RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

So Why on Earth Would You WANT To be a CISO?

SESSION ID: PROF-M05A

Todd Fitzgerald

CISSP, CISA, CISM, CRISC, CGEIT, PMP, ISO27000, CIPP, CIPP/US, ITILV3f
Global Director of Information Security
Grant Thornton International, Ltd.
@securityfitz

Disclaimer

- Todd Fitzgerald is a Director of Information Security with Grant Thornton International Ltd. The views expressed in this presentation are solely Todd Fitzgerald's personal views and do not necessarily represent the views of Grant Thornton or its clients or its related entities. The information provided with respect to Todd Fitzgerald's affiliation with Grant Thornton is solely for identification purposes and may not and should not be construed to imply endorsement or support by Grant Thornton of the views expressed herein.

Grant Thornton | An instinct for growth™

About Grant Thornton

Grant Thornton
An instinct for growth™

Global advisory revenues

$1.1bn

18% growth 2012

Ranked in the top 6 in major markets

WORKING MOTHER 100 BEST COMPANIES 2013

Global tax revenues

$909m 9% growth (2012)

GLOBAL TOP 50 World's Most Attractive Employers Powered by UNIVERSUM 2013

Mergers in 19 countries Q1-Q3 2012 adding revenues of **$250m**

35,000 people in over **100** countries

Total global revenues

$4.2bn (2012)

Grant Thornton | An instinct for growth™

Let's Level Set: The CISO Job Description/Expectations

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 •

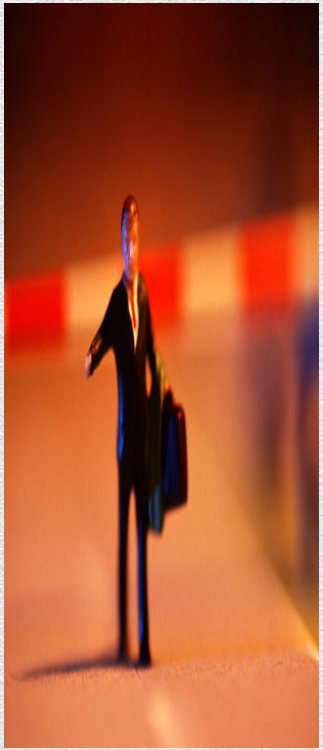
… Page 2

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

HELP!!!!

The *Real* DNA of the CISO Job

There IS a Selection Process!!!



- 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 !)

These "Techie Aspects" Got You Where You Are Today

- Analytical Problem Solving
- Tool Expertise
- Best Practices
- Industry Standards

- Technical Knowledge
- Team Work
- Emerging Technologies
- Crisis Mgmt

Leadership Competencies

Interpersonal Awareness

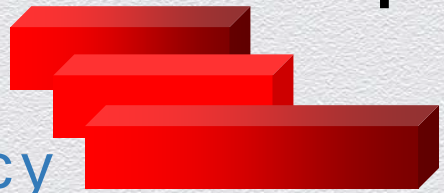
Self-control

Self-control

Perseverance

Adaptability

Technical Competency



Security/Audit/ Compliance Leadership & Managerial Competency

Results-Oriented

Flexibility

Thoroughness

Initiative

Self-Development

Critical

Efficiency

Orientation

Information Seeking

The Leadership Skills For Tomorrow's CISO Job

Vision Leadership

Financial/ Budgetary

Influencing Skills

Interpersonal Effectiveness

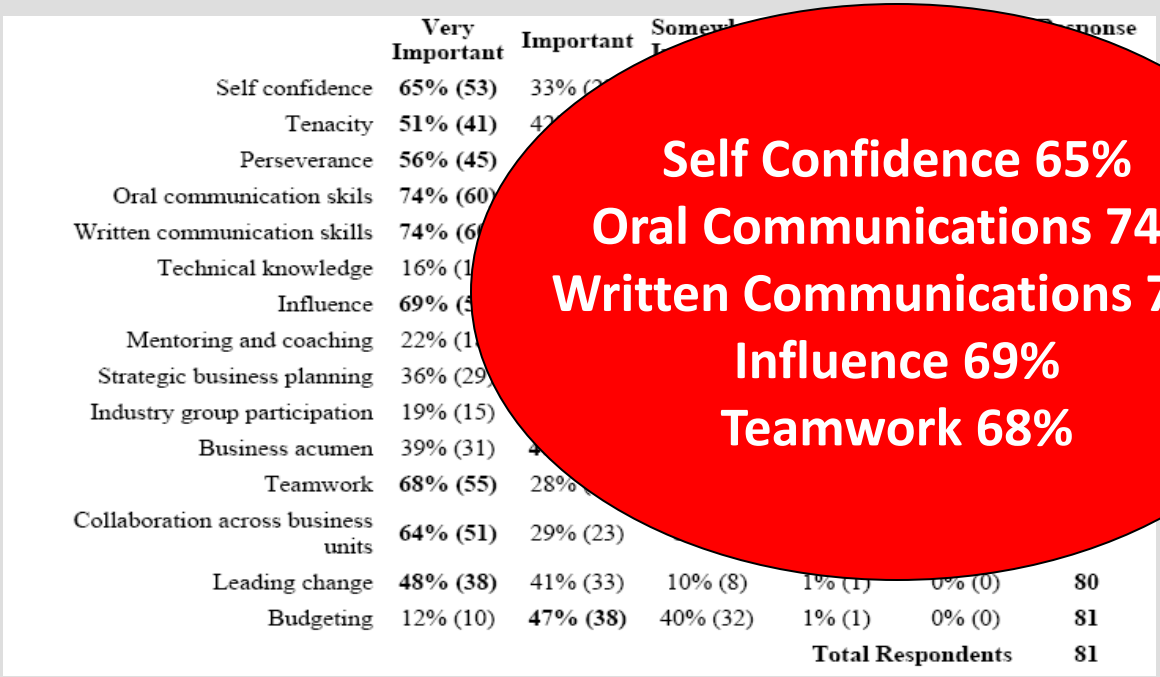
Team Work

Customer Focus

Conceptual & Strategic Thinking

Written/Oral Communication

Important Security Leadership Skills..



