Security Effectiveness Metrics

Creating a Compelling Business Case

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

State of the Onion

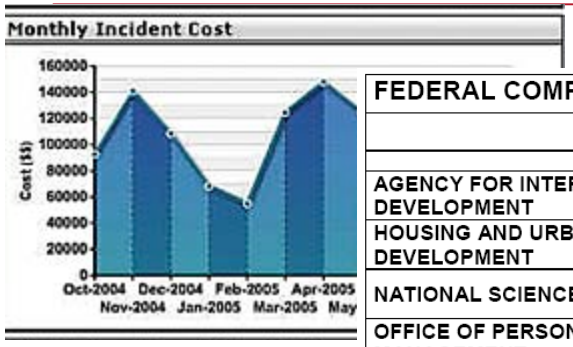
Still the Same

- Last to think of and first to blame
- Desired to be as invisible as IT
- Confusion on REAL risk

Forward Progress

- Evolving the CISO from technology to business
- Visibility (audit committees, board reporting, line item budgeting)
- Proof in REAL risk mitigation

Metrics Today

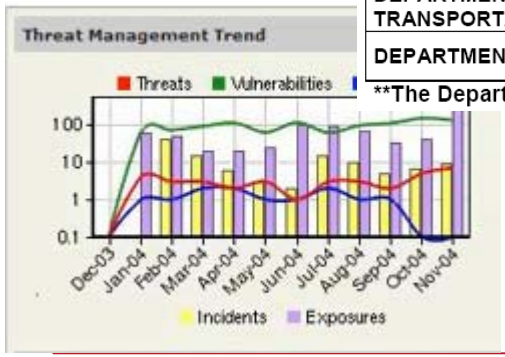


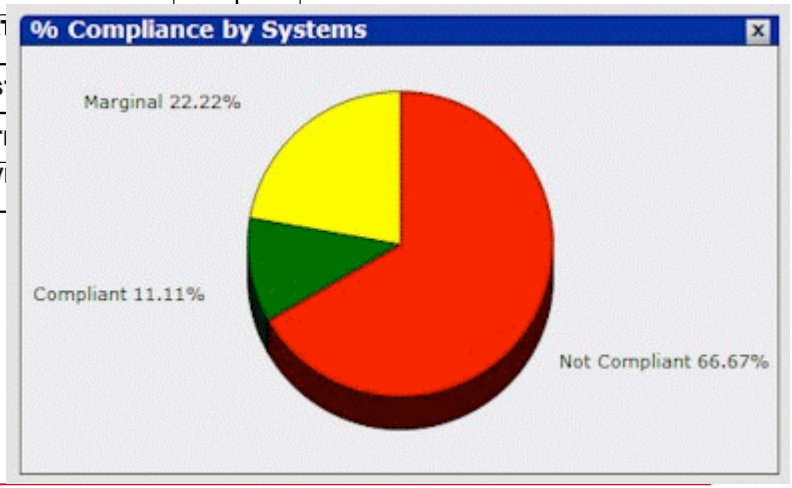
FEDERAL COMPUTER SECURITY REPORT CARD

GOVERNMENTWIDE GRADE 2006: C-

	2006	2005			
AGENCY FOR INTERNATIONAL DEVELOPMENT	A+	A+	DEPARTMENT OF ENERG		
HOUSING AND URBAN DEVELOPMENT	A+	D+	DEPARTMENT OF HOMEL SECURITY		
NATIONAL SCIENCE FOUNDATION	A+	A	NATIONAL AERONAUTICS SPACE ADMINISTRATION		
OFFICE OF PERSONNEL MANAGEMENT	A+	A+	DEPARTMENT OF AGRICU		
GENERAL SERVICES ADMINISTRATION	A	A-	DEPARTMENT OF COMMERCE	F	D+
SOCIAL SECURITY ADMINISTRATION	A	A+	DEPARTMENT OF DEFENSE	F	F
DEPARTMENT OF JUSTICE	A-	D	DEPARTMENT OF EDUCATION	F	C-
ENVIRONMENTAL PROTECTION AGENCY	A-	A+	DEPARTMENT OF THE INTERIOR	F	F
SMALL BUSINESS ADMINISTRATION	B+	C+	NUCLEAR REGULAT COMMISSION		
DEPARTMENT OF HEALTH AND HUMAN SERVICES	B	F	DEPARTMENT OF S		
DEPARTMENT OF TRANSPORTATION	B	C-	DEPARTMENT OF TI		
DEPARTMENT OF LABOR	B-	A+	DEPARTMENT OF VI AFFAIRS**		

