RSACONFERENCE2013

I, (MR. TECHIE) GOT THE CISO JOB! SHOULD I PREPARE 3 ENVELOPES?

Todd Fitzgerald
Director Global Information Security
Information Security Management Author
ManpowerGroup, Inc.
(NYSE:MAN, Fortune 500 #129)

Session ID: MASH-F43

Session Classification: Intermediate

(Security Architect/Officer)

(YES THIS WAS A REAL JOB POSTING!!!!)

Job description:
This position will represent the information protection program of the' region and requires the ability to understand business issues and processes and articulate appropriate security models to protect the assets of and entrusted to. A strong understanding of information security is necessary to manage, coordinate, plan, implement and organize the information protection and security objectives of the' region. This position is a senior technical role within our information protection and security department. A high-level of technical and security expertise is required and will be responsible for managing information security professionals. This position will play a key role in defining acceptable and appropriate security models for protecting information and enabling secure business operations. This person must be knowledgeable of current data protection best practices, standards and applicable legislation and familiar with principles and techniques of security risk analysis, disaster recovery planning and business continuity processes and must demonstrate an understanding of the management issues involved in implementing security processes and security-aware culture in a large, global corporate environment. He or she will work with a wide variety of people from different internal organizational units, and bring them together to manifest information security controls that reflect workable compromises as well as proactive responses to current and future business risks to enable ongoing operations and protection of corporate assets. RESPONSIBILITIES INCLUDE: • Manage a cost-effective information security program for the Americas region; aligned with the global information security program, business goals and objectives • Assist with RFP and Information Security responses for clients • Implementing and maintaining documentation, policies, procedures, guidelines and processes related to ISO 9000, ISO 27000, ISO 20000, European Union Safe Harbor Framework, Payment Card Industry Data Protection Standards (PCI), SAS-70, General Computer Controls and client requirements • Performing information security risk assessments • Ensuring disaster recovery and business continuity plans for information systems are documented and tested • Participate in the system development process to ensure that applications adhere to an appropriate security model and are properly tested prior to production • Ensure appropriate and adequate information security training for employees, contractors, partners and other third parties • Manage information protection support desk and assist with resolution • Manage security incident response including performing investigative follow-up, assigning responsibility for corrective action, and auditing for effective completion • Manage the change control program • Monitor the compliance and effectiveness of Americas' region information protection program • Develop and enhance the security skills and experience of infrastructure, development, information security and operational staff to improve the security of applications, systems, procedures and processes •

… A Complete Job Description

