

---

# Vulnerability Scanning at Notre Dame

Mike Chapple

Senior Director, Enterprise Support Services



---

IT is centralized  
but only to a certain  
extent!

---

# Five years ago, I had a Bad Day



## SECURITY THREATS TOOLKIT

### Hackers strike at Notre Dame

Tags: Break-in, College, Theft, University

Greg Sandoval, CNET News.com

## COMPUTERWORLD Security

## University of Notre Dame investiga

Jaikumar Vijayan

**January 24, 2006** (Computerworld) The University of Notre Dame in Indiack of a university server that may have exposed confidential data belong donors to the school.

The hack took place on Jan. 13 and was discovered the same day by the staff, said Hilary Crnkovich, Notre Dame's vice president of public affairs. any data that may have been exposed in the attack is being misused, she said.



Home > News

## Breach may have exposed donor information

Hacker causes Notre Dame's first significant computer security intrusion



## Notre Dame probes hack of comput

By Greg Sandoval

Staff Writer, CNET News.com

Published: January 23, 2006, 6:40 PM PST

Story Tools

TalkBack

E-mail

Print

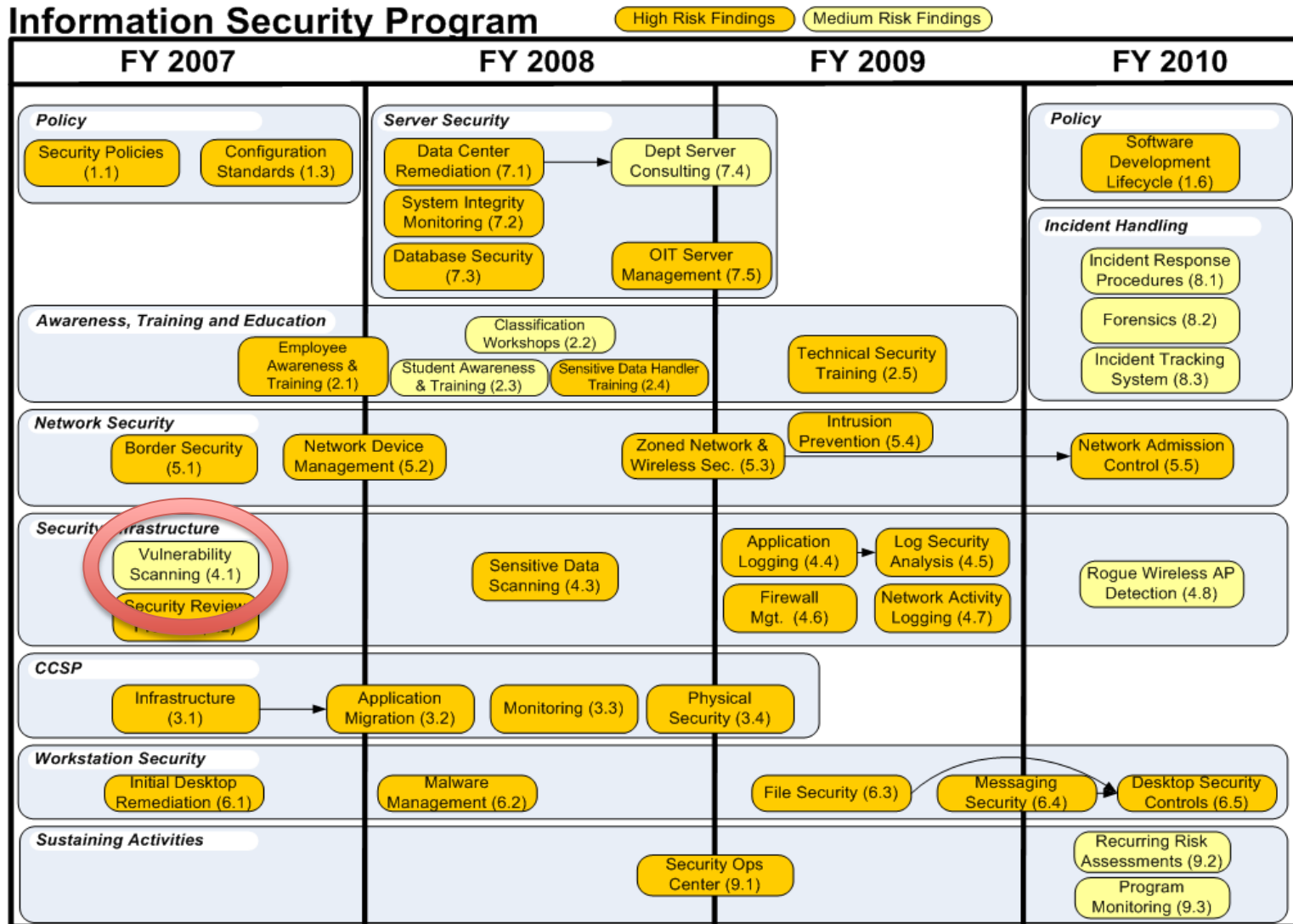
del.icio.us

Digg this

**Two computer-forensic companies are helping the University of Notre Dame investigate an electronic break-in that may have exposed the personal and financial information of school donors.**

