The Value of Vulnerability Management*

*ISACA/IIA Dallas

Presented by:

Robert Buchheit, Director
Advisory Practice, Dallas

Ricky Allen, Manager
Advisory Practice, Houston

*connectedthinking

PRICEWATERHOUSECOOPERS

Agenda

The need for Vulnerability Management

Common Vulnerabilities

Vulnerability Management Defined

Five Step Vulnerability Management Process

Vulnerability Management Benefits

Closing

The Problem:

IT costs are spiraling out of control and are among the top 5 corporate expenditures. On average, 15-25% of IT spending is wasted* and budgets are increased by only 5% per year. Information Security expenses are rising due to an alarming number of new vulnerabilities and compliance requirements (source: Aberdeen, The Strategic IT Budget Report Realities Benchmark Report, Bill Malik, Oct 2004)

U.S. Companies spent an estimated $15.5B in 2005 on compliance and will spend $80B in 2005 through 2009 to ensure compliance with regulatory requirements (source: AMR)

What is the cost of an incident?

- ChoicePoint granted unauthorized access to 145,000 customer accounts and spent $11.4 million in internal costs to remediate. Market capitalization dropped by $720 million
- Identity Theft Protection Act

  $11k – $11 million fine per incident
- 21 States currently required customers to be notified when their personal data has been lost
- Customer data compromise cost each company between $14 and $50 million
- Average total recovery costs were $140 per lost customer record
  - Lost Customer Information: What Does a Data Breach Cost Companies, Ponemon Institute
- FBI/CSI Survey showed an average loss of proprietary information to be $355,552.
- 95% of successful attacks are from known vulnerabilities according to CERT
- CERT reported that 5,990 new vulnerabilities were discovered in 2005, a 158% increase over 2004.

What is a vulnerability?

"A weakness of an asset or group of assets that can be exploited by one or more threats" (source: ISO 17799:2005)

Common vulnerabilities:

Un-patched or out of date software

Default or weak system passwords

Untrained users (lack of security awareness)

Weaknesses in facilities or infrastructure

A vulnerability is more than just a technical issue, it can be a weakness in ANY asset, process, or a policy violation which can be exploited to compromise security.

Traditional Vulnerability Assessment

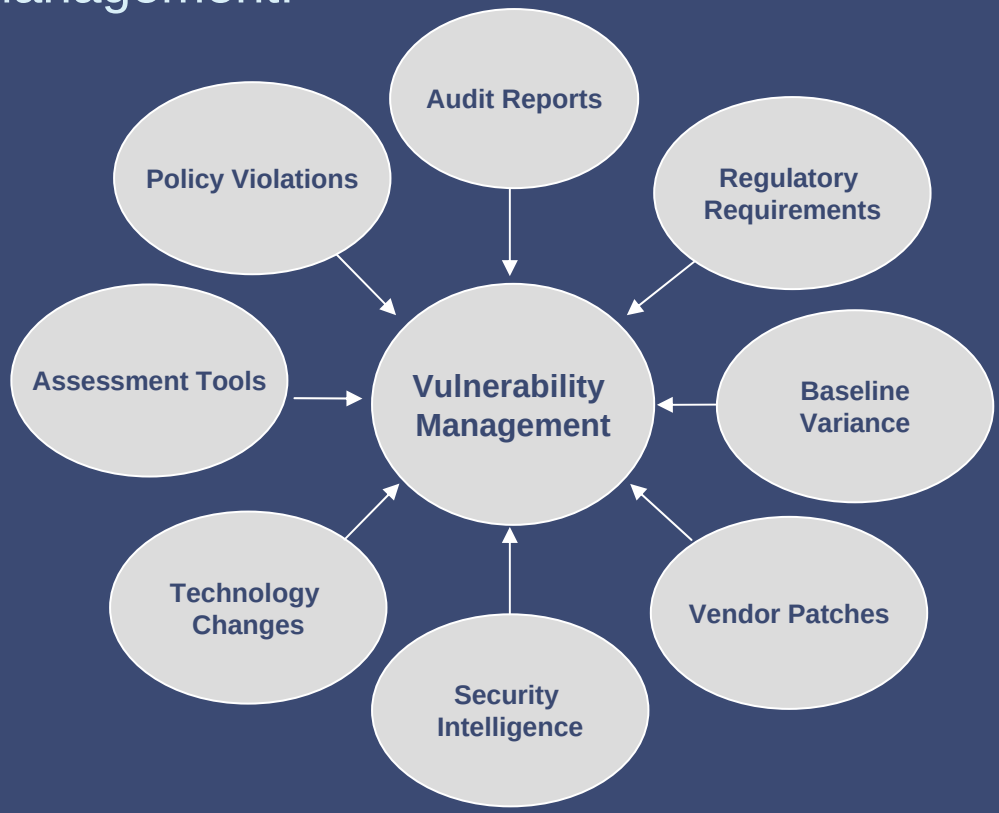
Vulnerability assessments has been a key part of most information security programs. Traditionally, vulnerability assessment has been a pure technical solution without remediation processes and business unit involvement.

