Information Assurance (IA) Challenges and Trends - for the Next Generation of IA Professionals?

Joint Workshop on Cyber Security
State University of New York - Buffalo

8 May 2008

Robert W. McGraw
Technical Director
IA Architecture & Systems Security Engineering Group
Information Assurance Directorate
National Security Agency

Purpose and Outline

- **Discuss some IA topics that will challenge the emerging generation of IA professionals**
  - These include:
    - Regulatory compliance
    - Influencing decision makers
    - Technology and other trends
- **Discuss some changes in NSA's IA Mission**

Regulatory Compliance

- **Federal**
  - SOX
  - GLBA
  - HIPAA
  - FISMA
  - FFIEC
  - …
- **State**
- **Industry**
  - PCI
- **International & Other Countries**

- **Goals**
  - Improve security
  - Mandate a minimum investment in IA
  - i.e. don’t leave it to the discretion of some corporate decision maker
- **Recent case of compliance enforcement**
  - Federal Trade Commission vs TJX Companies – March 2008

FTC vs TJX

- **FTC's complaint charged that TJX:**
  - (a) created an unnecessary risk to personal information by storing it on, and transmitting it between and within, in-store and corporate networks in clear text;
  - (b) did not use readily available security measures to limit wireless access to its networks, thereby allowing an intruder to connect wirelessly to in-store networks without authorization;
  - (c) did not require network administrators and other users to use strong passwords or to use different passwords to access different programs, computers, and networks;
  - (d) failed to use readily available security measures to limit access among computers and the internet, such as by using a firewall to isolate card authorization computers; and
  - (e) failed to employ sufficient measures to detect and prevent unauthorized access to computer networks or to conduct security investigations, such as by patching or updating anti-virus software or following up on security warnings and intrusion alerts

Regulatory Compliance – Some Questions

- Does compliance = Good IA?
- Does compliance = Good enough IA?
- How do we maximize the value of compliance?

We shouldn’t rely on compliance alone to achieve the right level of IA.
As IA professionals we must learn to influence discretionary investment beyond the minimum required when necessary to ensure the mission/operational goals of the enterprise.

Influencing Decision Makers

- IA Professionals need to improve ability to influence investment in IA
- In order to do this we need to improve the way we communicate with those that make such investment decisions
- Two suggested areas for improvement
  - Speak in terms that decision makers can understand
  - Provide analytic, value-based modeling to support IA recommendations

Decision Making at its Best!

Let's be realistic. The purpose of the system is to deliver functioning bombs on correct targets. The system with the best performance is obviously the only way to go!

Of course everyone knows that the best system is the most secure system! If you don't have security, you don't have squat!

This is all very good but as I look at the required milestones, we don't have any time to build in performance, security or to hold down costs. We have to ship tomorrow so our only option is to choose the one with the shortest schedule.

HELP!!

And who's going to pay for all that performance and security? It makes perfect financial sense to get about the same level of performance and security out of the system that costs the least. Isn't that what we should be talking about here?

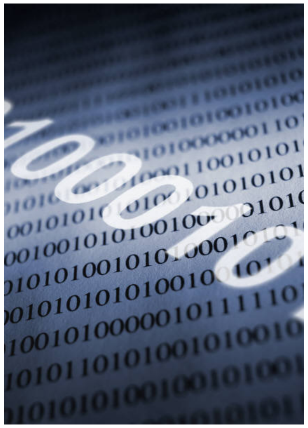
FTC vs TJX Redux

- **FTC's complaint charged that TJX:**
  - (a) created an unnecessary risk to personal information by storing it on, and transmitting it between and within, in-store and corporate networks in clear text;
  - (b) did not use readily available security measures to limit wireless access to its networks, thereby allowing an intruder to connect wirelessly to in-store networks without authorization;
  - (c) did not require network administrators and other users to use strong passwords or to use different passwords to access different programs, computers, and networks;
  - (d) failed to use readily available security measures to limit access among computers and the internet, such as by using a firewall to isolate card authorization computers; and
  - (e) failed to employ sufficient measures to detect and prevent unauthorized access to computer networks or to conduct security investigations, such as by patching or updating anti-virus software or following up on security warnings and intrusion alerts.

Compliance aside, how would you convince a CEO or a military general officer to make the necessary investments to fix these problems?

Other Challenges

- Technology churn
- Cyber threat is constant, and constantly changing
- Virtualization of IT Resources
- Direct protection of critical data assets
- Protection of data at rest



NSA’s Information Assurance Mission

- **NSA’s Information Assurance mission focuses on protecting National Security Information and Information Systems, in accordance with National Security Directive 42 (NSD 42).**
- **What we do**
  - We deliver IA technology, products and services meeting the operational needs of our clients and customers to secure their information and information systems

NSA Information Assurance Mission – Some Areas of Transition

Coming From	Moving To	Transformation Areas
Protecting confidentiality of classified data…	and real-time defense of information and systems	Bring a dynamic, operational focus
Providing government unique cryptographic equipment	Applying a broad spectrum of commercial IA & IT, with niche use of government products	Improve the security of commercial solutions
Providing more products than services	Providing more services than products, and influence by sharing of our knowledge	Build a knowledge vs product business and influence stakeholders
Avoiding risk	Managing risk	Risk analysis and value engineering processes

NSA’s Information Assurance Mission

- **Our Lines of Business**
  - IA Guidance
  - Security Engineering
  - Integrated Computer Network Operations
- **Our Focus**
  - Comprehensive vulnerability and threat analysis
  - Guidance on IA security solutions
  - Tiered security assessments
  - Network security products and solutions for assured information sharing
  - A 24/7 watch and analysis activity providing threat warnings, attack alerts and bulletins
  - Training and security awareness support
  - Key Management Infrastructure that supports fielded cryptographic equipment
  - Security engineering services that leverage government and commercial solutions
  - Leading edge IA research in areas not addressed by others

Recruiting Info

- If you are a US citizen and have skills in any of these areas:
  - Computer Science
  - Cryptography
  - Data Analysis
  - Information Assurance
  - Information Systems Management
  - Information Systems Security Engineering
  - Intelligence Analysis
  - Mathematics
  - Project Management
  - Risk Assessment
  - Security Product Development
  - Specification writing, standards requirements, design guidance
  - Systems Engineering
  - Threat Analysis
  - Vulnerability Discovery

Check out what a career in the IA Mission at NSA has to offer!

Summary and Questions