The hackers may have made off with Social

# But the Cloud had a Silver Lining



---

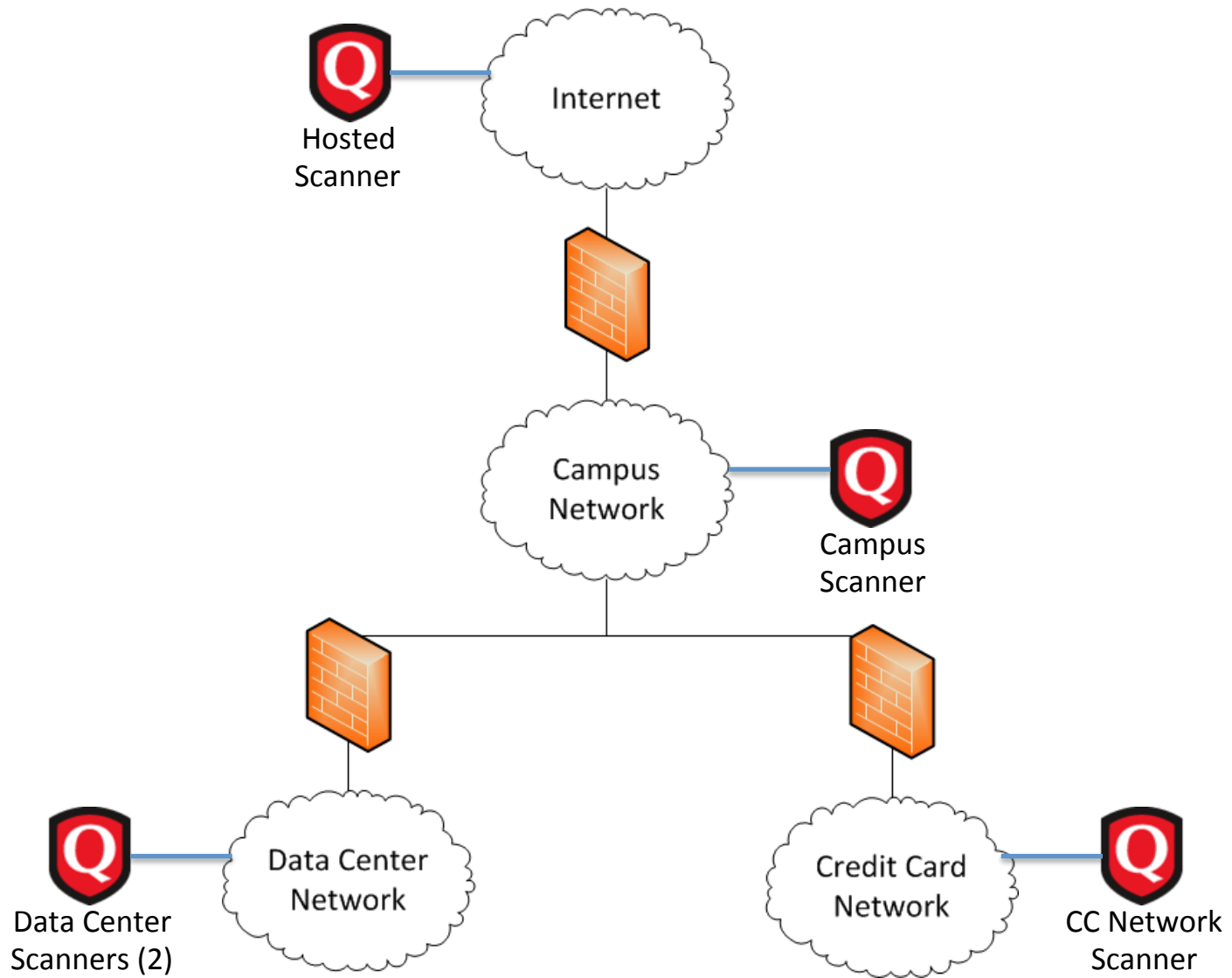
# We Needed Something...

