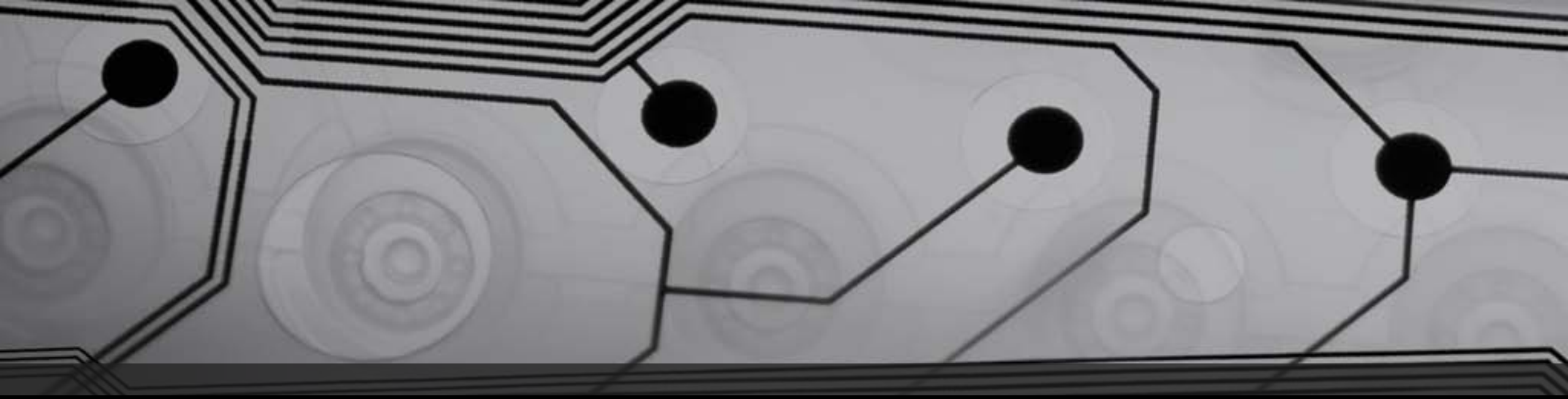


Security is so yesterday

The move to Information Assurance

About Aaron Wampach

- Aaron Wampach has been active in the field of technology for 18+ years. In the last 12 years, he has focused primarily on the area of Information Assurance. He holds several industry certifications: CISSP, GSEC, GCIH, CRISC, and CISM certifications; and is currently a Ph.D. (ABD) candidate. In his spare time he is an active member of the local Information Assurance community: volunteering his time in the local ISSA chapter board of directors; is a senior member of ISSA International; a SANS mentor; and teaches various CS and IT classes.
- His previous experience includes working or consulting for numerous Fortune 500 organizations to small start-up organizations. He has experience in several business verticals ranging from government and transportation to medical device manufacturing and healthcare. He is currently an Information Security Architect for a local healthcare organization and is also an adjunct associate professor at a local university.

