SOLUTIONARY
MAKING SECURITY MANAGEABLE

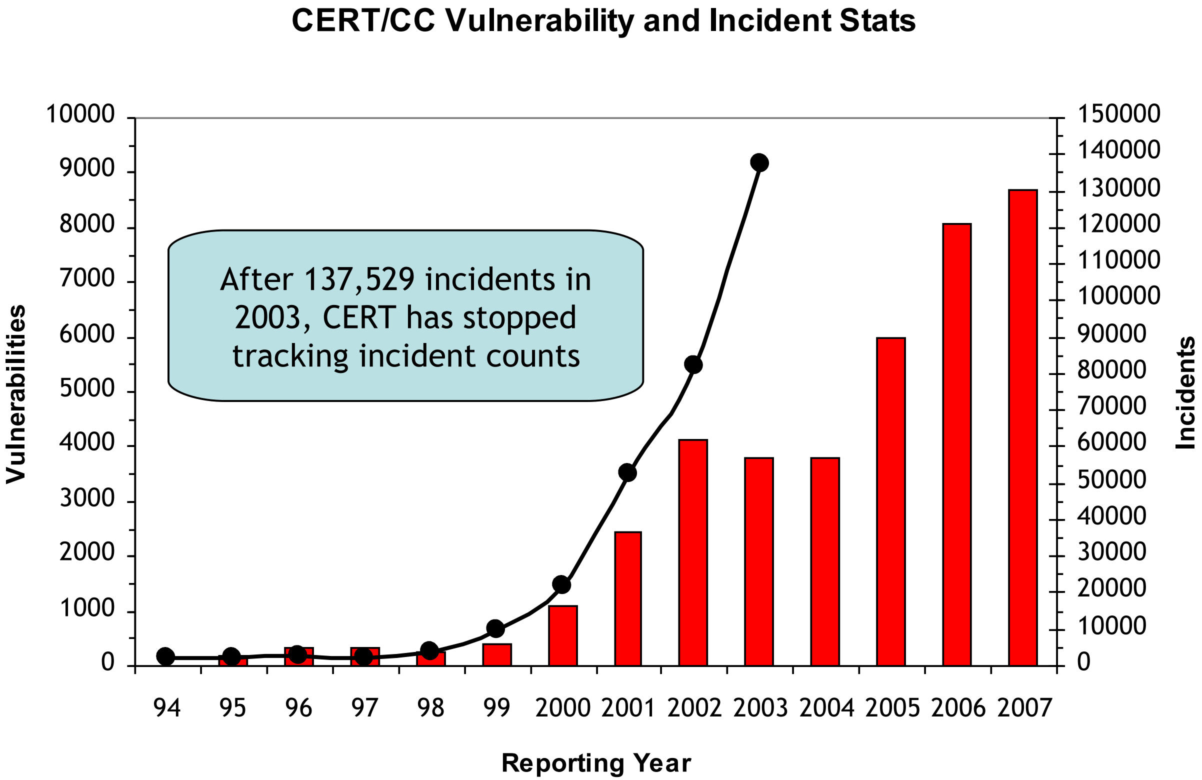
Security Requirements:

Competitive Advantage or Barrier

The need for security

Software Companies Release Code More Frequently

Faster Releases = More Bugs = More Exploits



After 137,529 incidents in 2003, CERT has stopped tracking incident counts

The initial release of Windows 2000 contained approximately 63,000 known defects. Windows XP has 45,000,000 lines of code

Current legislation

- PCI
- HIPAA
- FTC Act
- EU Data Privacy Directive
- Sarbanes-Oxley
- Bank Secrecy Act
- California Data Privacy Law
- Feinstein Data Privacy Reporting Proposal
- OFAC –OCC Rules
- USA Patriot I and II(?)
- SEC Regulations 10(b)(5)
- AB 1950 - Mandates reasonable level of security to databases

