Information Security Metrics
@
Citigroup

Thomas M. Dunbar

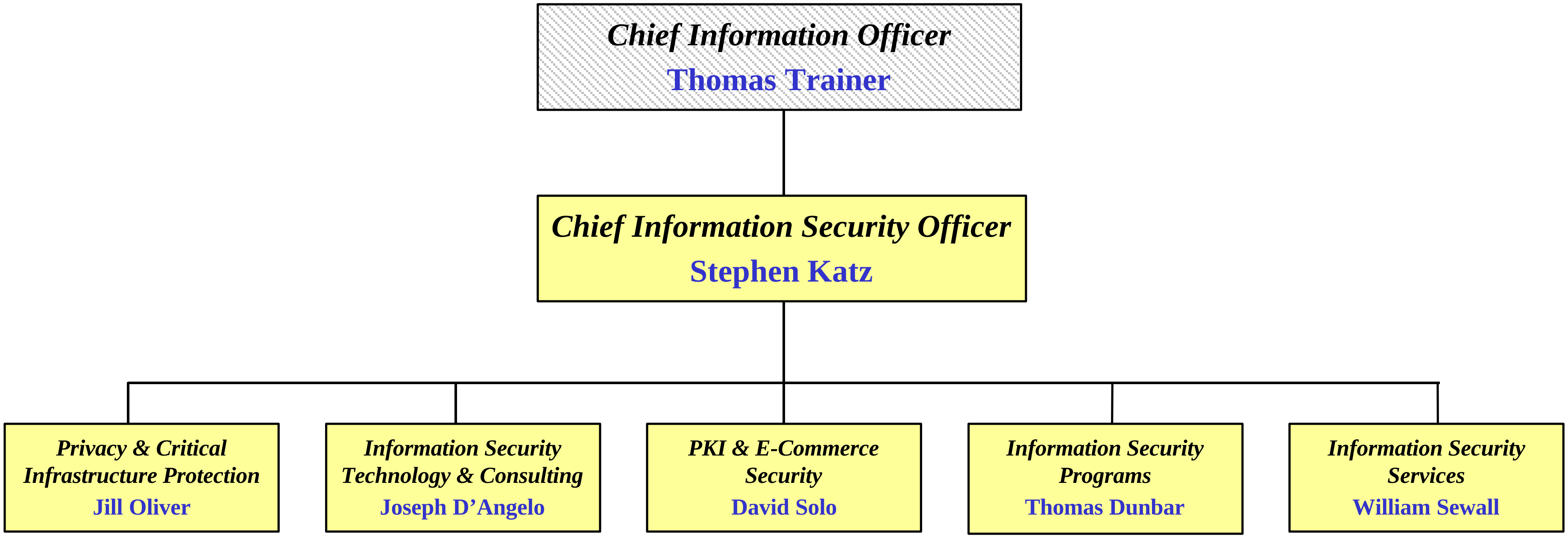
Director, Information Security Programs

June 14, 2000

Agenda

- CISO (Corporate Information Security Office)
- CISO Programs
- Information Security Metrics
- Citi-ISEM

Corporate Information Security Office



Chief Information Officer
Thomas Trainer

Chief Information Security Officer
Stephen Katz

Privacy & Critical Infrastructure Protection
Jill Oliver

Information Security Technology & Consulting
Joseph D'Angelo

- *Ethical Hacking*
- *Investigations*
- *Security Architecture*
- *Security Assessments*
- *Threat Assessments*

PKI & E-Commerce Security
David Solo

Information Security Programs
Thomas Dunbar

- *ISO Coordination*
- *Awareness*
- *Training & Education*
- *ISEM*
- *Metrics*

Information Security Services
William Sewall

- *Alerts*
- *Products Approval*
- *ISLC Coordination*

CISO Programs

Prevention

- Form/Lead E-Commerce Cross-Functional Teams
- Ethical Hacking
- Organization and Management
- Policies, Standards, & Practices
- Awareness & Education
- Tools, Technologies, & Technology Evaluations
- Government/Regulatory Support