Direct senior security personnel in order to achieve the security initiatives • Participate in the information security steering and advisory committees to address organization-wide issues involving information security matters and concerns, establish objectives and set priorities for the information security initiatives • Work closely with different departments and regions on information security issues • Consult with and advise senior management on all major information security related issues, incidents and violations • Update senior management regarding the security posture and initiative progress • Provide advice and assistance concerning the security of sensitive information and the processing of that information • Participate in security planning for future application system implementations • Stay current with industry trends relating to Information Security • Monitor changes in legislation and standards that affect information security • Monitor and review new technologies • Performs other Information Security projects / duties as needed MINIMUM QUALIFICATIONS: Transferable Skills (Competencies) • Strong communication and interpersonal skills • Strong understanding of computer networking technologies, architectures and protocols • Strong understanding of client and server technologies, architectures and systems • Strong understanding of database technologies • Strong knowledge of information security best practices, tools and techniques • Strong conceptual understanding of Information Security theory • Strong working knowledge of security architecture and recovery methods and concepts including encryption, firewalls, and VPNs • Knowledge of business, security and privacy requirements related to international standards and legislation (including ISO 9001, ISO 27001, ISO 20000, Payment Card Industry data protection standard (PCI), HIPPA, European Union Data Protection Directive, Canada's Personal Information Protection and Electronic Documents Act, SAS-70 Type II, US state privacy legislation and Mexico's E-Commerce Act) • Knowledge of risk analysis and security techniques • Working knowledge of BCP and DR plan requirements and testing procedures • Working knowledge of Windows XP/2000/2003, Active Directory, and IT Infrastructure security and recovery methods and concepts • Working knowledge of Web-based application security and recovery methods and concepts • Working knowledge of AS400 security and recovery methods and concepts • Working knowledge of PeopleSoft security and recovery methods and concepts • Working Knowledge of anti-virus systems, vulnerability management, and violation monitoring • Strong multi-tasking and analytical/troubleshooting skills • Knowledge of audit and control methods and concepts a plus • Knowledge of SAS-70 audit requirements a plus • Knowledge of ISO 9001 requirements a plus • Knowledge of ISO 27001 requirements a plus • Knowledge of ISO 20001 requirements a plus • Knowledge of COBIT requirements a plus • Knowledge of EU / Safe Harbor requirements a plus • Knowledge of Linux security a plus • Knowledge of VB.NET, C++, JAVA, or similar programming languages a plus • Proficient in MS-Office suite of products • Professional, team oriented Qualifications • Bachelor's Degree (B.A., B.S.), or equivalent combination of education and experience in Information Security, Information Technology, Computer Science, Management Information Systems or similar curriculum • 7+ years of Information Technology or Information Security experience, including at least 5 years dedicated to Information Security • 2+ years of Travel Industry experience preferred • Must be a Certified Information Systems Security Professional (CISSP) • Certified Information Security Manager (CISM) preferred • Strong organizational, time management, decision making, and problem solving skills • Strong initiative and self motivated professional • Professional certifications from ISACA, (ISC)2, or SANS preferred • Experience with ISO certified systems a plus