**The Department did not provide its FY06 FISMA Report

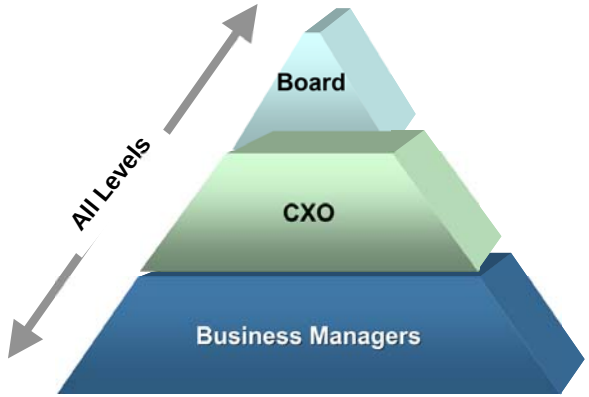




Step 1

Establish Management Commitment/Expectations

- Must be a Visible Priority from the Top
- Consistent and Committed Communication
- Earned Credibility



Engagement At All Levels

Easier Said Than Done

- Know thy buyer!
  - Pain Buyer: Feasts on FUD
  - Gain Buyer: Feasts on Risk
  - Cost/Efficiency Buyer: Feasts on Appearing Smart

The Pain Buyer

WIRED BLOG NETWORK

Federal Court Slaps Data Theft Victims

By David Kravets | August 23, 2007 | 3:50:55 PM | Categories: Identification

Tens of thousands of Old National Bancorp customers whose personal and financial information was hijacked by a computer hacker cannot recover damages from the Indiana banking institution who lost the data in 2005, a federal appeals court ruled Thursday.

In dismissing a proposed class action against Old National Bancorp, the 7th U.S. Circuit Court of Appeals said damages were unavailable to victims of data theft if those victims did not suffer economically.

The three-judge panel of the circuit, mirroring decisions of federal courts in Ohio, Minnesota, Arizona and Michigan, ruled (.pdf): "Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared

COMPUTERWORLD Security

Bank of India site hacked, serves up 22 exploits

Reminiscent of Super Bowl site hack in January; notorious Russian gang suspected

Gregg Keizer Today's Top Stories ▸ or Other Security Stories ▸

Comments (0) Recommend this article

August 31, 2007 (Computerworld) -- The Bank of India Web site was hacked sometime Wednesday night (U.S. time) and seeded with a wide, wild array of malware that infected any users running unpatched browsers, security researchers said today.

Although the **bank's site** had been scoured of all malware by Friday morning, it's currently offline. "This site is under temporary maintenance and will be available after 09:00 IST on 1.09.07," a prominent message currently reads.