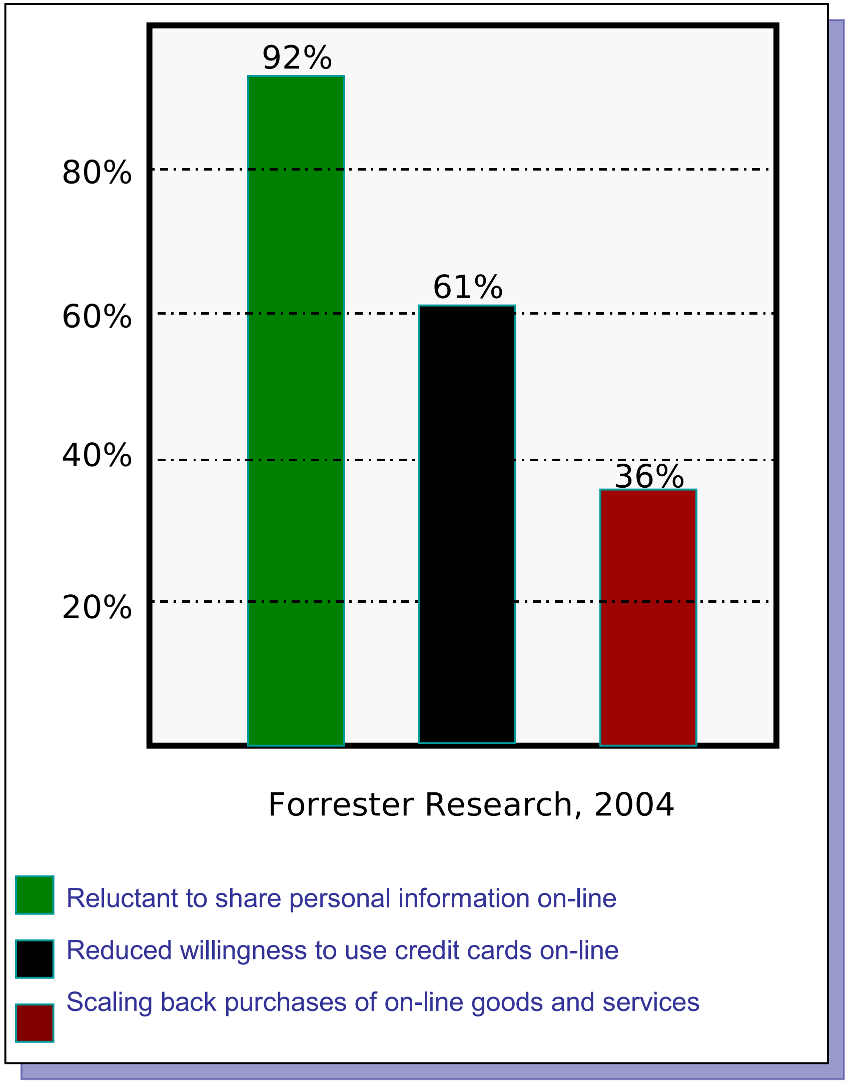
Security is beginning to affect consumer behavior

Identity Theft is Exploding

- One of the fastest growing categories of crime (FBI)
- 9.4 million incidents of identity theft last year (Gartner)
- Majority of identity fraud incidents rooted in stolen credit card data (Gartner)
- $33 billion total loss to businesses from credit card fraud in 2003 (FTC)
- 60 million credit cards compromised in 2004 (Merchant Risk Council)
- 120 million expected to be compromised in 2005 (Merchant Risk Council)

Change in Hacker Motivation

- More than just e-vandalism – motive is increasingly financial gain
- Hackers can sell credit card numbers on Eastern European / Russian sites
- 700 carding and e-commerce websites brokering illegally obtained card numbers closed by MasterCard (Between June 2004 and May 2005)[4]



Forrester Research, 2004

How does organized crime get this data?

- ~1 New Compromise Reported per Day in the United States
  - Merchants (Retailers + Higher Education, Healthcare, Utilities, Insurers…)
  - Independent Sales Organizations (ISOs)
  - Payment Processors
  - Acquirers
  - Issuers
  - Not Card Associations, yet
- Typical Attacks
  - Man-in-the-Middle
  - Data Store Compromise
- Discovered Through
  - Fraud Analysis, not Internal Security Controls

Visa’s published stats

- 2007 Visa Initiative to focus on Level 4 Merchants
- 6,000,000 Merchants representing 32% of transaction volume
- 80% of the compromises since 2005 are Level 4 Merchants
- Focus is to be on
  - Risk Profiling
  - Merchant Education
  - Compliance Strategy
  - Compliance Reporting