Where Did The Security Officers Come From ?

- Raised their hand at the wrong time during a meeting
- Didn’t attend the selection meeting
- Last IT guy in the shop
- Working on compliance/privacy – must know something about security
- Chose this career (full deck not in order !)

QUICK 5 QUESTION TECHIE OR CISO QUIZ (to determine the roadmap for the rest of your life)

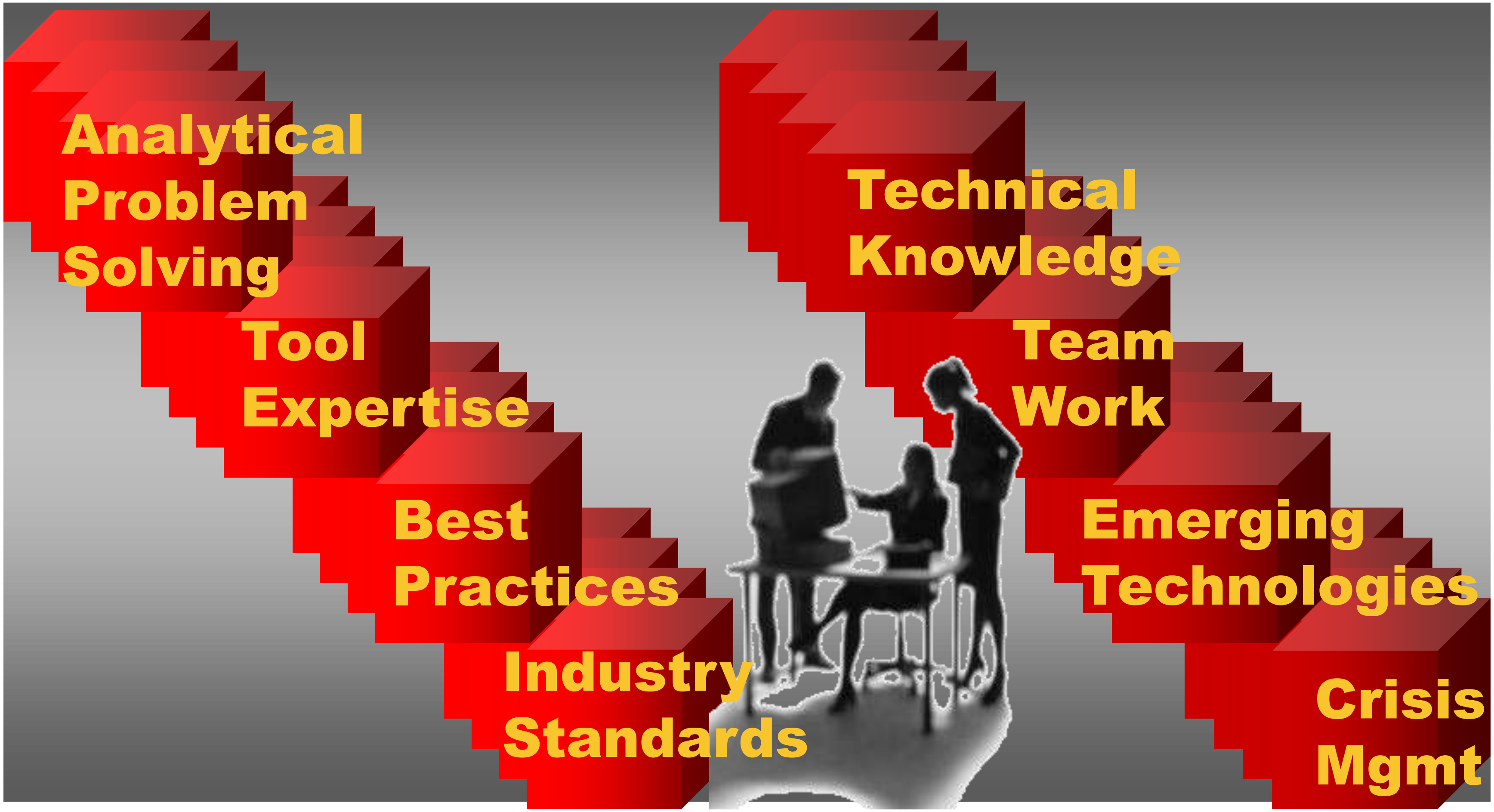
- For each pair of images flashed on the screen
- Pick the image that you 👍 the most
- Rely on your first impression