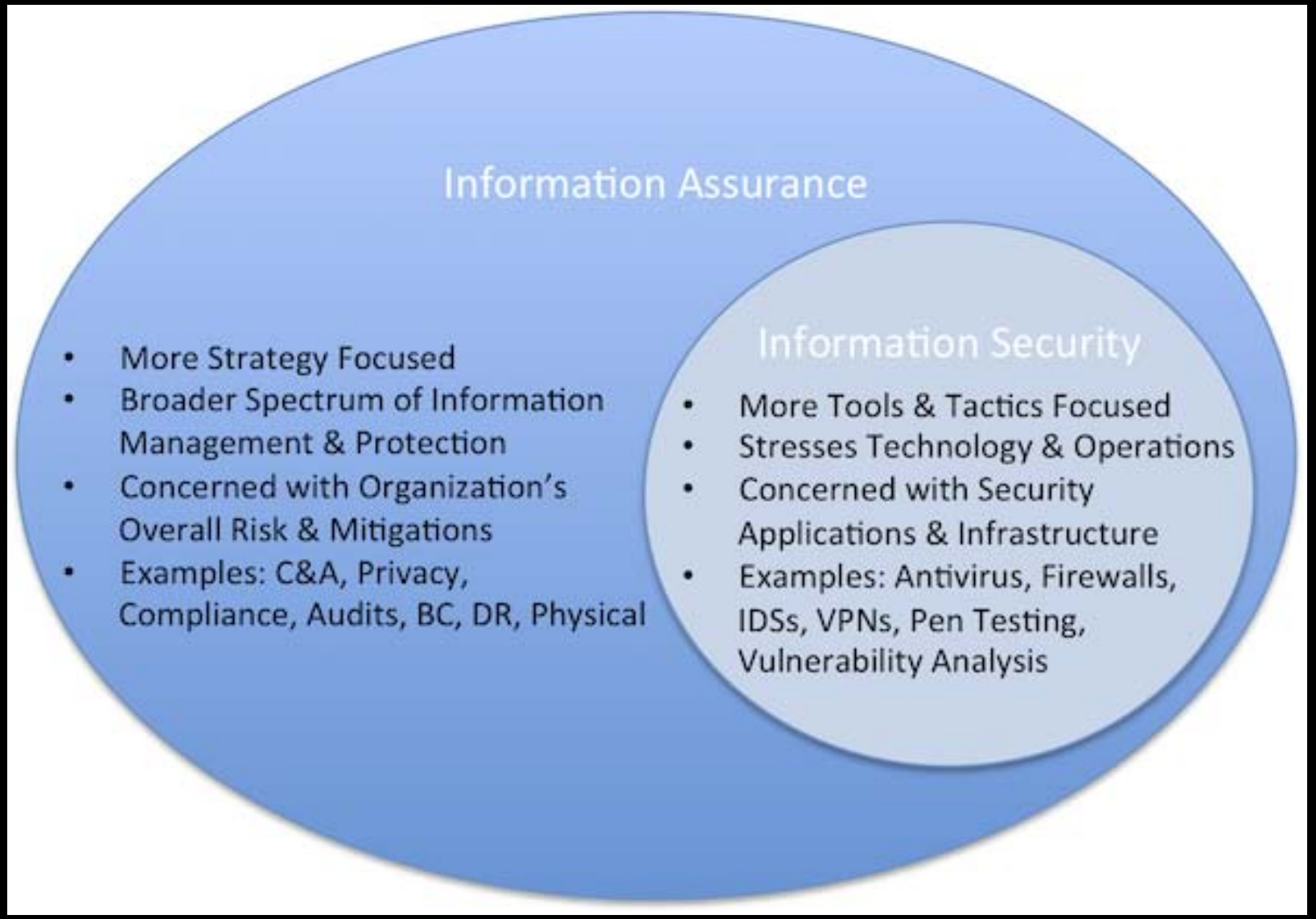
Agenda

- Introduction
- History
- Definition
- The progression to Information Assurance

Introduction

- Computer Science
- Software Engineering
- Information Technology
- Information Assurance
  - NSTISSI-4011
  - CNSSI-4012
  - CNSSI-4013
  - CNSSI-4014
  - NSTISSI-4015
  - CNSS-4016

Introduction – IA vs. IS



https://www.novainfosec.com/2011/08/30/information-assurance-versus-information-security/

History

- 1953 – Committee on National Security Systems (CNSS) formally National Security Telecommunications and Information Systems Security Committee (NSTISSC).
- July 5, 1990 – National Security Directive (NSD) 42.
- February 1996 – Clinger-Cohen Act (CCA) "Information Technology Management Reform Act of 1996 (ITMRA)"
- December 9, 1996 - DoD Directive S-3600.1 "Information Operations (U)"
- May 11, 1999 – NSA Designates first CAE in IA Education
  - James Madison University; George Mason University; Idaho State University; Iowa State University; Purdue University; University of California at Davis; and University of Idaho.

History

- April 2001 – Machonachy, Schou, Ragsdale and Welch publish “A model for Information Assurance: An Integrated Approach”
- October 16, 2001 – Executive Order (EO) 13231 “Critical Infrastructure Protection in the Information Age” – renames NSTISSC to CNSS
- January 23, 2003 – Executive Order (EO) 13284 “Executive Order Amendment of Executive Orders and Other Actions in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security”
- October 2005 – Dark, Ekstrom, and Lunt publish “Integration of Information Assurance and Security into the IT2005 Model Curriculum
- 2013 ACM and IEEE announce new CS curriculum requirements.
  - Includes Information Assurance knowledge area.