Visa's published stats

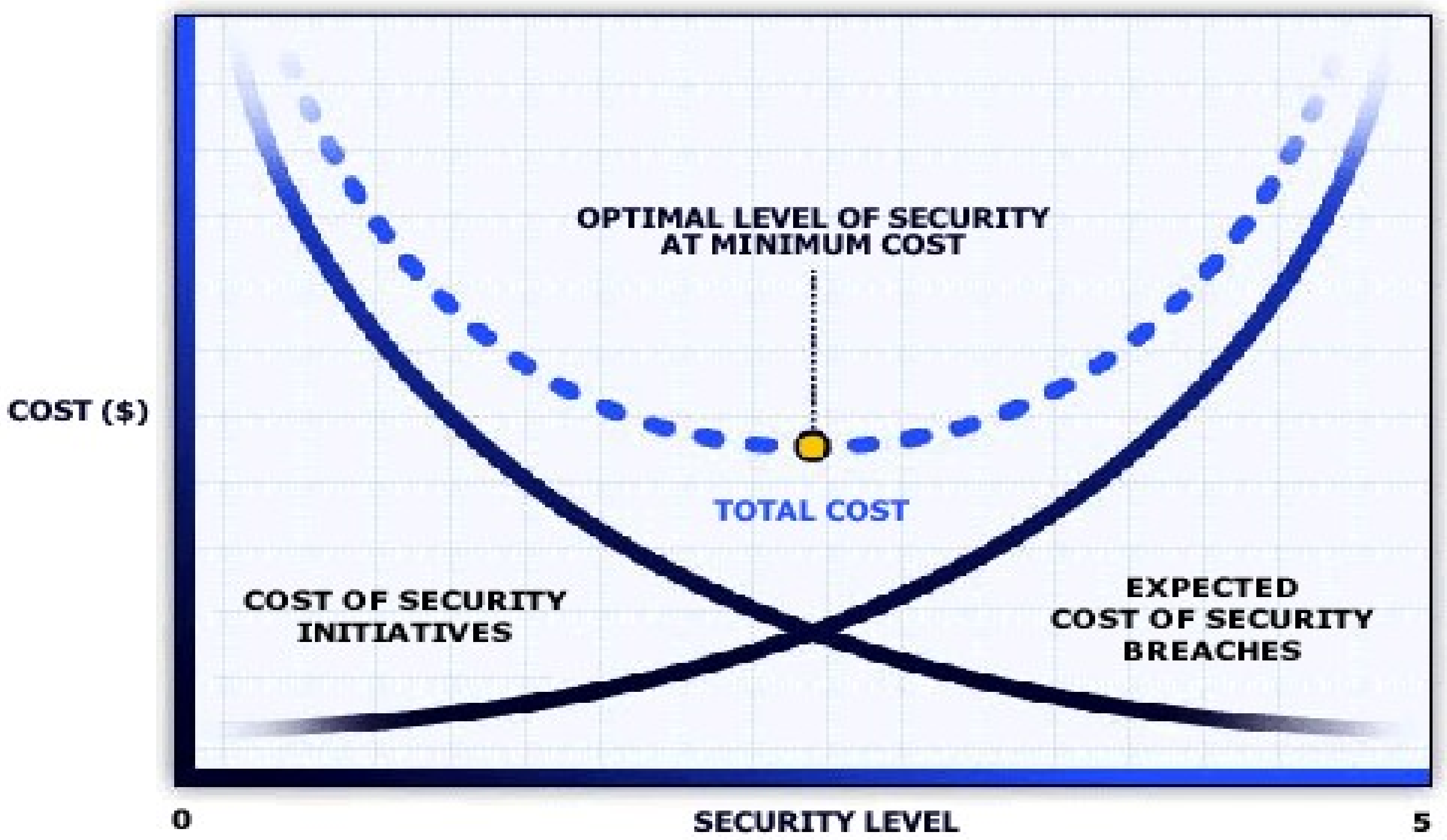
Visa USA Pledges $20 Million in Incentives to Protect Cardholder Data

First Payment Brand to Combine Financial Incentives and Fines to Encourage Adoption of Industry Security Standards