Standard Issues Include:

- Technology driven program
- Expert technical knowledge required
- Tried to remediate ALL identified vulnerabilities
- Difficult to track the never ending process
- Limited by capabilities of assessment tools

What is Vulnerability Management?

The people, processes, and technology used to reduce the exposure of corporate assets. Vulnerability management addresses the entire lifecycle from identification to remediation. Many issues point to the need for vulnerability management:



Five Step Vulnerability Management Process

Assess	Analyze	Strategize	Align	Communicate
• Determine current security initiatives • Staff Capabilities • Leverage Asset Management	• Collect Information from various feeds • Identify vulnerabilities • Determine root causes	• Develop an action plan for remediation • Develop an effective risk weighting system for vulnerabilities • Utilize business understanding to prioritize vulnerabilities	• Align priorities with IT to reduce vulnerabilities on critical systems • Align with other IT processes to reduce the effort of remediation	• Communicate the value of remediation efforts • Difficulties communicating technical issues to a business audience

1. Assess the environment by collecting information through interviews, scanning, diagrams and documentation. Determine what regulatory, compliance and industry requirements are involved with managing vulnerabilities.

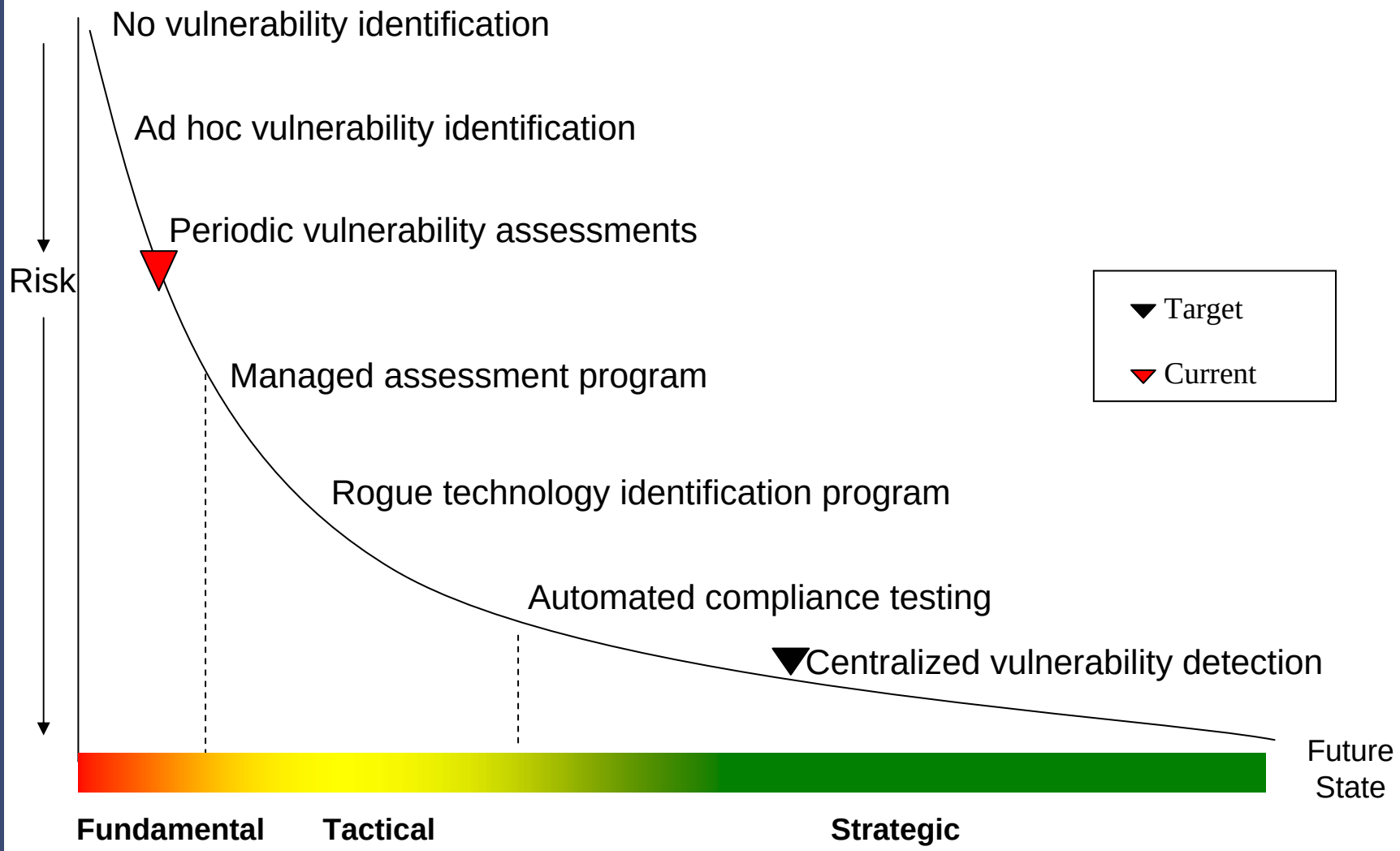
2. Determine if assets have been classified for business criticality and are tracked through an asset management database. Discover rogue systems and devices and begin efforts to identify owners for the business need for unmanaged technologies.

