



**TENABLE**

Network Security<sup>®</sup>

***Maximizing ROI for Vulnerability  
Management***

# Carole Fennelly

---

- Director of Content and Documentation for Tenable Network Security
- Technical writer on Information Security
- Editor of CIS Solaris 10 benchmark
- Co-founder of Hacker Court

# Overview

---

Businesses spend money to make money.

Choices for how money is spent:

- Develop proactive Vulnerability Management program
- Pay for cost of breach and cleanup

# Dataloss Statistics

Data reprinted with permission from [datalossdb.org](http://datalossdb.org). For any questions about this site or the data contained within the site, please contact [curators@datalossdb.org](mailto:curators@datalossdb.org).

## Largest Incidents

RECORDS	DATE	ORGANIZATIONS
<u>94,000,000</u>	2007-01-17	TJX Companies Inc.
<u>40,000,000</u>	2005-06-19	CardSystems, Visa, MasterCard, American Express
<u>30,000,000</u>	2004-06-24	America Online
<u>26,500,000</u>	2006-05-22	U.S. Department of Veterans Affairs
<u>25,000,000</u>	2007-11-20	HM Revenue and Customs, TNT
<u>17,000,000</u>	2008-10-06	T-Mobile, Deutsche Telekom
<u>12,500,000</u>	2008-05-07	Archive Systems Inc, Bank of New York Mellon
<u>11,000,000</u>	2008-09-06	GS Caltex
<u>8,637,405</u>	2007-03-12	Dai Nippon Printing Company
<u>8,500,000</u>	2007-07-03	Certegy Check Services Inc, Fidelity National Information Services

# Dataloss Statistics

Data reprinted with permission from [datalossdb.org](http://datalossdb.org). For any questions about this site or the data contained within the site, please contact [curators@datalossdb.org](mailto:curators@datalossdb.org).

## Latest Incidents

[twitter/](#) DataLossDB

RECORDS	DATE	ORGANIZATIONS
<u>2,300</u>	2009-03-11	Gwent Police
<u>1,000</u>	2009-03-09	Sonoma County Sheriff
<u>59,000</u>	2009-03-06	UPS, Idaho National Laboratory
<u>50</u>	2009-03-06	Federal Emergency Management Agency
<u>60,000</u>	2009-03-06	Bottle Domains
<u>3,470</u>	2009-03-06	New York City Office of Payroll Administration, The Organization of Staff Analysts
<u>1,393</u>	2009-03-05	Landlord's Source Centre
<u>80,000</u>	2009-03-04	New York City Police Department
<u>242</u>	2009-03-04	St. Rita's Medical Center
<u>520</u>	2009-03-04	Elk Grove Unified School District

# Vulnerability Management Programs Goals

---

## Demonstrate Compliance

- Meet the minimum requirements of compliance checklists
- The focus is on getting “the clean scan”

## Secure Systems

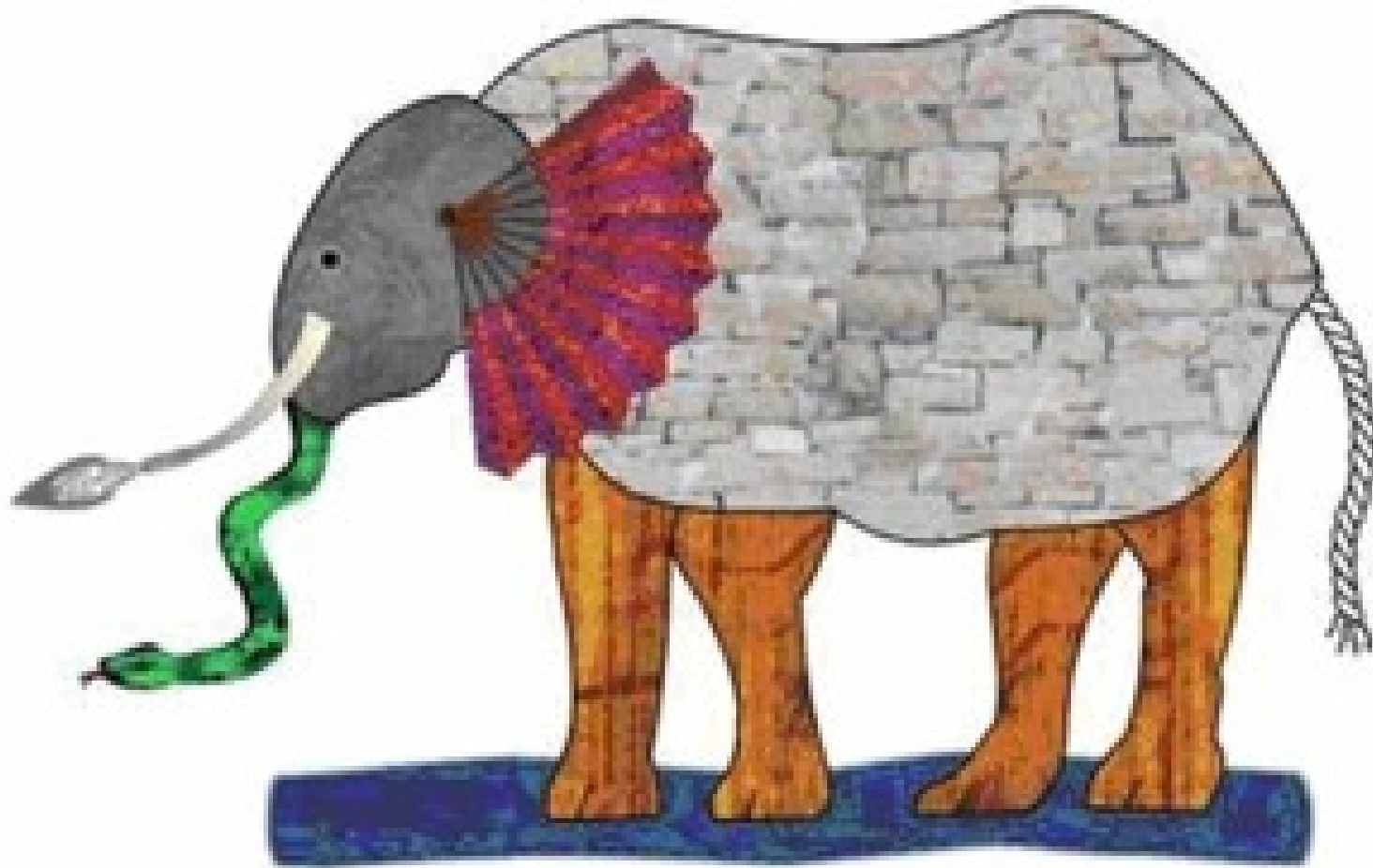
- Create a proactive Vulnerability Management program

