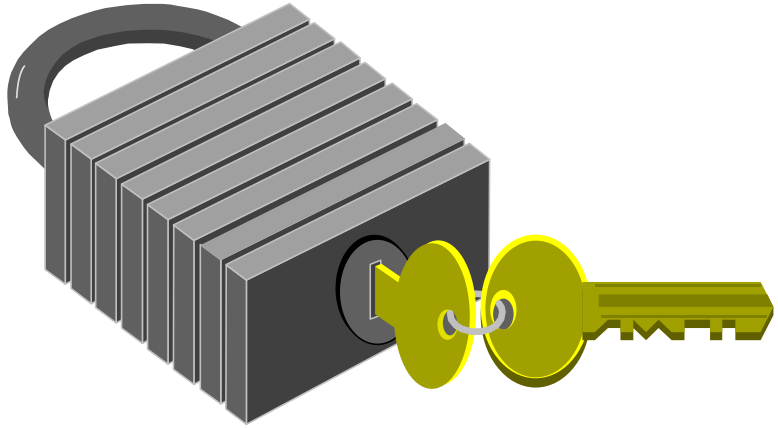

Who Should Really Manage Information Security in the Federal Government?

by

Alexander D. Korzyk, Sr. and

A. James Wynne

Who Should Really Mange Information Security?

Agenda

- Managing information
- Managing security
- ITMRA of 1996
- Federal Chief Information Security Officer (CISO)
- Federal CIO
- Federal CEO
- Federal Chief Technology Officer
- Federal Senior Information Resource Manager
- Managing Information Security
- Conclusions

Who Should Really Manage Information Security?

Federal CIO Top 10 Challenges

Number By Rank	Challenge	Percent
1	**Implementing IT capital planning and investment management**	**76**
2	Measuring IT contribution to mission performance	56
3	**Formulating or implementing an agency IT architecture**	**52**
4	Aligning IT and organizational mission goals	41
5	Championing BPR as a precursor to IT decisions	37
6	Building effective relationships with agency senior executives	35
7	Gaining a seat at the senior management table	32
8	Engaging senior executives on IT strategic directions	30
9	Providing effective IT infrastructure and related services	27
10	Ensuring Year 2000 operations	25

Survey results from AFFIRM October 1996

Who Should Really Manage Information Security?

Federal CIO Top 10 Critical Technologies

Number By Rank	Critical Technology	Percent
1	Internet/Intranet/Web	73
2	**Security Technology**	**68**
3	Electronic Commerce/Electronic Data Interchange	57
4	Distributed Computing	47
5	Data Warehousing	42
6	Client/Server Computing	41
7	Workflow	35
8	Executive Information Systems/DS S	28
9	Groupware	22
10	Relational Databases	21

Survey results from AFFIRM June 1996

Who Should Really Manage Information Security?

CIO Top 10 Emerging Technologies

Number By Rank	Critical Technology
1	Internet and the WorldWideWeb
2	Electronic Commerce
3	Groupware
4	Knowledge Management
5	**Network Security**
6	Broadband networks
7	Object-oriented technologies
8	New user interfaces
9	Wireless communications
10	Modeling and simulation

Survey results from CIO June 1, 1997

Who Should Really Manage Information Security?

Internet Concerns

No.	Concern	Percent
1	Inadequate security for our network	43.3%
2	Inadequate transaction security	37.4%
3	Employees will be distracted and surf too much	33.3%
4	Overloading the network	31.2%
5	Unpredictable performance	28.7%
6	Unreliable connections from ISP	20.2%

Survey results from InfoWorld Dec. 23/30, 1996

Who Should Really Manage Information Security?

Creating the Chief Information Security Officer

Change Elements	Security Culture	Actions
Information Security Model	Business Risk Management	CISO Office
Information Security Programs acceptance and creditability	Fundamental Behavior by entire organization	Business Information Security Officers
Link to Business Objectives	Infrastructure Cornerstone	Sell Security

CISO Paradigm from NCSA News, July 1996

Who Should Really Manage Information Security?

Federal Chief Information Officer

- Political appointee vs. government bureaucrat
- Renamed the senior IRM bureaucrat
- Reports to whom?
- Industry beginning to eliminate CIOs
- Pressured by deadlines to cut security short

Who Should Really Manage Information Security?

Federal Chief Executive Officer

- Political appointee
- Concerned with core competencies
- Outsourcing information technology and information security
- Privatizing the agency
- Reengineering the bureaucracy

Who Should Really Manage Information Security?

Federal Chief Technology Officer

- Don’t automate. Obliterate!
- CIO vs. CTO
- Industry replacing CIOs with CTOs
- Technology moving too fast
- Personnel must retrain more often to keep up with new technology

Who Should Really Manage Information Security?

Federal Senior Information Resource Manager

- IRM officials have become ineffective
- Professional bureaucrats
- Dual chain of command with contractors who perform the work
- Government employees non-productive
- Culture of avoiding blame and responsibility

Who Should Really Manage Information Security?

Federal Chief Information Security Officer

- Separate from CIO
- Same level as CFO or CIO
- Upper management Security expert
- Provides independent verification
- Unbiased by internal pressures to deliver a product on time by cutting short security
- Everyone knows who is in charge of Information Security