San Francisco, December 12, 2006

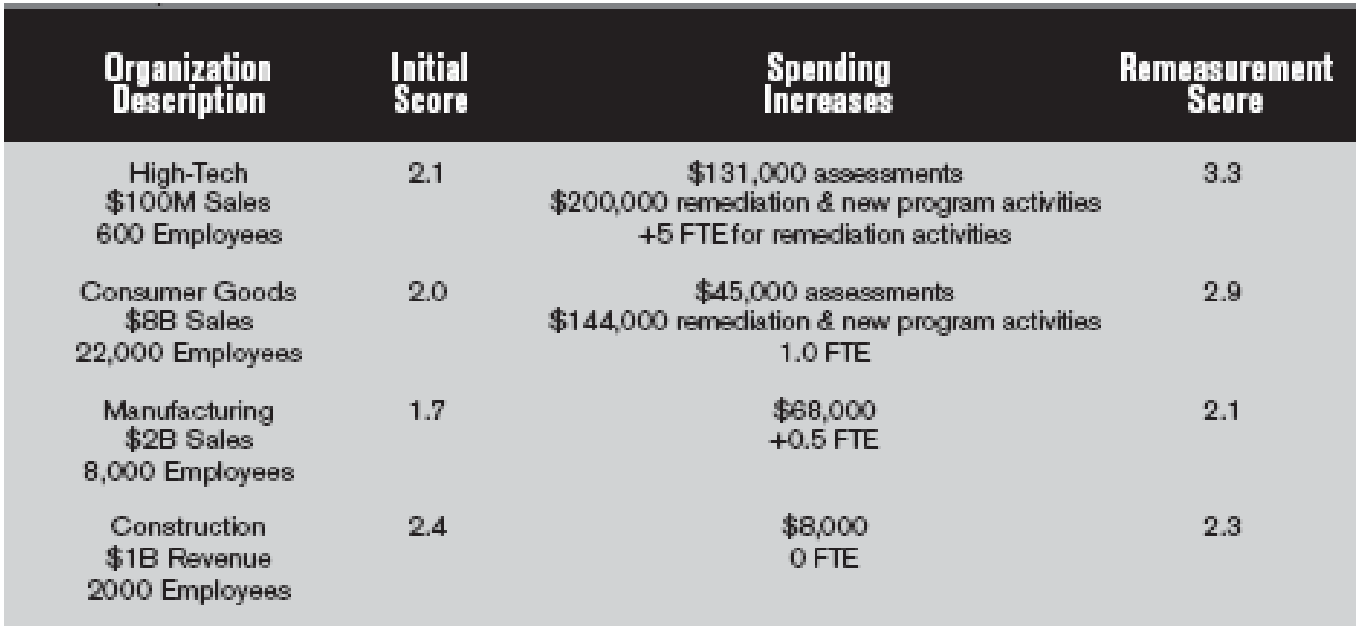
Visa USA today announced it will offer $20 million in financial incentives and create new sanctions in an effort to further merchant compliance with the Payment Card Industry Data Security Standard (PCI DSS). The new effort, called the Visa PCI Compliance Acceleration Program (PCI CAP), is the first of its kind to provide positive reinforcement to the industry's traditional, fine-only approach. Visa PCI CAP represents one component of Visa's comprehensive strategy to address payment card fraud.b

Economics of security



The need for security measurement

- An alternative explanation:
  - Security measurement is not part of the existing performance metrics or management system of the organization
  - Security is managed as a “best practices” issue
  - Measurable goals and plans are not tracked and managed



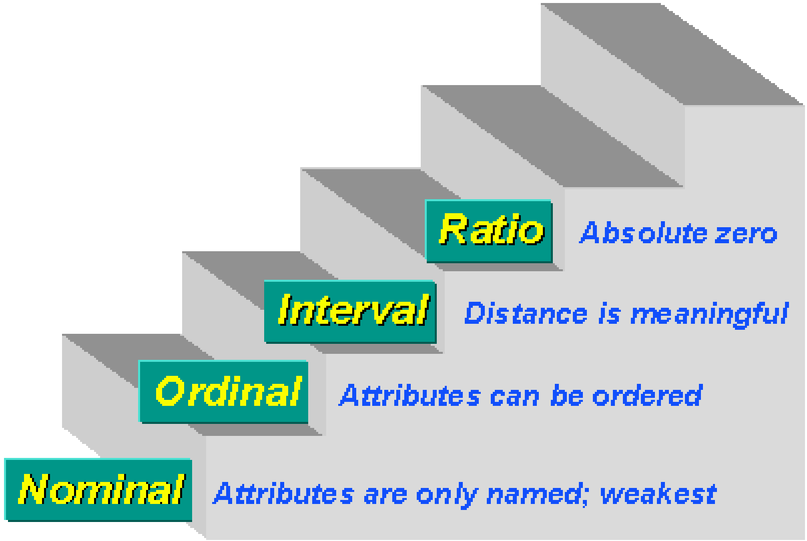
Organization Description	Initial Score	Spending Increases	Remeasurement Score
High-Tech $100M Sales 600 Employees	2.1	$131,000 assessments $200,000 remediation & new program activities +5 FTE for remediation activities	3.3
Consumer Goods $8B Sales 22,000 Employees	2.0	$45,000 assessments $144,000 remediation & new program activities 1.0 FTE	2.9
Manufacturing $2B Sales 8,000 Employees	1.7	$68,000 +0.5 FTE	2.1
Construction $1B Revenue 2000 Employees	2.4	$8,000 0 FTE	2.3