Definition

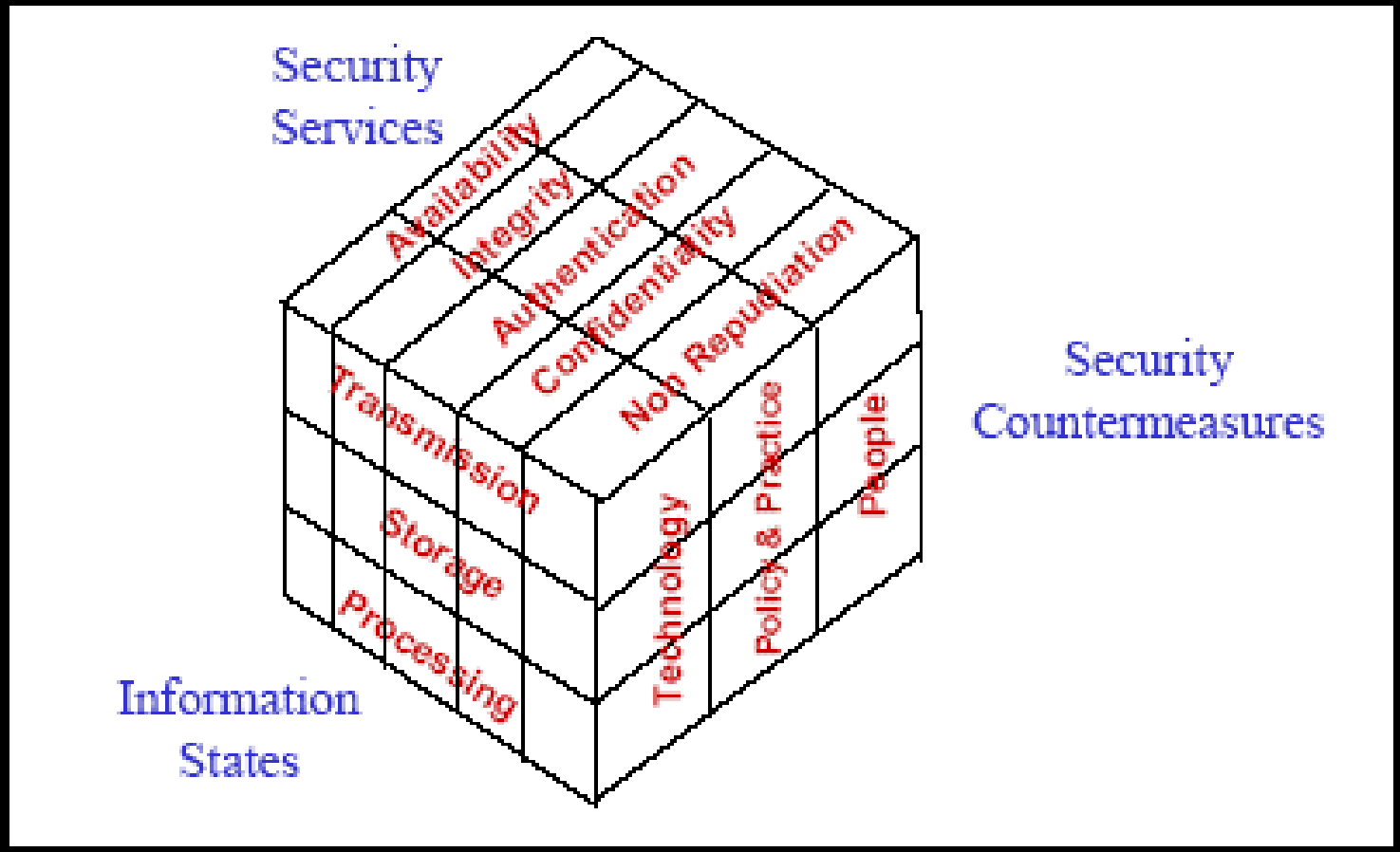
“A set of measures intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.”

-- Dark, Ekstrom, and Lunt (2005)

Definition

- Security Services
  - Confidentiality, Integrity, Availability, Authentication, and Non-Repudiation
- Security Countermeasures
  - Technology, People, and Policy & Practice
- Information States
  - Transmission, Storage, and processing

McCumber Information Assurance Model



Machonachy, W. Victor; Schou, Corey D.; Ragsdale, Daniel; Welch , Don; "A model for Information Assurance: An Integrated Approach", Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point , NY, 5-6 June 2001.

Availability

Availability (of systems and data for intended use only)

Availability is a requirement intended to assure that systems work promptly and service is not denied to authorized users. This objective protects against:

- Intentional or accidental attempts to either:
  - perform unauthorized deletion of data or
  - otherwise cause a denial of service or data.
- Attempts to use system or data for unauthorized purposes

Availability is frequently an organization's foremost security objective.

--NIST SP800-33 (2001)

Integrity

Integrity (of system and data)

Integrity has two facets:

- Data integrity (the property that data has not been altered in an unauthorized manner while in storage, during processing, or while in transit) or

- System integrity (the quality that a system has when performing the intended function in an unimpaired manner, free from unauthorized manipulation).

Integrity is commonly an organization's most important security objective after availability.

--NIST SP800-33 (2001)

Confidentiality

Confidentiality (of data and system information)

Confidentiality is the requirement that private or confidential information not be disclosed to unauthorized individuals. Confidentiality protection applies to data in storage, during processing, and while in transit.