Researchers at Sunbelt Software Inc. first posted **details of the hack** yesterday afternoon after finding rogue code embedded in the site's HTML. That code, actually an IFRAME exploit, silently redirected users to a hacker server, which pushed 22 different pieces of malware onto vulnerable PCs. By Sunbelt's tally, the malware included one worm, three rootkits, five Trojan downloaders, and several password stealers.
"The biggest issue is the sheer volume of malware we've had to analyze," said Alex Eckelberry, Sunbelt's

washingtonpost.com Hello news3 Change Preferences | Sign Out

The Washington Post Print Edition | Subscribe

washingtonpost.com > Technology > Special Reports > Cyber-Security

TechNews.com

Print This Article
E-Mail This Article

QUICK QUOTES
Enter Symbol go
Tables | Portfolio | Index

MOST VIEWED ARTICLES
Technology On the Site
Updated 1:46 p.m. ET
• On the Internet, A Tangled Web Of Classified Ads

Latest News: Bush Seeks Legal Immunity for Telecoms

Computer Stolen From VA Subcontractor

Missing PC May Contain Names, Social Security Numbers, Medical Data

By Mary Mosquera and Patience Wait
Special to washingtonpost.com
Monday, August 7, 2006; 4:54 PM

The Veterans Affairs Department today confirmed that a subcontractor, Unisys Corp., had informed the department that a desktop computer containing sensitive personal information of veterans is missing from the company's offices. It is the second

ZDNet Where Technology Means Business

PCI compliance: Don't become another headline

By Nir Gertner, News.com
Published on ZDNet News: Aug 8, 2005 6:47:00 PM

Nir Gertner,
CTO, Cyber-Ark

***Commentary*--Bank of America, Morgan Stanley, Citibank. What do they all have in common? Within the past six months, each one of these companies has had a breach of security which resulted in thousands of customers' personal data being stolen or compromised. Many within the industry are at a loss—every day, hackers, thieves and even a company's own employees are finding new ways to access consumers' personal data. Enter the Payment Card Industry (PCI) Data Security Standard.**

In response to the overwhelming occurrences of data theft, the Standard, developed by MasterCard and VISA and also being enforced by American Express, is designed to protect cardholder information and must be implemented by members, merchants and service providers. The PCI Data Security Standard is broken into six specific parts and its implementation implies the development and adoption of security policies, the use of various security technologies and products, as well as adaptation of existing systems to use these technologies. Today, all merchants using payment cards, including electronic commerce merchants, and service providers must comply with the PCI Data Security Standard or they will face fines of up to $500,000 per incident of non-compliance.

Step 2

Use Business Terms … Not Security Ones

Payback period

Risk to Uptime

Damage to Brand

Material Weakness

Gross Margin

Annualized Loss Expectancy

Shareholder value

Fines for Non-Compliance

Return on Capital Employed

Apply their terms based on buyer type

Step 3

Develop a Marketing Plan

Case Study: Citigroup Building Permit Process

- New York City Centric
- Safety Centric
- Highly Visible with Company-wide Messaging
- Provable, Simple results (Permit vs. Permit-less Development)

The Right Brand Will Shift a Culture

Step 4

Develop Management Strategy

- Know Where You Are Today
- Existing Process On Track?
- Establish Practical, Measurable, and Attainable Metrics/Goals
- Build a Business Case for Success

Under Promise, Over Deliver

Step 5

Communicate in Rates

- Attacks prevented per day
- Productivity loss per week
- Incidents per month
- Traffic Volume per hour