Measurement system evolution

Stage of Evolution	Description	Example
Stage I	Little or no economic value or need for consistent standards or measurement exists.	Length measurement is inconsistent, but often based on a body part (such as arm, forearm, or hand).
Stage II	Independent standards and measurement approaches arise based on the requirements of specific economic agents in the market.	A yard is the length of your arm.
Stage III	A given standard and measurement system spreads widely among a population of economic agents enabling efficiencies.	A yard is the length of the right arm of the English King Edward the 1st. This length was measured and recorded on a brass bar with a gold button on each end.
Stage IV	Consolidation reaches critical mass and a comprehensive standard attains stability and broad adoption under the pressure of alternative competing standards. Measurement and compliance against the accepted standard is enforced.	A yard is .914 meters. A meter is the distance that a beam of light travels in a vacuum in 1/299792458 of a second. Countries around the world validate the standard, accept this measure as accurate, and have adopted it as part of the International System of Measurement.

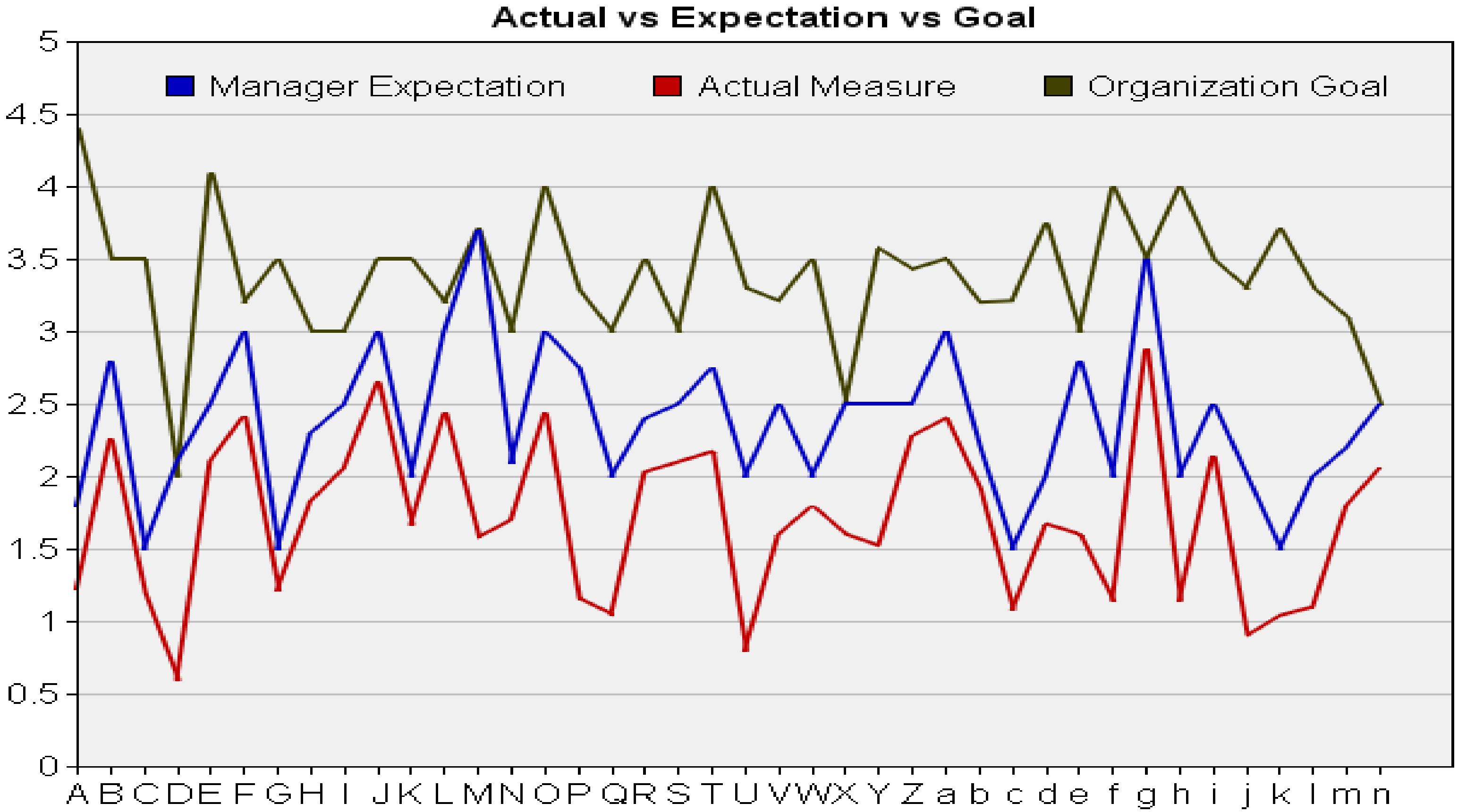
Levels of measurement

- Nominal – numerical values just name attribute uniquely
  - Basketball Jersey numbers
  - A player with number 30 is not better or worse than 15
- Ordinal – attributes can be rank ordered.
  - Distances between attributes have no meaning
  - Educational Attainment: 0=less than H.S.; 1=some H.S.; 2=H.S. degree; 3=some college; 4=college degree; 5=post college
- Interval – the distance between attributes has meaning
  - Fahrenheit, the distance between 30-40 is same as 70-80
  - Averages start to have meaning
  - Ratios don’t make sense
    - 80 degrees is not twice as hot as 40 degrees
    - (although the attribute value is twice as large)
- Ratio – An absolute zero that is meaningful