- Easy to deploy
- Scalable
- Accessible to non-security IT staff
- Low administrative overhead

---

# Scanning Services


- Managed scanning of central IT systems
- Public IP space scanning
- PCI DSS compliance management
- Variety of services for distributed IT
  - On-demand scanning
  - Build scanning
  - Recurring scanning





---

# Example of a Vulnerability

 3 SSL Server Supports Weak Encryption Vulnerability (50)

---

# Example of a Vulnerability



## 3 SSL Server Supports Weak Encryption Vulnerability (50)

### THREAT:

The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server.

SSL encryption ciphers are classified based on encryption key length as follows:

HIGH - key length larger than 128 bits

MEDIUM - key length equal to 128 bits

LOW - key length smaller than 128 bits

Messages encrypted with LOW encryption ciphers are easy to decrypt. Commercial SSL servers should only support MEDIUM strength ciphers to guarantee transaction security.

---

# Example of a Vulnerability




3 SSL Server Supports Weak Encryption Vulnerability (50)

## IMPACT:

An attacker can exploit this vulnerability to decrypt secure communications without authorization.

---

# Example of a Vulnerability

 3 **SSL Server Supports Weak Encryption Vulnerability (50)**

## **SOLUTION:**

**Disable support for LOW encryption ciphers.**

### **Apache**

**Typically, for Apache/mod\_ssl, httpd.conf or ssl.conf should have the following lines:**

**SSLProtocol -ALL +SSLv3 +TLSv1**

**SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM**

**For Apache/apache\_ssl include the following line in the configuration file (httpsd.conf):**

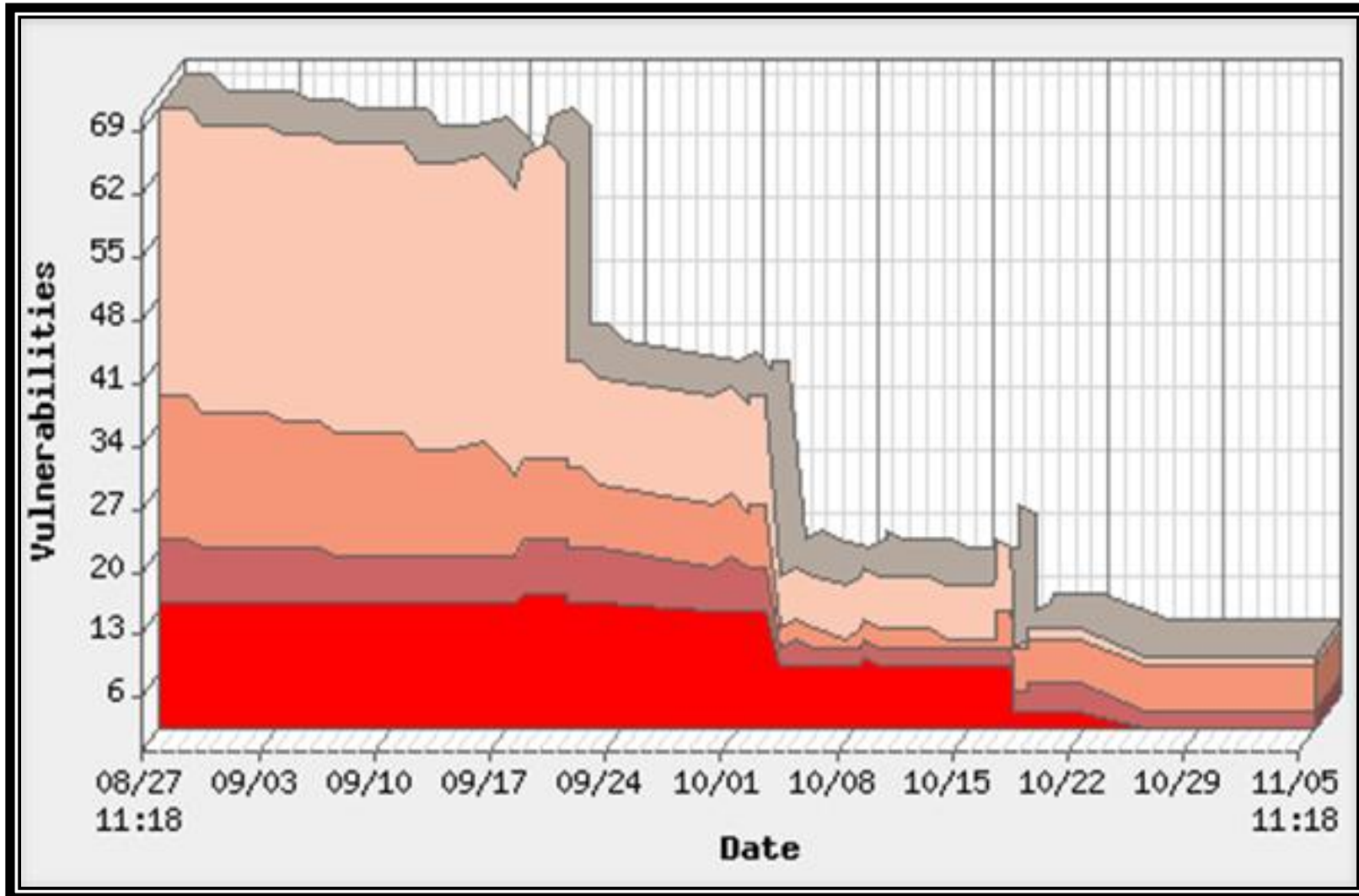
**SSLRequireCipher ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM**