Dollars Per Hr Drives a Sense of Urgency

Step 6

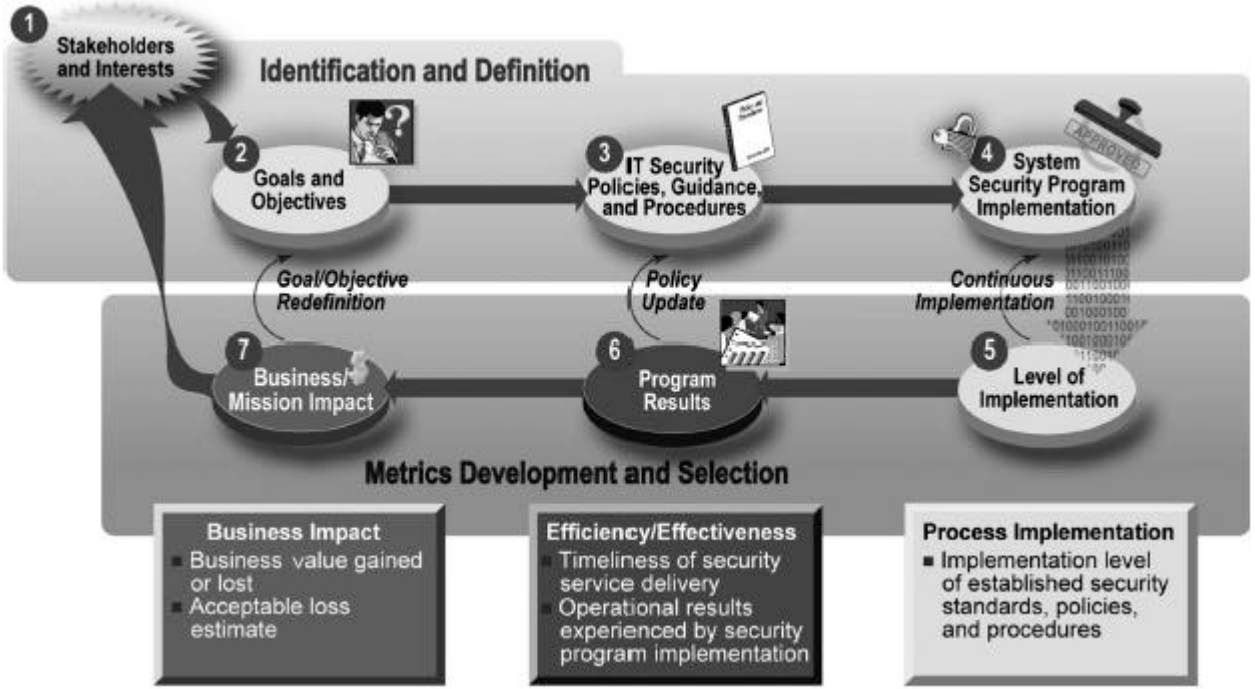
Track your time

- Track and Analyze Time Spent on Key Initiatives
- Develop and Validate Your Fully Loaded Cost Per Hr Assumption
- Rank Order Time Intensive Initiatives
- Model Real Automation Efficiencies

Soft Costs are Neglected Most Often

Step 7

Categorize your Metrics



NIST 800-55 IT Security Metrics Development Process

Provides a Framework for Your Audience

Step 8

Use Your Supplier Network for Metrics

- Easiest Way to Stretch Your $$$
- Fresh Set of Eyes
- What are Others Like Me Doing?

It's Free Work …Take It!

Step 9

Evaluate Metrics Periodically

- Replace Metrics that Show Little Variance
- Track which ones are reused the most by your management
- Replace Sandbag Metrics
- Focus on Accuracy, not Precision

Improving Your Metrics Earns Credibility

Step 10

Keep it Simple!!!

- How am I doing?
- Compared to who?
- Compared to when?
- Focus on Largest Discrepancies
- Throw Away the Spider Charts!

If Your 5 Year Old Gets It, Then Stop There

Summary

1. Management Commitment
2. Use Business Terms
3. Develop a Marketing Plan
4. Develop a Management Strategy
5. Communicate in Rates
6. Track Your Time
7. Categorize Metrics
8. Use Your Supplier Network
9. Evaluate Metrics Periodically
10. Keep it Simple

Resources

- http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf
- http://www.sans.org/reading_room/whitepapers/auditing/55.php
- **Security Metrics: Replacing Fear, Uncertainty, and Doubt** - Andrew Jacquith
- http://www.csoonline.com/read/070105/metrics.html

Questions?

Yong-Gon Chon

Senior Vice President, Services

703-245-9753

ychon@secureinfo.com

SecureInfo™

THE INFORMATION ASSURANCE EXPERTS™