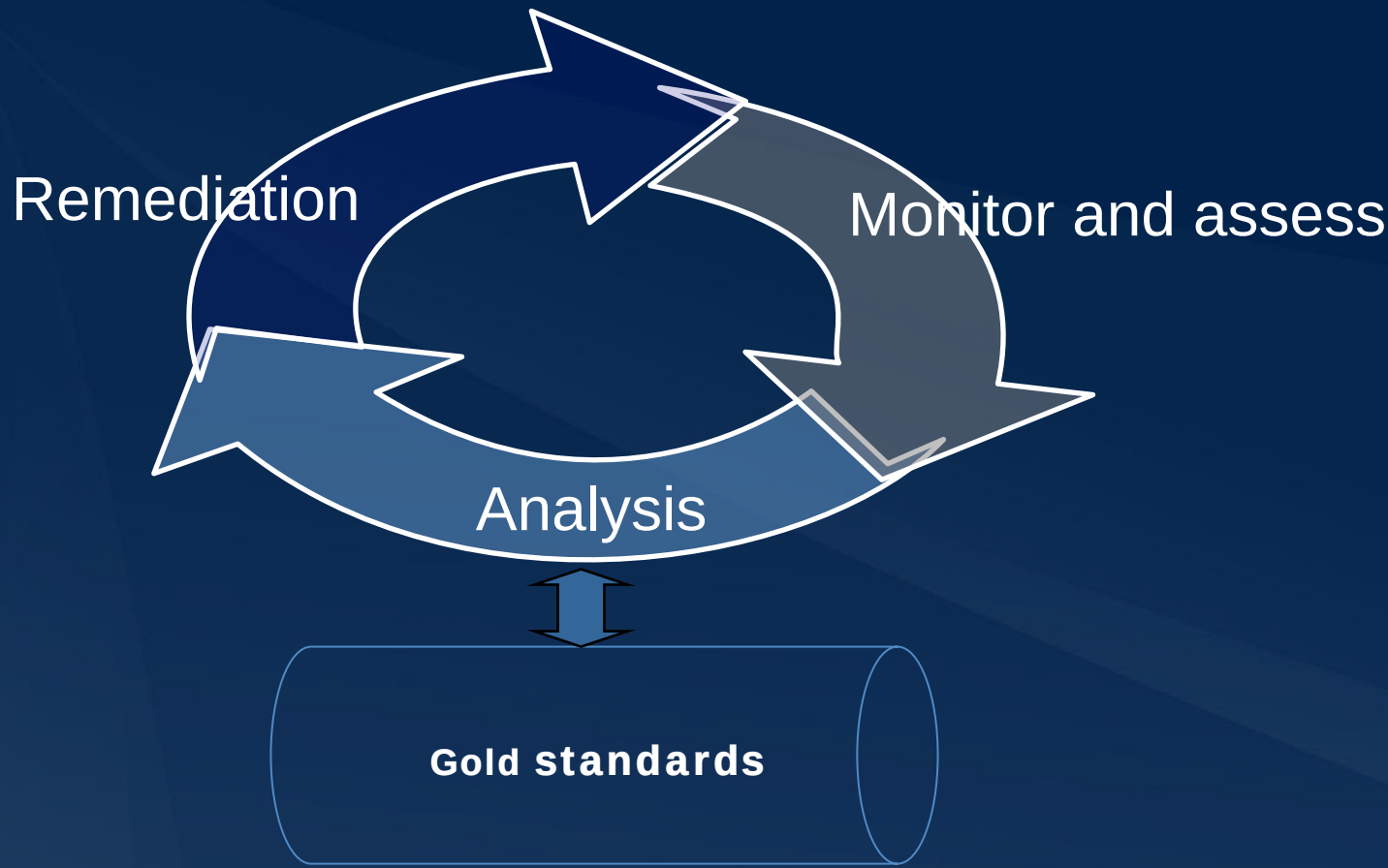
Security is unattainable without vulnerability management

