Establishing a Winning CIO/CISO Team in the Midst of a Changing Leadership Environment

W. Hord Tipton, CISSP-ISSEP, CAP, CISA
(ISC)² Executive Director

FISSEA 2009
March 26, 2009

Session Objectives

- ISOs – Who Should They Report to?
- The Role of the CIO
- To Integrate or Not to Integrate?
- Recent Trends
- What Every CIO Should Understand about Security
- Security/IT Personnel Integration
- FISMA 2
- CNCI
- Recent Developments
- Suggested Components of the Workforce Initiative
- Comments

ISOs – Who Should They Report to?

- Assess atmosphere for security tolerance
- Catastrophe Theory
- Questions:
  - What are you trying to protect?
  - What happens if you lose your data?
  - Who gets fired?
- Who beyond CIO wants to listen to ISOs? Speak a foreign language, always want $$ and bring bad news.

CIO = Translator

- CIOs need accountability for security.
- CIOs generally give security lower priority if they have no purview over it.
- CISOs don't get attention until the roof caves in.
- CIOs are well-positioned to act as translator to rest of executive team/boards.

To Integrate or Not to Integrate?

Cons

- Negative results occur unless:
  - Functions are integrated, allowing CIO to "bake in" security up front, enhancing security posture throughout.
  - Separated functions = loss of CIO ability to control security although the CIO remains accountable.

Pros

- Segregation gives security direct access to the top *(only successful if CISO is strong communicator and s/he is preaching to the converted)*.
- CISO will remain stable if CIO gets downgraded to reporting to CFO.

Recent Trends

- Recent shifts in IT governance are in the wrong direction.
- CIOs back to reporting to CFOs.
- Breaches are commonplace and more and more are recognized as cost of doing business.

What Every CIO Should Understand about Security

- SOA = security-oriented architecture as it fits within your overall architecture.
- Know how your networks work.
- Understand network security issues:
  - Perimeter control
  - Application security
  - Where your data is, how it's categorized, how accessible it needs to be, what kind of information assurance goes with it, set data standards.

What Every CIO Should Understand about Security (Cont.)

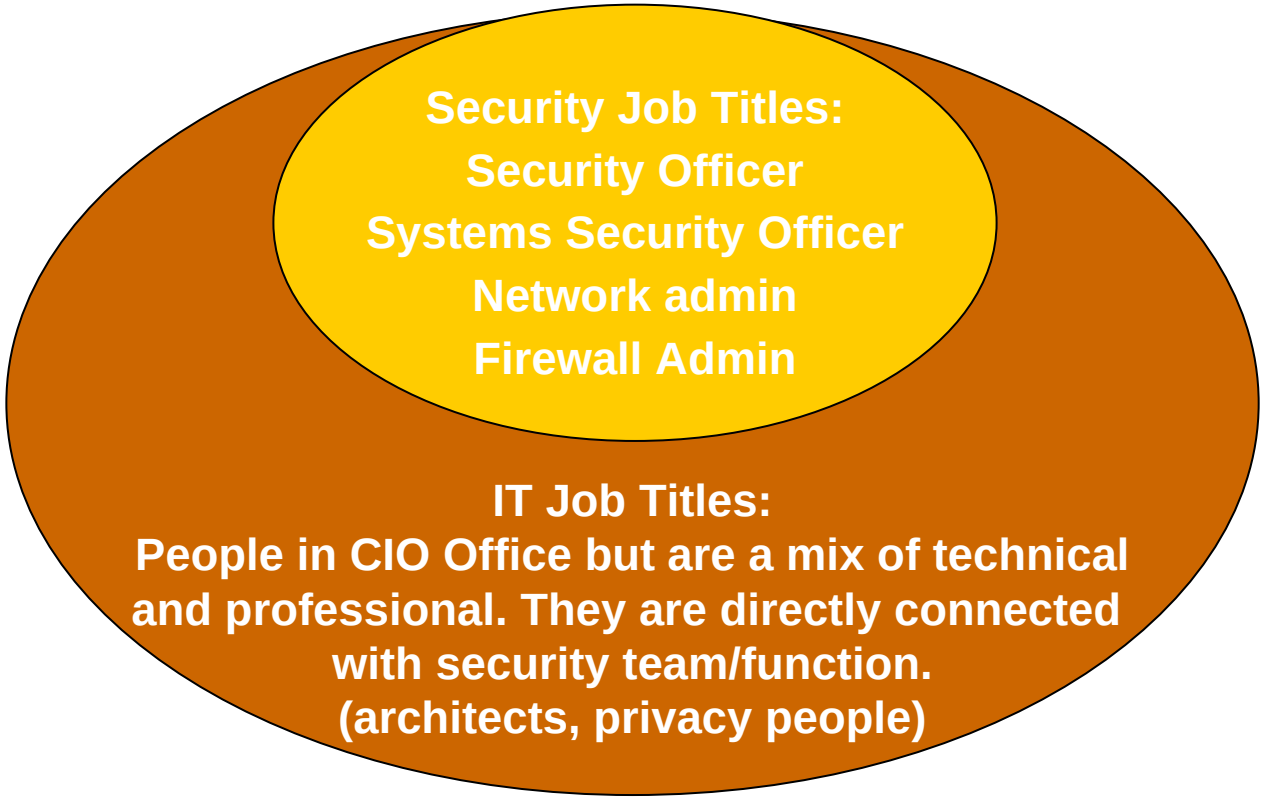
- When you modernize systems, bake security in.
- CISO serves as your bridge.