	Very Important	Important	Somewhat Important	Not Important	No Response	
Self confidence	**65% (53)**	33% (27)				
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**

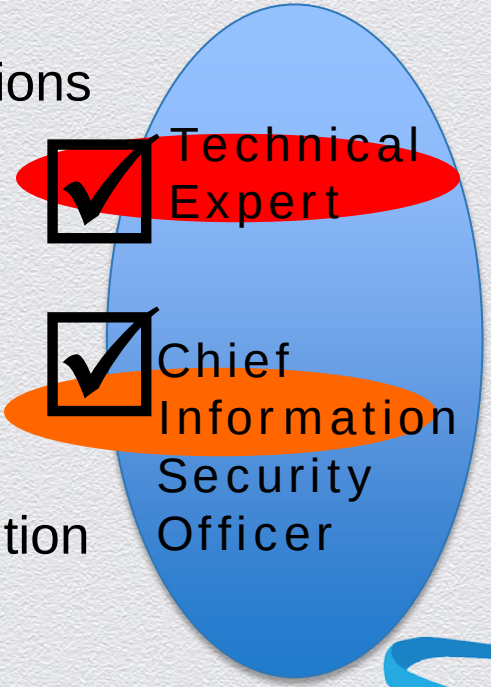
Self Confidence 65%
Oral Communications 74%
Written Communications 74%
Influence 69%
Teamwork 68%

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

It Is Not For Everyone! 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



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

Leadership/ Managerial

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

Forrester Says.. Leadership Skills Paramount As Security Skills Wane In Importance for 2018 CISO

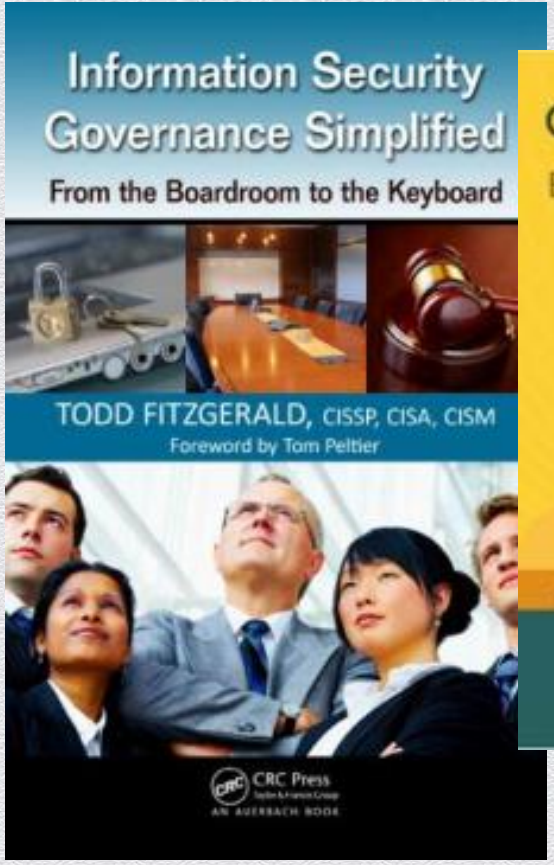
- Plan a path away from operations
- Refine risk management processes to business language
- Widen vision to privacy, data management and compliance
- Build a support network for insights
- Leverage new business skills to create focus and attention of business leaders

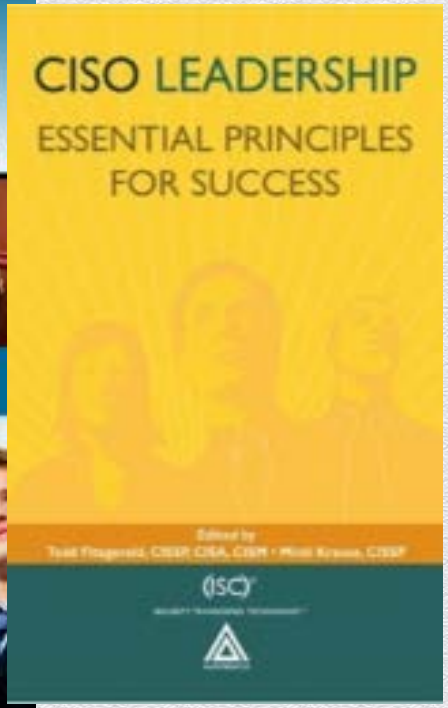
Final Thoughts

- Both technical and leadership security jobs will be in demand
- Be honest with yourself and get EXCITED!!!
- Explore lateral/broad security experiences (technical)
- Immerse yourself in leadership literature (managerial/leadership)
- Build social networks and learn from each other
- Nothing is permanent, Nothing is wasted

Suggested References

- *Information Security Governance Simplified: From The Boardroom to the Keyboard (Fitzgerald)*
- *CISO Leadership: Essential Principles for Success (Fitzgerald & Krause)*
- *Do What You Are: Discover the Perfect Career for you through the Secrets of Personality Type (Tieger and Tieger)*





Grant Thornton | An instinct for growth™

Thank You!

Grant Thornton
An instinct for growth™

Todd Fitzgerald
Global Information Security Director
Grant Thornton International, Ltd.
Oak Brook Terrace, IL
todd.fitzgerald@gti.gt.com
linkedin.com/in/toddfitzgerald
Todd_fitzgerald@yahoo.com

Grant Thornton | An instinct for growth™