Continuous scanning of your network is an essential step to compliance

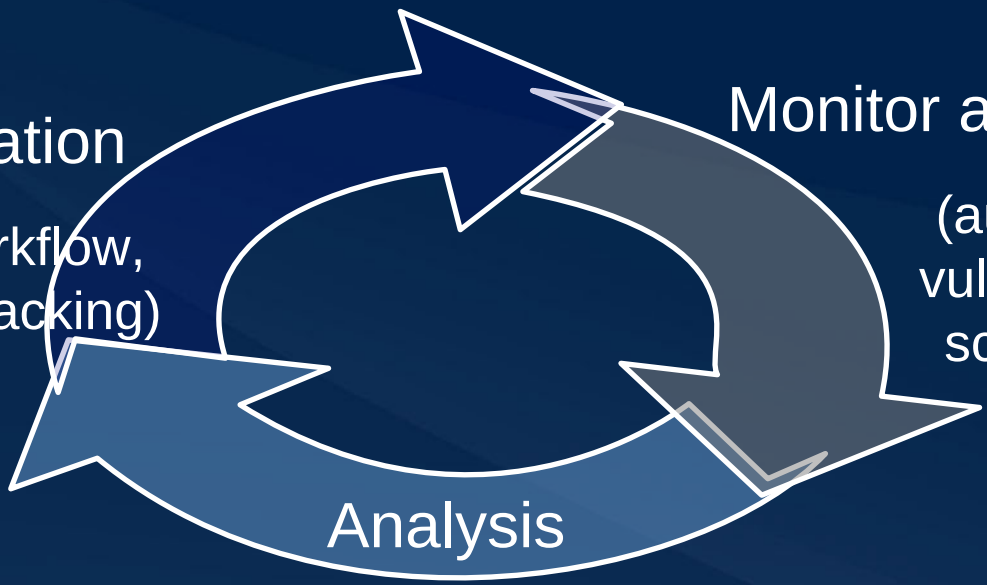
Regulations require

- Continuous evaluation of your IT security postures
- Continuous discovery, analysis, and monitoring of vulnerabilities and compliance of devices
- Timely implementation of security measures to mitigate risks and vulnerabilities

You need to establish a vulnerability management program



Vulnerability Management Diagram



(Risk and criticality analysis
Remediation analysis)

FORRESTER®

Other aspects of the program

- Should include external partners and service providers
- Consider internal compliance
  - » Internal regulations requiring the establishment and maintenance of secure IT infrastructure
  - » Ensuring infrastructure security needs same measures as those for government regulations

How well are people doing?

Case study: Standard chartered bank

- SCB has 60,000 employees operations in >50 countries
  - » Very complex network environment with diverse platforms and applications
- Manual audits are impossible
- Automatic scanning provides them with an accurate inventory of network topology and assets
- SCB can quickly identify and prioritize vulnerability remediation
- Vulnerability scanner also helped identify viruses that were uncaught by firewalls, IDSes, and AV products

Case of non-compliance

- TJX International
  - A $13 billion retail empire in US
- TJX has firewalls, anti-virus products
- But internal wireless communication between employee laptops and servers is not encrypted
- Attackers used wireless antenna to tap into the network and stole 45 million credit card and account numbers
- **Visa fined TJX nearly $1 million, and $100,000/month until compliant**
- **TJX's overall loss is $25 million and counting …**

Best practices for vulnerability management

Steps to compliance

- Initiate a risk assessment procedure internally
  - » What resources are important to you? What devices? Infrastructure components? Applications?
- Determine what needs to be scanned & how often
  - » Establish a policy
- Establish the management/remediation processes
  - » Who is responsible for scanning?
  - » Steps to follow when vulnerabilities are discovered?
  - » Who is responsible for remediation? Chain of escalation?

Best practices

- For critical assets, maintain weekly or even daily scanning
  - » e.g., web servers, firewalls, financial web apps
- Other assets, monthly or quarterly scanning
- For critical vulnerabilities (e.g., remote exploitable)
  - » Mean time to fix should be less than 48 hours
- Use data to understand the effectiveness of your controls, vulnerability history, and security postures

Best practices

- Your VA process should include
  - » An enterprise workflow system to assign, track, and validate remediation tasks across the enterprise
- Procure regulatory compliant vulnerability management technologies
  - » e.g., PCI certified
- Run periodic penetration testing to validate your security status

Vulnerability management technology selection criteria

What to scan on the device

- It exists
- Services & apps running on the device
- Vulnerabilities
  - » Extra apps or services
  - » Patch versions
  - » Configuration error (default account is on)
  - » Application or system vulnerabilities

Selection criteria for VA (Technology)

- Scanning capabilities
  - » Ability to provide network coverage, asset discovery, depth of scanning, and versatility of working with different platforms
  - » Ability to discover known vulnerabilities
  - » Comprehensive vulnerability coverage and up to date info
  - » Ability to perform internal & external scans
  - » Operations do not interfere with normal operations
- Remediation support
  - » Actionable guidance for remediation
  - » Integration with trouble ticketing systems

Selection criteria for VA (Management)

- Enterprise support
  - » Scalable to hundreds of thousands of devices, systems
  - » Support centralized management
  - » Support for distributed scanning and central analysis
  - » Ability to automatically scan on schedule, on demand
- Reporting
  - » Cater to macro and micro information needs
  - » Customizable
  - » Role-based reporting

Services vs. on-premise solutions

- Vulnerability scanning should be on schedule, on demand
  - » Without human supervision
- On-premise solution requires setting up a scanning apparatus – more operational overhead
- Services allows complete scanning on demand
- Ability to deliver signature updates more quickly

To summarize …

Vulnerability Management Maturity Model

Phase I → Phase II → Phase III

- Predominately reactive measures: patch management
- Ad hoc scanning and penetration testing
- Isolated web application firewall deployment

- Proactive security measures
- Established process for systematic scanning and penetration testing
- Systematic tracking of vulnerability databases

- Enterprise-wide vulnerability management policies
- Integrated with corporate risk management
- Integrated with enterprise workflow system
- Clearly defined success metric
- Ongoing and proactive vulnerability management

Thank you

Chenxi Wang, Ph.D.

cwang@forrester.com

Principal Analyst

Forrester Research, Inc.