  --Should hold minimum of CISSP or CSSLP.

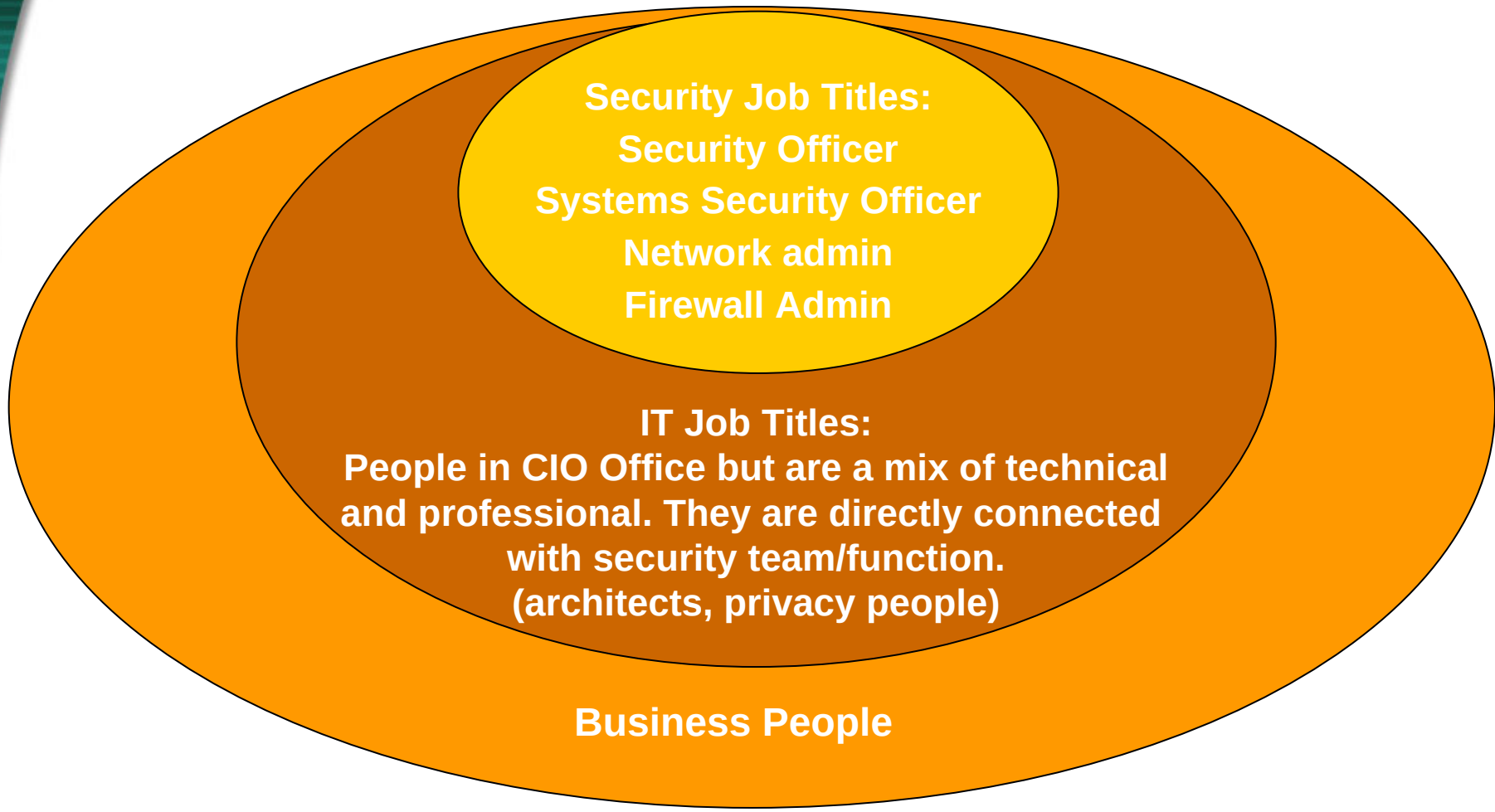
  --CISSP domains translate into realms CIO is responsible for.