Detection

- Intrusion Detection Systems
- Security Violation Reports
- Incident Response

Verification

- Metrics
- Compliance Checking/Self Assessment Tools
- Ethical Hacking -- Infrastructure
- Citi-ISEM

Information Security Metrics

IS Metrics

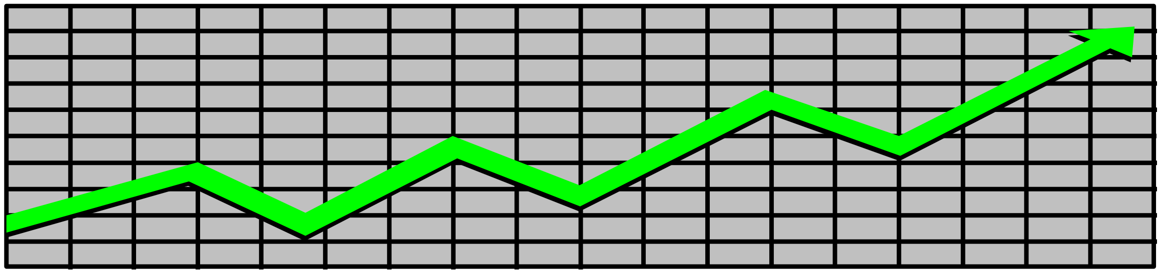
Objectives

- Meaningful to target audience (EVPs, Sr. Mgmt)
- Easy to collect and interpret
- Performance measurement to continuously improve security
- Yardstick to prioritize corrective action plans
- Assessment of GISO effectiveness

IS Metrics

Sample metrics

- Security related audit issues or comments
- Self assessments
- Alert responses
- Building permit process
- Desktop security (Protect!, Virus, NT, etc.)
- Risk Acceptance/Deviations
- Staff awareness and training



Information Security Status Report
March 2000 - NACB

GENERAL HEALTH

GISO Name: John Smith

Received assignment: June 1998

The GISO has been certified by CISO.

80 % of your business units have Business Unit Information Security Officers (BISOs) assigned.

90 % of your business units have completed an Information Security Gap Analysis this quarter.

75 % of your business unit Gap Analysis are in process.

In total 10 % have completed the analysis to date.

RISK / ISSUES

As a result of the vulnerability assessments completed this quarter, 6 high risk issues were identified.

95 % of your Information Assets have Information Owners identified.

83 % of your Information Assets have been classified.

74 % of your desktop computers have been identified as high risk.

100 % of these high risk desktop computers are protected.

99 % of your laptops are protected.

A total of 4 security issues were reported by audit this quarter.

A total of 2 security issues identified by audit remain open to date.

Citigroup
Information Security Evaluation Model

citi -ISEM

citi ISEM

citi *ISEM is a five-level production model based on Information Security sound practices and the concepts of* ***Prevention**, **Detection**, and **Verification**.*

citi *ISEM*:

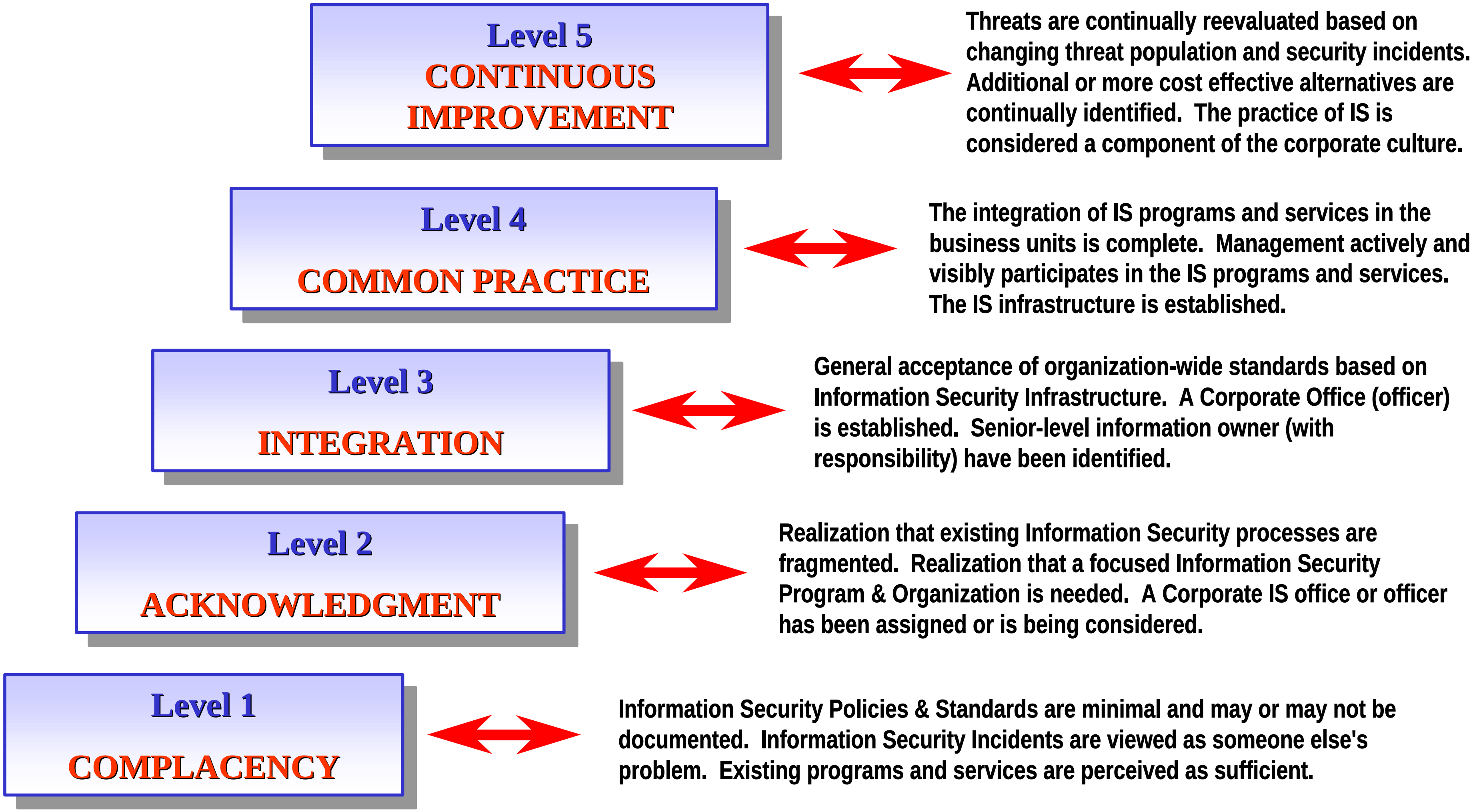
- Sets Information Security goals and monitors status.
- Defines a set of controls for assessing and compensating for vulnerabilities.
- Provides a means for classifying risk.
- Assists in determining the nature of threats.
- Provides tools for impact assessment and analysis and recommends solutions.

The Five Levels Of The Information Security Evaluation Model

Level 1	**=**	***COMPLACENCY***
Level 2	**=**	***ACKNOWLEDGEMENT***
Level 3	**=**	***INTEGRATION***
Level 4	**=**	***COMMON PRACTICE***
Level 5	**=**	***CONTINUOUS IMPROVEMENT***

citi ISEM

Sample Characteristics



Level 5
CONTINUOUS IMPROVEMENT

Threats are continually reevaluated based on changing threat population and security incidents. Additional or more cost effective alternatives are continually identified. The practice of IS is considered a component of the corporate culture.

Level 4
COMMON PRACTICE

The integration of IS programs and services in the business units is complete. Management actively and visibly participates in the IS programs and services. The IS infrastructure is established.

Level 3
INTEGRATION

General acceptance of organization-wide standards based on Information Security Infrastructure. A Corporate Office (officer) is established. Senior-level information owner (with responsibility) have been identified.

Level 2
ACKNOWLEDGMENT

Realization that existing Information Security processes are fragmented. Realization that a focused Information Security Program & Organization is needed. A Corporate IS office or officer has been assigned or is being considered.

Level 1
COMPLACENCY

Information Security Policies & Standards are minimal and may or may not be documented. Information Security Incidents are viewed as someone else's problem. Existing programs and services are perceived as sufficient.