For many organizations, confidentiality is frequently behind availability and integrity in terms of importance. Yet for some systems and for specific types of data in most systems (e.g., authenticators), confidentiality is extremely important.

--NIST SP800-33 (2001)

Accountability

- Accountability (to the individual level)
- Accountability is the requirement that actions of an entity may be traced uniquely to that entity.
- Accountability is often an organizational policy requirement and directly supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

--NIST SP800-33 (2001)

Non-Repudiation

Assurance (that the other four objectives have been adequately met)

Assurance is the basis for confidence that the security measures, both technical and operational, work as intended to protect the system and the information it processes. The other four security objectives (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation when:

- required functionality is present and correctly implemented,
- there is sufficient protection against unintentional errors (by users or software), and
- there is sufficient resistance to intentional penetration or by-pass.

Assurance is essential; without it the other objectives are not met. However, assurance is a continuum; the amount of assurance needed varies between systems.

--NIST SP800-33 (2001)

Progression to Information Assurance

Information Assurance Workforce

- Self Taught
- On the job training
- Peer-to-peer exchange
  - Conferences
  - Vendors
- Academia
- CERT 10 Principles of Information Assurance

Progression to Information Assurance

CERT Principle 1: Survivability is an enterprise wide concern

- Corporate culture
  - Top down
  - Policy driven
- Long term objective
- It is not if you will be compromised; it is when and how fast you react

Progression to Information Assurance

CERT Principle 2: Everything is Data

- Data exists in the following states
  - Storage
  - Transport
  - Processing (Endpoint)
- Understanding an organizations data allows an Information Assurance professional to apply the appropriate controls (TRIAD).
  - Public
  - Internal
  - Confidential
  - Protected Information (PHI, PII, PCI)

Progression to Information Assurance

CERT Principle 3: Not all data is of equal value to the enterprise – risk must be managed.

- Information Assurance professionals cannot protect everything
- Manage Risk
  - Transfer
  - Reduce / Mitigation
  - Accept
- Risk Assessment Frameworks
  - OCTAVE
  - FAIR
  - NIST-RMF
  - TARA

Progression to Information Assurance

CERT Principle 4: Information Assurance policy governs actions

- Policies / Standards / Procedures define the controls that protect and defend the availability, integrity, authentication, confidentiality, and non-repudiation of data.
- Protection controls
- Detection controls
- Reaction capabilities controls

Progression to Information Assurance

CERT Principle 5: Identification of users, computer systems, and network infrastructure components is critical.

- User Identification
  - Reliable
  - Strong
  - Usable
- Non-repudiation

Progression to Information Assurance

CERT Principle 6: Survivable Functional Units (SFU) are a helpful way to think about an enterprise's networks.

- Survivable Functional Units (SFUs) are collections of systems and related infrastructure components that deliver authenticated information services. For example a PCI zone is an SFU.
- SFUs should be constructed to provide vital information services in the presence of attacks and failures, and full recovery in a timely manner.

References: SFUs: Balancing an Enterprise's Mission and Technology
http://www.cert.org/archive/pdf/04tn04.pdf

Progression to Information Assurance

CERT Principle 7: Security knowledge in practice provides a structured approach.

- Hardware / Software (Vendors)
- Harden / Secure
- Prepare
- Detect
- Respond
- Improve

Progression to Information Assurance

CERT Principle 8: The roadmap guides implementation choices (all technology is not equal).

- Data complexity / security
  - Do Nothing
  - Be aware of data security issues
  - Identify Critical Assets
  - Apply Access Control Lists (ACLs) to data objects
  - Assign access permissions
  - Use encryption to protect data objects
  - Employ cryptography-based integrity checking

Progression to Information Assurance

CERT Principle 9: Challenge assumptions to understand risk.

- Think like a hacker
- Assess vulnerabilities of implemented technology
- Document assumptions
- It’s only ankle deep… when diving head first

Progression to Information Assurance

CERT Principle 10: Communication skill is critical to reach all constituencies.

- Adjust language based on the audience
- Know thy business
- Translate business terms into appropriate actions / controls
- Communication skills are critical

Conclusion

Quote from Robert M. Pirsig

“What follows is based on actual occurrences. Although much has been changed for rhetorical purposes, it must be regarded in its essence as fact. However, it should in no way be associated with that great body of factual information relating to orthodox Zen Buddhist practice. It’s not very factual on motorcycles either.”

This presentation does not give a definitive answer to how to move to Information Assurance, rather change your thinking on how to get there… hopefully.

Questions

Aaron Wampach

Aaron.Wampach@securademics.org