THIS

or

THAT ?

"Techie" Core Competencies



Analytical Problem Solving

Tool Expertise

Best Practices

Industry Standards

Technical Knowledge

Team Work

Emerging Technologies

Crisis Mgmt

Leadership Competencies

Interpersonal

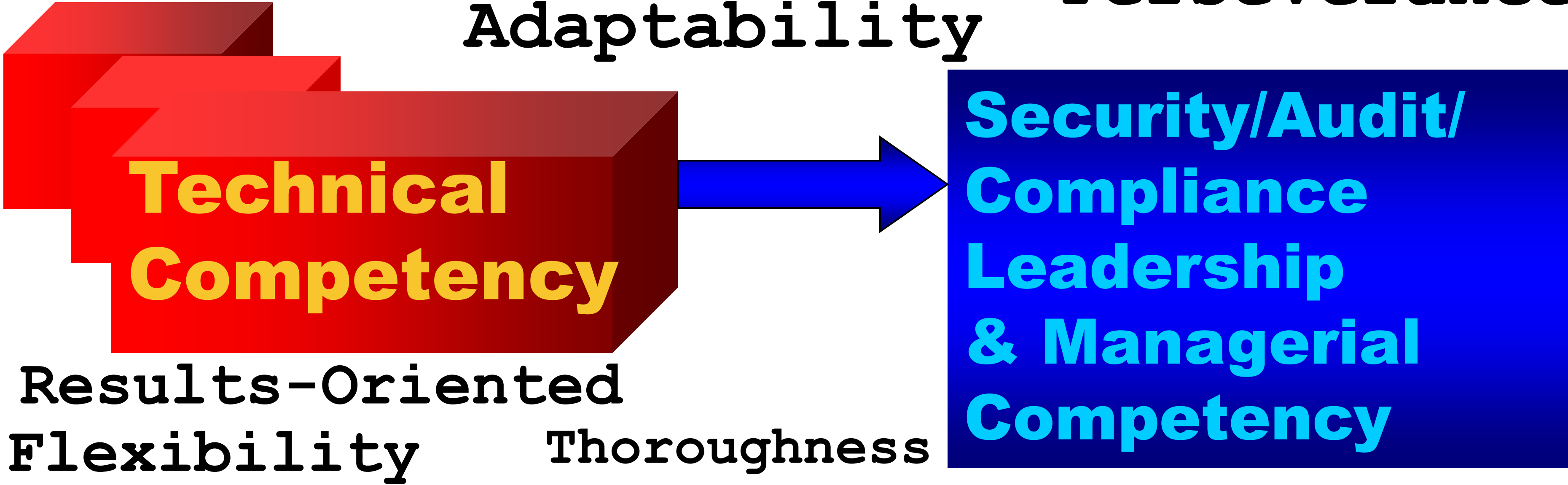
Awareness

Self-control

Self-control

Perseverance

Adaptability



Technical Competency

Security/Audit/ Compliance Leadership & Managerial Competency

Results-Oriented

Flexibility

Thoroughness

Initiative

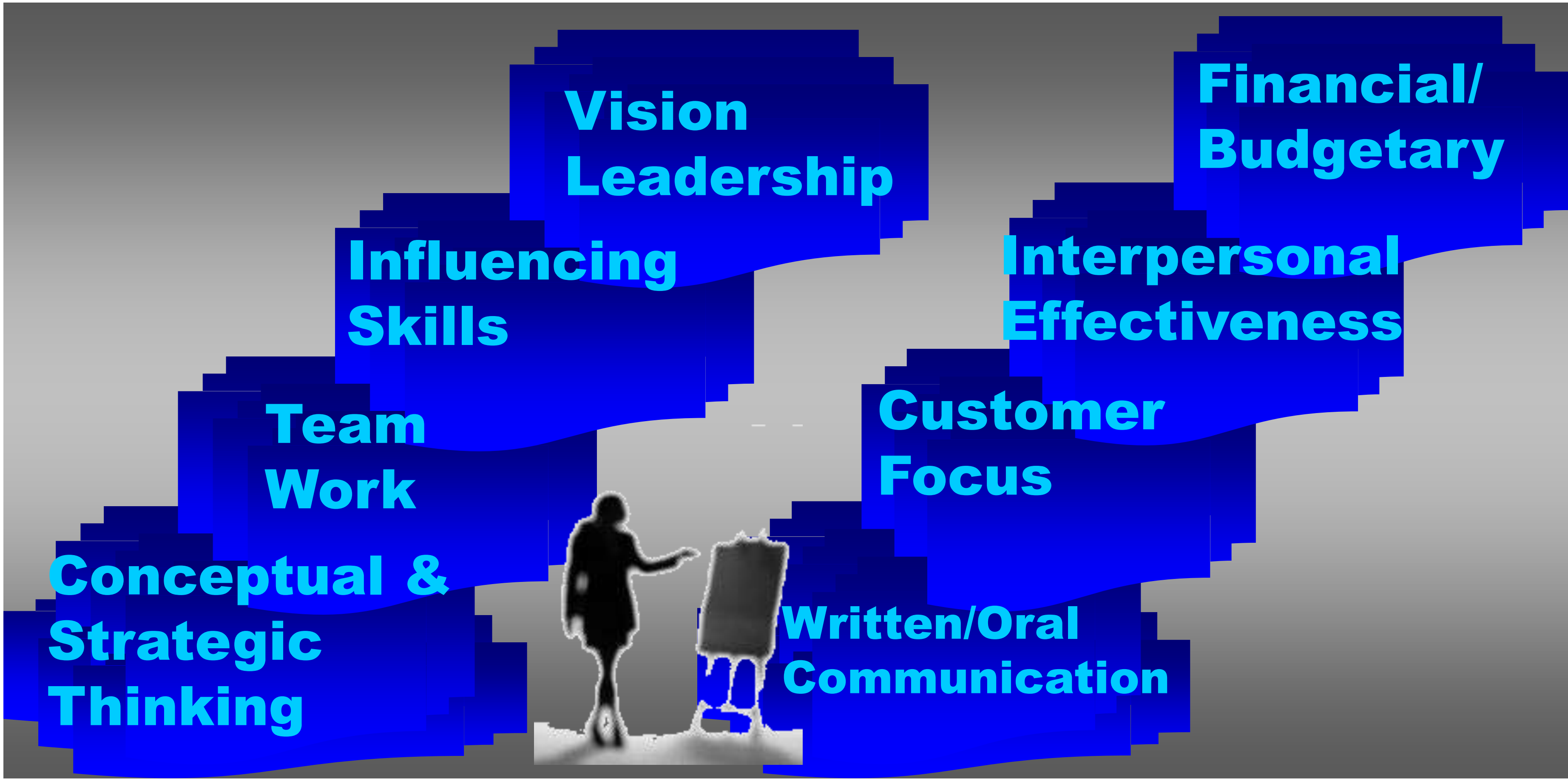
Self-Development Orientation

Critical

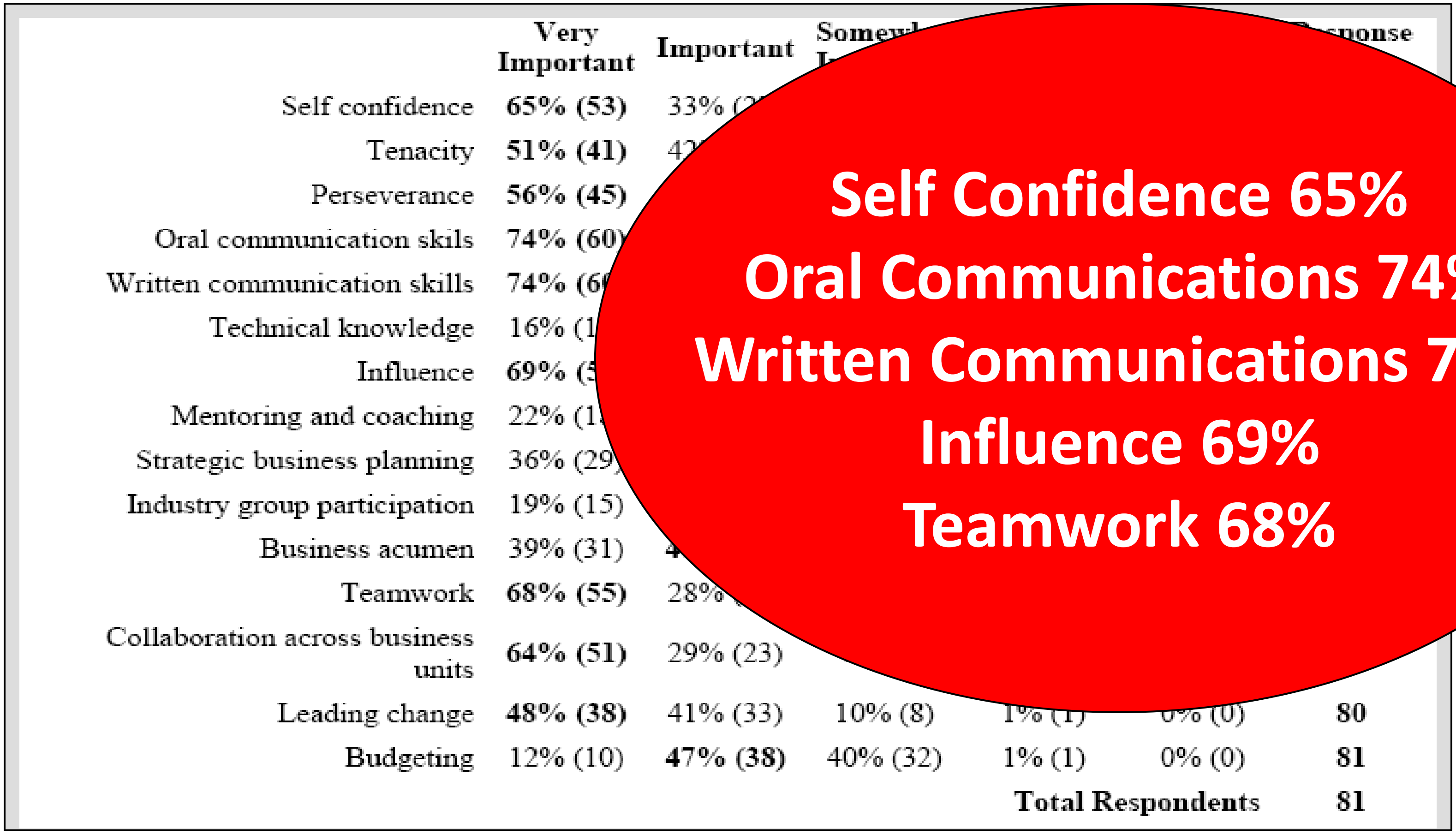
Efficiency

Information Seeking

Non-Technical Core Competencies


Vision Leadership
Financial/ Budgetary
Influencing Skills
Interpersonal Effectiveness
Team Work
Customer Focus
Conceptual & Strategic Thinking
Written/Oral Communication