# Typical Problems

## Lack of Corporate Direction

- No clear-cut policy
- Lack of defined process
- Failure to achieve consensus between business, IT and security

# Blind Men & the Elephant



# Typical Problems (cont'd)

## Lack of Resources

- Insufficient funding to buy the appropriate tools and supporting infrastructure
- Qualified staffing to deploy, manage and maintain the tools
- No organization and process to support the program

# Typical Problems – Cont'd

## Ineffective Scanning

- Only looking for vulnerabilities
- Patch Audits
  - False positives
  - No patches available for older systems
- Relying on Anti-virus
  - Does not plug the attack vector
  - May have vulnerabilities themselves
- Not Using Credentials
  - Credentialed scan gets information about hardware drivers and configuration

# Making it Payoff – Risk Analysis

- Identify Assets
  - Critical business servers
  - Critical infrastructure devices
  - Managed servers
  - User / Desktop
  - Off-site (VPN, Managed)
  - Production servers
  - Development servers
  - Test systems
- Classify Data
  - Patient Health Information
  - Credit Card Data
  - Client Financial Data
  - Intellectual Property
  - Material Non-public
  - Business Critical Data

# Making it Payoff- Requirements

## Create a Vulnerability Program Blueprint

- Business requirements
- Technical requirements
- Product requirements for implementation
- Operational Requirements (who and how to run it)
- Scanning and Reporting Process
- Budget (product costs, staff hours)
- Roles and Responsibilities
- Metrics

# Making it Payoff: Solution Analysis

- What is already in-house?
- Is it supported on/can scan multiple platforms?
- How well does it scale?
- Do the features align with technical and business requirements?
- Costs (both one time and recurring)
- What is the long-term viability of the product?
- What is the update process?
- What is the learning curve?
- What could it break?
- How effective and flexible is the reporting?
- Who else uses it?

# Making it Payoff- Solution Analysis

- Third Party
  - **Managed Service**
  - **Penetration Testing / Vulnerability Assessments / Compliance Audits**
- In-house
  - **Patch Management**
  - **Configuration Management**
  - **Incident Response**
  - **Software Development**

# Making it Payoff- Motivation to Deploy



## Fluffi Bunni OWNZ YOU.

A BamBam here a dot slash there  
here a dot there a slash  
everywhere a dot slash

look mommy im on sans !

# Making it Payoff - Deployment

- Establish a Baseline
- Tune scanning parameters
- Scan scheduling
- Correlate Results
- Analyze Results
- Communicate Results
- Mitigation and Remediation
- Develop Trending Reports
  - Status vs risk metrics

# Conclusion

---

Compliance requirements can provide useful checklists to ensure you've addressed specific security concerns, but it is dangerous to base a vulnerability management program solely on a checklist.

A proactive vulnerability management program that addresses specific business needs of the organization will do far more to provide real value to the organization. Planning requires effort, but poor planning results in wasted resources.

# Comments/Questions

---

[cfennelly@tenablesecurity.com](mailto:cfennelly@tenablesecurity.com)