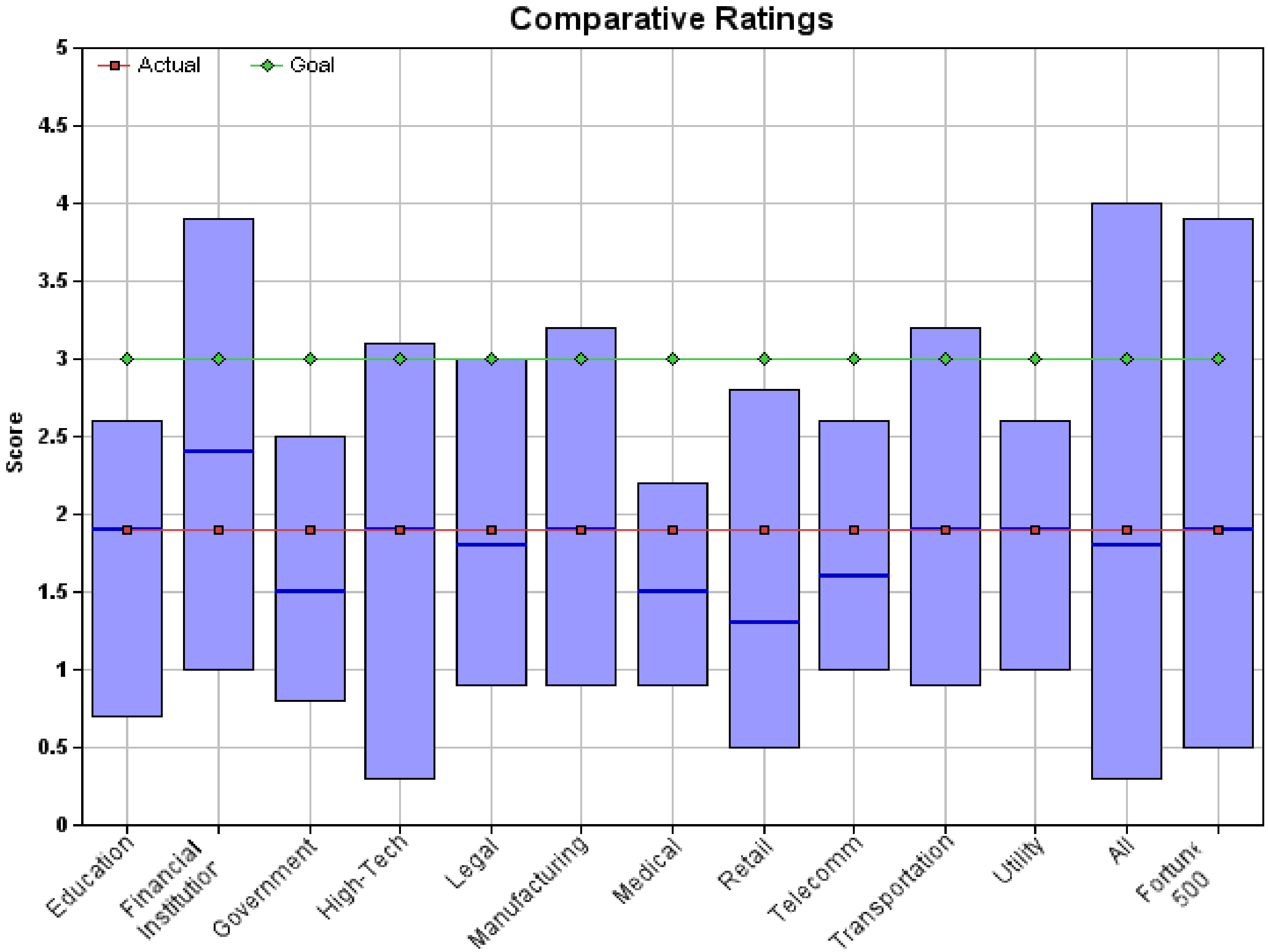


Compared to management expectations

- From 40 measurements, the average goal was 3.4
- The average expectation was 2.4
- The average actual measurement was 1.7
- In every case, the actual security measurement was lower than what management expected
- Managers tend to understand they need to improve



Rating results