Important Security Leadership Skills



	Very Important	Important	Somewh I			esponse
Self confidence	**65% (53)**	33% (2				
Tenacity	**51% (41)**	42				
Perseverance	**56% (45)**					
Oral communication skils	**74% (60)**					
Written communication skills	**74% (6**					
Technical knowledge	16% (1					
Influence	**69% (5**					
Mentoring and coaching	22% (1					
Strategic business planning	36% (29)					
Industry group participation	19% (15)					
Business acumen	39% (31)	**4**				
Teamwork	**68% (55)**	28%				
Collaboration across business units	**64% (51)**	29% (23)				
Leading change	**48% (38)**	41% (33)	10% (8)	1% (1)	0% (0)	**80**
Budgeting	12% (10)	**47% (38)**	40% (32)	1% (1)	0% (0)	**81**
				Total Respondents		**81**

Self Confidence 65%

Oral Communications 74%

Written Communications 74%

Influence 69%

Teamwork 68%

Source: Fitzgerald/Krause CISO Survey, *CISO Leadership Skills*, 2008 ISC2 Press

Career Path Decision Point: Techie or CISO *Differences In Thought Processes*

Technical

- Technical challenge
- Concrete non-ambiguous solutions
- Task-oriented
- Mastery of technical skill
- Hands-on training focus
- Documentation aversion
- High level of individual contribution
- Meetings are distractions

☑ Technical Expert
☑ Chief Information Security Officer

Career Path Decision Point: Techie or CISO

Differences In Thought Processes ?

Managerial

☑ **Technical Expert**

☑ **Chief Information Security Officer**

- Business relationships
- People-oriented/Conflict Resolution
- Consensus building
- Many presentations
- Influence
- Team building
- Accepting ambiguity and uncertainty
- Meetings, meetings, Meetings!
- Oral communication with all organizational levels