Security/IT Personnel Integration

Security/IT Personnel Integration (Cont.)



Security/IT Personnel Integration (Cont.)



FISMA 2

- Appears that the bill that will be introduced by Senator Carper will go beyond FISMA.
- OMB seems to be interested in revising the annual reporting process.
- Continuous monitoring will become an integral part of the FISMA process.
- FISMA revision must be looked at from the CNCI perspective.

CNCI -- Project 1

- Response to a very serious problem.
- Criticisms about lack of transparency and over classification are correct.
- Workforce aspect of CNCI is a prime example.
- Hope the 60-day review addresses these issues.
- Need to bring resources of private sector, academic, and non-profit to bear on problem.

The Cyber Initiative and the Federal IT Security Workforce (Project 8)

- Speaking as an interested outsider who has followed this effort from my time in government.
- We do know that one of the twelve components of the CI pertains to workforce.
- An interagency working group has been focused on the workforce issue for the past year or so.
- Has not been a lot of public outreach or interaction with non-government parties.

Recent Developments

- Admiral Brown of DHS recently stated that the workforce effort has been refocused on the federal workforce.
- NIST is in the process of revising special publication 800-16, "Information security training requirements"—will retain the role based focus—draft coming soon.
- OPM is conducting an information systems security qualifications matrix study—completion soon.

Suggested Components of the Workforce Initiative

- Increase the size of the federal IT security workforce by reversing the impetus to outsource this function.
- Some of the civilian agencies have minimal staffing to accomplish baseline programs and functions. It is time to provide the staff resources needed to manage IT security programs.
- There is a need to infuse Scholarship for Service graduates into all parts of the government—not just those that have the most positions (usually in DoD, NSA, etc.).
- Need to provide assistance to all higher education information security programs to include community colleges.

Suggestions (Cont.)

- Establish IT/IA as a separate, distinct job series within the federal personnel management system.

  --Existing 2210 job series is an improvement, but it does not reflect the fact that it security has grown in size, importance and granularity.

  --Federal IT security professionals have the numbers, visibility and recognized body of professional doctrine to support a separate job series.

- There is a need for increased resources devoted to the professional development of existing IT security workforce. Interesting to note that the 2002 draft of the national plan called for the establishment of a federal cyber security academy.

- Professional certification is a prerequisite for improving the professionalism of the workforce. Question is how to implement this across the government.

Suggestions (Cont.)

- DoD model vs. State Department approach.
- Given the dynamic nature of the IT security field, additional resources need to be allocated to continuing education programs for IT security professionals.
- Establish a federal cyber security management academy for mid-level and senior IT security career officers.
- There is a need to reach out to new groups within our population to enhance the future IT security workforce—Veterans, Inner City Youth, etc.

Comments On The Cyber Initiative and Related Programs

- Despite the classified, closed nature of the Cyber Initiative, the workforce component should be accomplished in an open, collaborative environment.
- There is a need for reaching out to the academic, certification and private sector practitioner communities in the development of the Cyber Initiative workforce program.
- There is a need to provide some sort of roadmap to such activities as: the DHS EBK, NIST 800-16 and the OPM/CIO Council IT Security Qualifications Matrix Initiative.
- We see no indication or realization that information security is regarded as an international problem—except in the threat arena. Shouldn't we be working to leverage the strengths of the international community?

SECURE INFORMATION TECHNOLOGY THROUGH CERTIFIED PROFESSIONALS