3. Assess the existing infrastructure to identify security policies and risk management models. Translate policies to technical checks such as the enforcement of an 8 character password or the use of default system passwords.

4. Understand the resources that belong to your organization and which do not. A reliable asset management process is necessary for the success of any vulnerability management program. The asset management solution should be able to tie into the help desk and trouble ticket system for centralized tracking.

5. Identify and understand current business and technology objectives that require security involvement. Identify business drivers and how IT and security can drive the results.

Vulnerability Identification Capability Curve



1. Security Intelligence information can significantly decrease the time required to apply and deploy patches in the organization. A database is maintained with your technologies and Alerts will only be sent when you are affected.

2. Analyze existing audit and security reports to identify existing security weaknesses. Review Sarbanes Oxley IT or SAS70 Controls to identify critical systems in the environment.

3. Vulnerability scan output should be analyzed to remove false positives and insignificant findings. Track the new, reoccurring and corrected vulnerabilities.

4. Identify change control windows allowed for scanning across the organization. Work with IT management to obtained an agreed upon time and intensity of scanning. Regardless to the tool or methodology, a risk exists to crash the server.

5. Analyze the identified vulnerabilities to make sense of the information. Combine or remove vulnerabilities and identify root causes.

1. Address strategy to evaluate identified vulnerabilities and determine false positives, criticality and feasibility. Determine the acceptable limit of false positives allowed in each report. Work with the vulnerability assessment tool vendor to reduce the number of false positives.
2. Prioritization and validation of vulnerabilities is one of the most time consuming but important steps. Work within configuration baselines for each technology to identify and document the remediation steps required.
3. Develop an effective risk weighting system for vulnerabilities which takes business processes, asset value and likelihood to determine risk ratings. See the vulnerability evaluation checklist*
4. Focus on the high risk areas for the company first to protect perimeters and critical business applications. All of the identified vulnerabilities (potentially 10,000+) do not need to be corrected immediately.
5. Combine reports from various tools and processes to obtain a holistic understanding of the risk to the applicable applications, technology, processes and personnel.