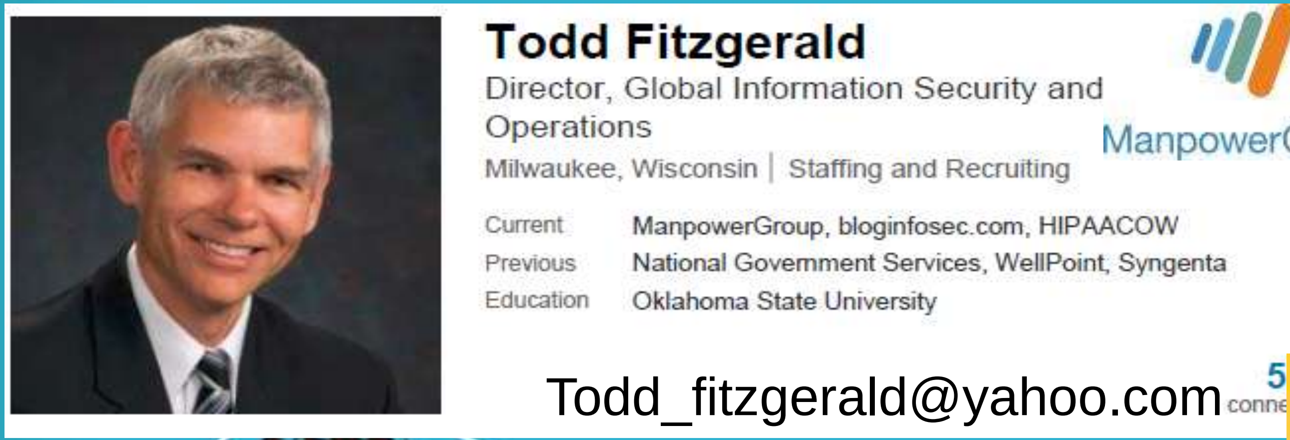
Gartner Research Says The CISO…

Gartner

Source: Emerging Role and Skills
For the CISO Gartner Report

- Balances needs of the business with
  - Increased regulated controls
  - Increased complexity
- Translates “technical speak”
- Has a solid background
  - 5-7 Years Information Security
  - Additional IT Background
- Thinks strategically, Politically Savvy
- Knowledgeable of key aspects of business
- Possesses certification

RSACONFERENCE2013



Todd Fitzgerald

Director, Global Information Security and Operations

Milwaukee, Wisconsin | Staffing and Recruiting

ManpowerGroup

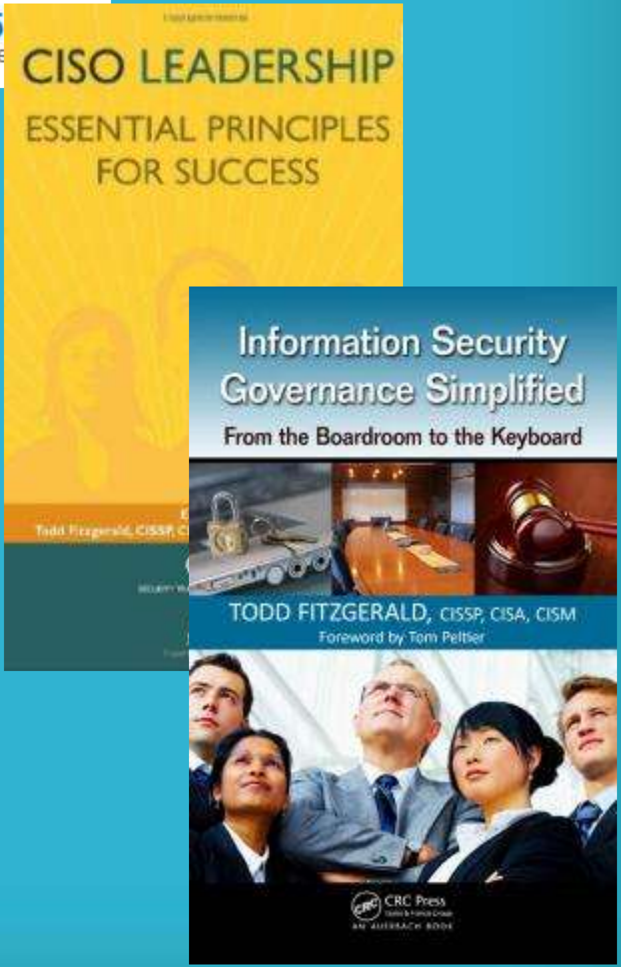
Current	ManpowerGroup, bloginfosec.com, HIPAACOW
Previous	National Government Services, WellPoint, Syngenta
Education	Oklahoma State University

Todd_fitzgerald@yahoo.com

5

conne

QUESTIONS?