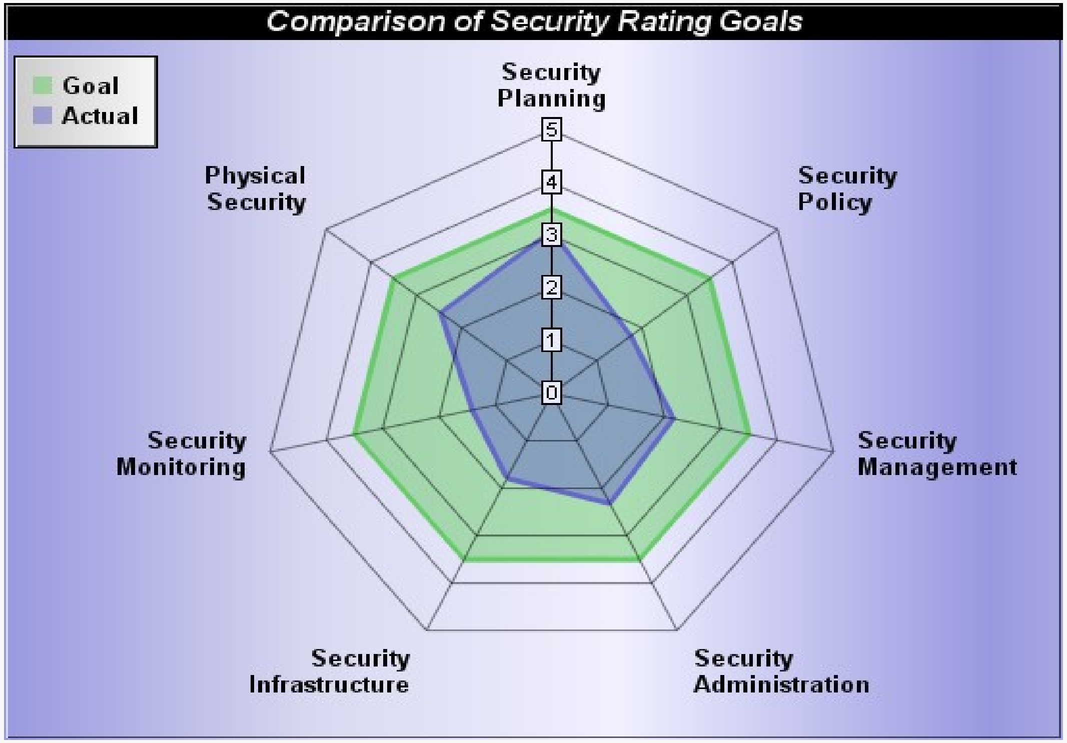


Security measurement will:

Benefit:

Allow the comparison of the current state to security program goals

Issues:


Comparison of Security Rating Goals
🟩 Goal
🟦 Actual
Security Planning
Security Policy
Security Management
Security Administration
Security Infrastructure
Security Monitoring
Physical Security