---

# Case Study: PCI DSS Compliance

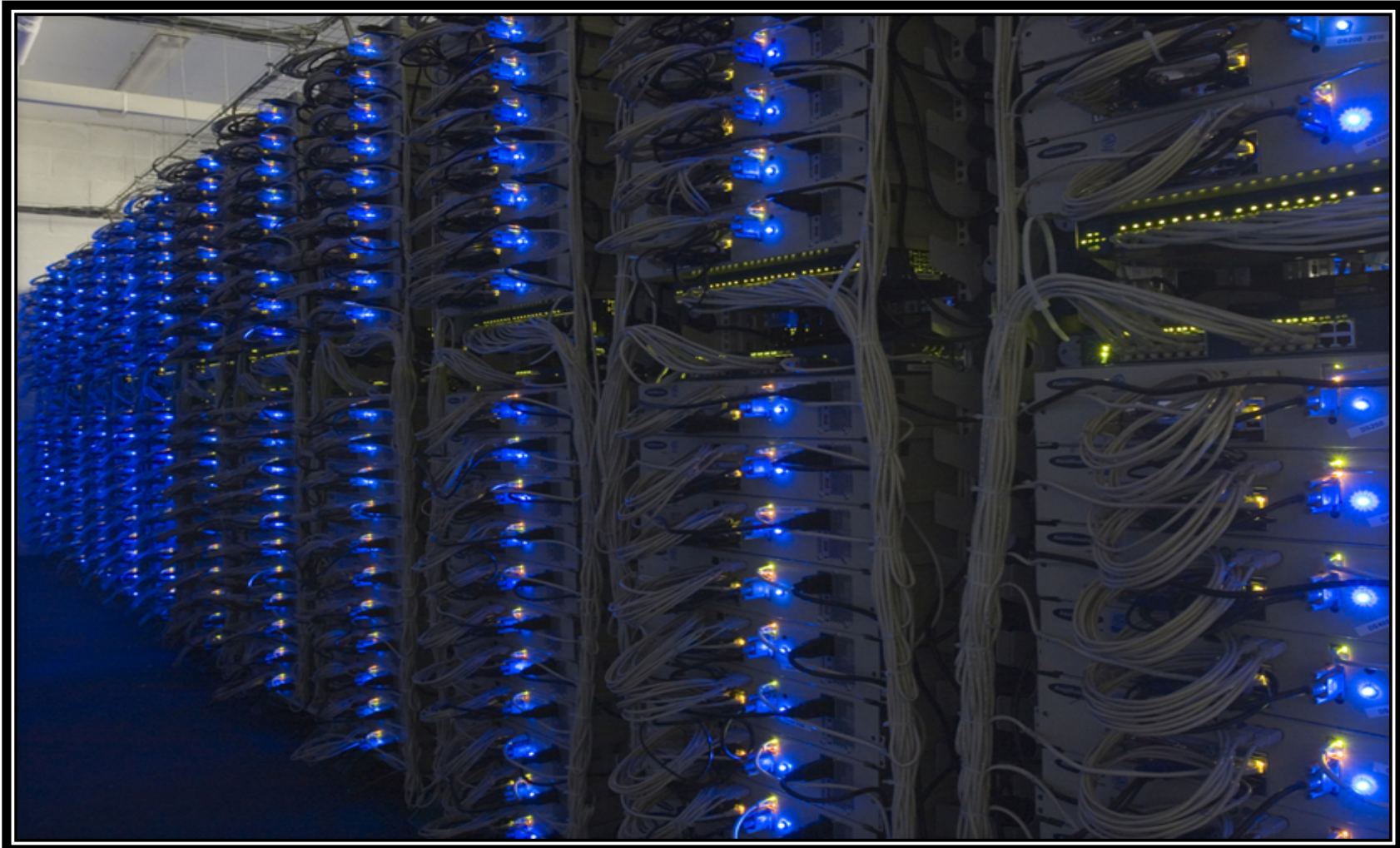


# Two Wonderful Months...



---

# Case Study: Research Computing



---

# Questions?