CISO LEADERSHIP

ESSENTIAL PRINCIPLES FOR SUCCESS

Todd Fitzgerald, CISSP, C

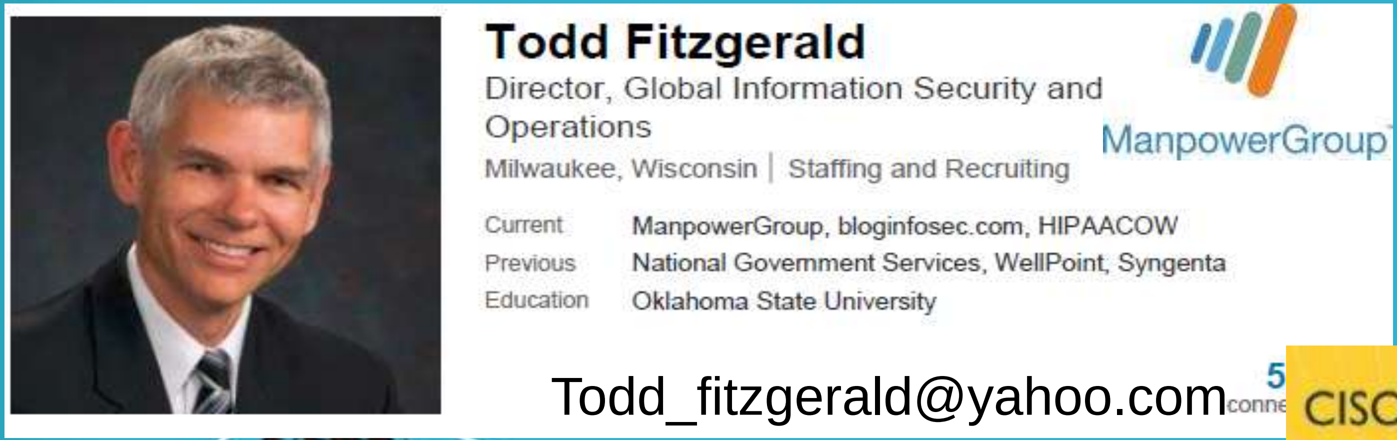
Information Security Governance Simplified

From the Boardroom to the Keyboard

TODD FITZGERALD, CISSP, CISA, CISM

Foreword by Tom Peltier

CRC Press



Todd Fitzgerald

Director, Global Information Security and Operations

Milwaukee, Wisconsin | Staffing and Recruiting

ManpowerGroup

Current ManpowerGroup, bloginfosec.com, HIPAACOW

Previous National Government Services, WellPoint, Syngenta

Education Oklahoma State University

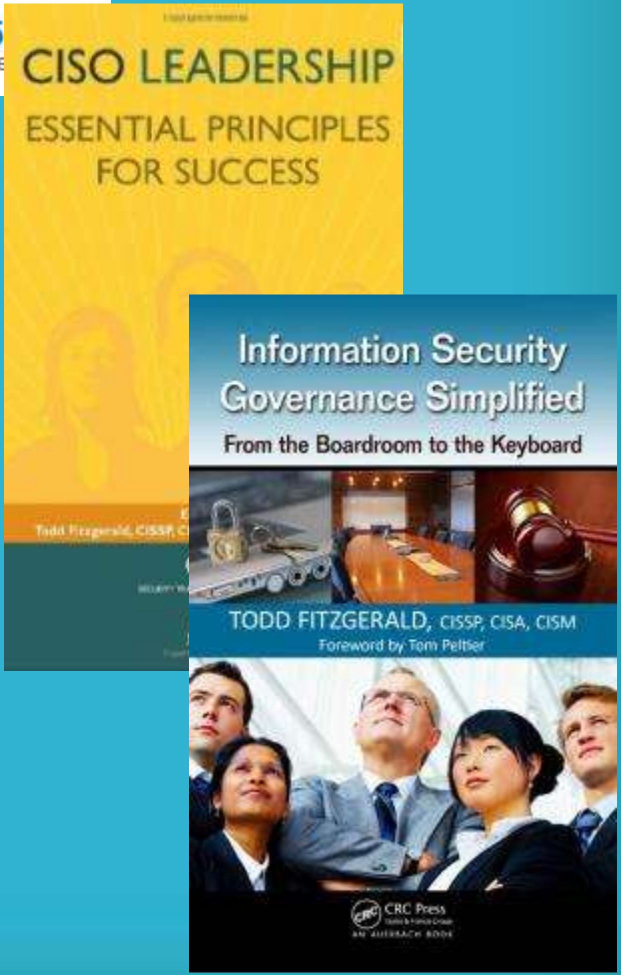
5
conne

Todd_fitzgerald@yahoo.com

THANK YOU

FOR YOUR

PARTICIPATION


CISO LEADERSHIP
ESSENTIAL PRINCIPLES FOR SUCCESS
Todd Fitzgerald, CISSP, C
Information Security Governance Simplified
From the Boardroom to the Keyboard
TODD FITZGERALD, CISSP, CISA, CISM
Foreword by Tom Peltier
CRC Press