Vulnerability Evaluation Checklist

- Does the vulnerability affect systems within the organization's network?
- Are critical business systems impacted by the vulnerability?
- Do hosts run the vulnerable version of software?
- Can the vulnerability be exploited remotely?
- Is a patch available for the identified vulnerability?
- What is the relative ranking provided by the vendor or assessment tool?
- How prevalent is the vulnerable application on the network?
- Can the vulnerability be mitigated?
- Are there exploits available for this vulnerability?
- Has a propagating worm been developed?
- Do security policies and standards need to be updated in response to this vulnerability?

1. Align priority vulnerabilities with asset classification to remediate the highest risk systems first. Leverage deployment and configuration management technology for speedy remediation.

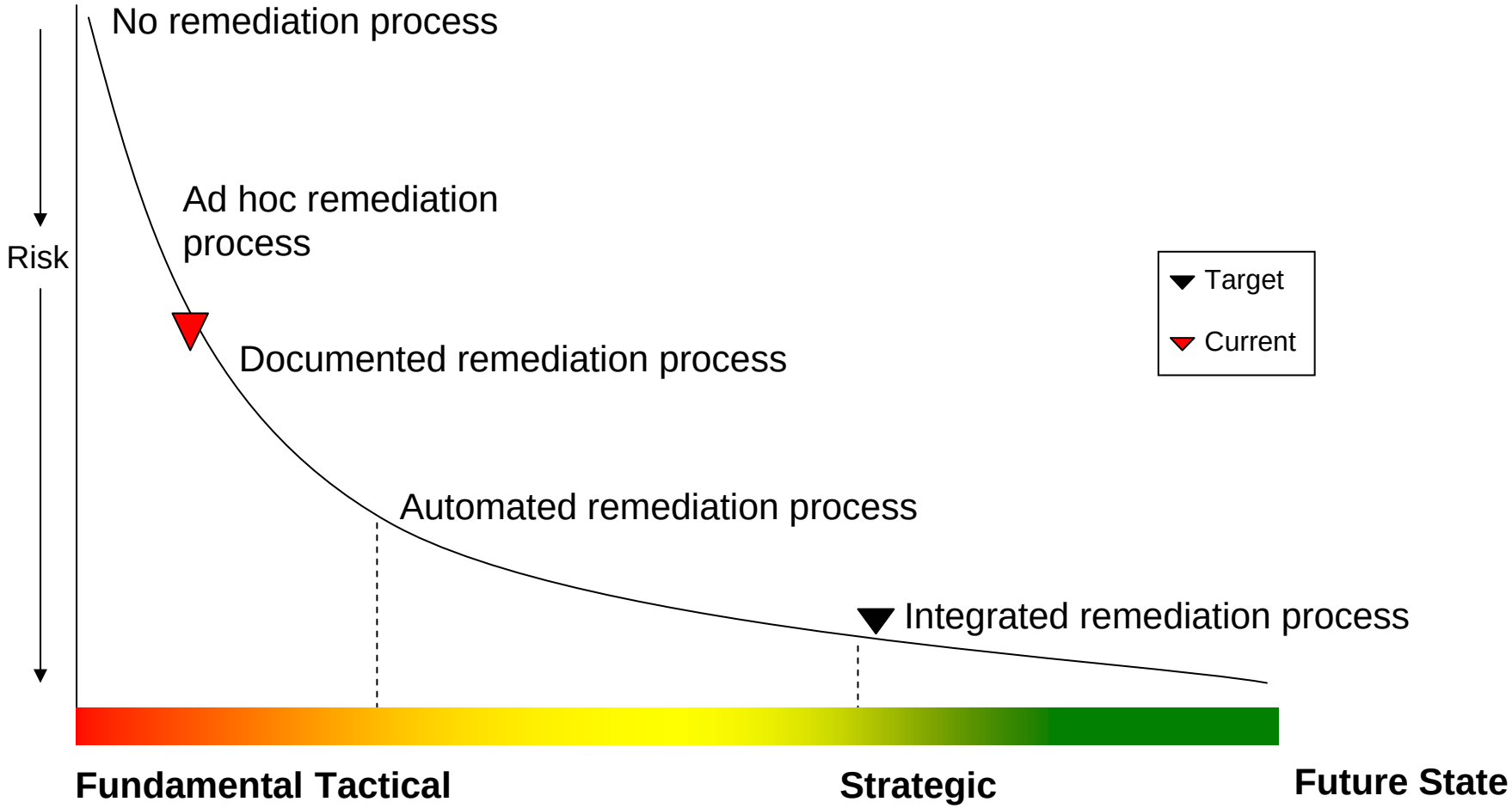
2. Change control and testing processes are important when deploying and tracking security remediation changes. Many vulnerability management products will integrate with existing trouble ticket systems, to effectively track time and resources.

3. Significant cost savings can be realized by integrating software to automate the deployment of remediation patches, changes and updates. Remediation is the most important step of the entire process.

4. Vulnerability management is dependent on other processes such as automated patch management, change control and incident response to effectively operate.

5. Perform compliance monitoring through continued scans to verify the vulnerability is corrected. System restores and new patches may reintroduce the vulnerability.

Vulnerability Remediation Capability Curve



1. Communicate the current status of the vulnerability management program to management on monthly intervals. Define the key issues and challenges for your organizations security program and the progress you have made to achieve the goals. Integrate the vulnerability management progress with your other security initiatives.
2. Map protection efforts against business applications and not just physical servers. Reporting should also created based on the existing organizational chart, usually by business unit or geographic region.
3. Identify the metrics that show creditable change in the organization. Traditional metrics such as; 40,375 vulnerabilities were identified should be replaced with; internal security incidents are down 84% and system uptime is 99%.
4. Identify efficiencies that can be gained by improving the process and communicate them to the vulnerability management team.
5. While it may be difficult to show impact to corporations earnings, profitability and shareholder value, show how much you can save by reducing risk to the organization and by being prepared for an incident to limit overall impact.

How to get results

Participants

- Business unit and/or process area representatives
- Project Teams
- Information Security
- Information Technology
- Risk / compliance

- Prioritized Remediation Roadmap
- Maintenance organization identified
- Roles / responsibilities
- Hardening Procedures
- Enabling technology requirements identified
- Response procedures

- Training requirements identified
- Ongoing monitoring requirements identified
- Effectiveness metrics
- Policies and procedures identified
- Reduced Vulnerability Signature
- Compliance program

Where savings occur

❶ Have a well defined process workflow
❷ Reliable asset management process
❸ Efficient scanning and identification
❹ Drawing vulnerabilities from multiple processes and not just a technology
❺ Security intelligence services can reduce research time significantly
❻ Integration with trouble ticket system to track compliance and cost
❼ Use of automated configuration management remediation tools
❽ Standard platform baselines help define the gap and reduces vulnerabilities
❾ Reduce wasted time chasing down the system owner and location of unmanaged systems.
❿ Show executives that action is being taken and that the process is working

The Value of Vulnerability mgmt

Reactive measures are not enough to deal with current vulnerabilities. Zero day attacks are here and worms can propagate faster than we can deploy patches. The value of a vulnerability management program:

- Increases compliance with regulatory issues (e.g., SOX, HIPAA, PCI) by enhancing the control network
- Creates increased transparency with management by collecting and automating reports for executive dashboards
- Improves management of IT assets and processes
- Reduces risk by more effectively allocating controls

CISO Forum

“There is still a tendency within security organizations to focus on **reactive** security rather than taking a **proactive** approach. **Reactive** security appears, at first hand, to be less resource-consuming, with faster results and more flexibility, but this is a misconception. In the medium to long term, **reactive** security provides no scope for growth or adaptation and amounts to little more than expensive firefighting.”

“**Proactive** security requires early identification of the business and technical requirements that can give a security chief the necessary edge to build an organization flexible and adaptable enough to provide holistic services, meeting both immediate need and providing structure for future growth. Taking the time to get it right in the early stages reaps huge benefits in the long term.”

Craig Thomas, Global CISO, PricewaterhouseCoopers LLP

Questions?

For more information and to download our latest Whitepaper: “How to align security with your strategic business objectives”, please visit:

www.pwc.com/techspotlight

Other Questions:

Robert Buchheit
robert.buchheit@us.pwc.com
214-754-4516

Ricky Allen
richard.allen@us.pwc.com
713-356-5155

PRICEWATERHOUSECOOPERS