RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: CXO-F01

Super CISO 2020: How to Keep Your Job

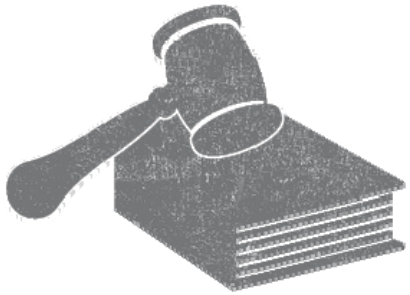
Todd Fitzgerald, CISSP, CISA, CISM, CIPP, CIPP/US, CIPP/E, PMP, ISO27001, CGEIT, CRISC, CIPM

Global Director Information Security
Grant Thornton International, Ltd
Oak Brook Terrace, IL
@securityfitz

#RSAC

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™

The CISO Job


ROYAL

The CISO Job Description

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 •

…Continued

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

APPROVED

Grant Thornton
An instinct for growth™

The CISO's Knowledge Base Must Be Very Broad

Source: 2016 RSA Conference Submission Titles

Business Card Version…

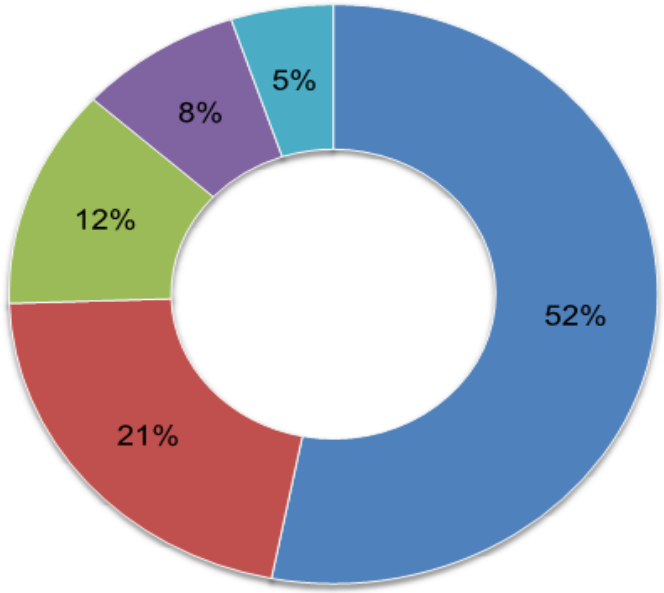
I.M. SuperCISO

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 investigation, 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 •

Grant Thornton
An instinct for growth™

Primary Rationale for Establishing the CISO Function

Study of companies with 1,000 or more employees



- Ex-post response to a security incident or breach
- Ex-post response to compliance and regulatory snafus
- To keep pace with other companies
- In response to liability and exposure
- To preserve reputation

Source: CISOS: The Good, The Bad, & The Ugly, Ponemon Institute, 12/13

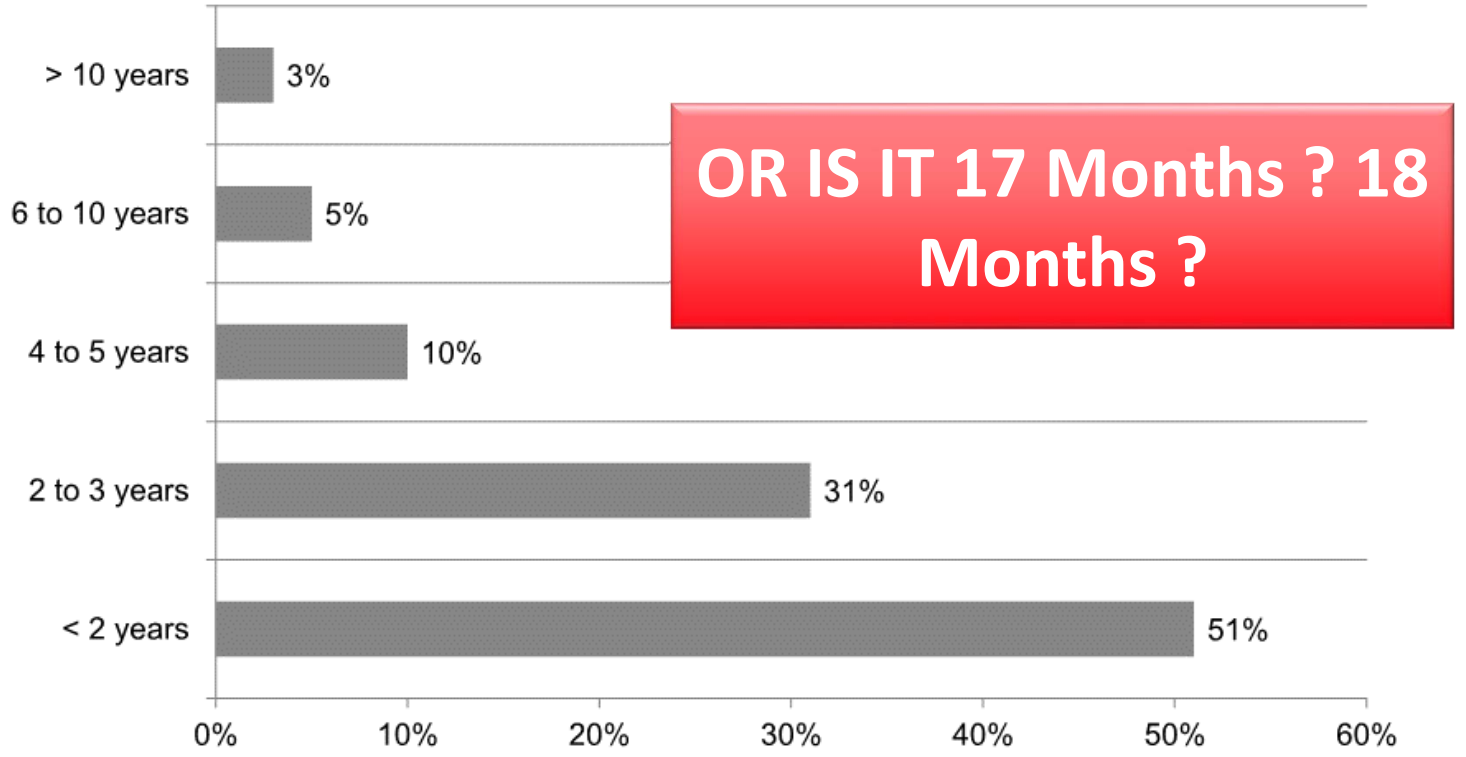
…But The CISO Is Still Viewed As Necessary

*** Does your organization have a Chief Information Security Officer?**

Answer	0% — 100%	Response Ratio
Yes, and it's a good thing.		58.8%
Yes, but I think it is unnecessary. I could handle the security-related work.		0.0%
No, and we're fine without one.		29.4%
No, but we need one.		11.7%
No Responses		0.0%
	Totals	100%

Source: http://healthsystemcio.com/2014/06/26/survey/

CISOs are Very Mobile Today: Average is 2.1 years or less



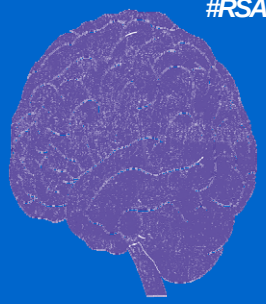
OR IS IT 17 Months ? 18 Months ?

Source: CISOs: The Good, The Bad and the Ugly, Ponemon Institute, 12/2013

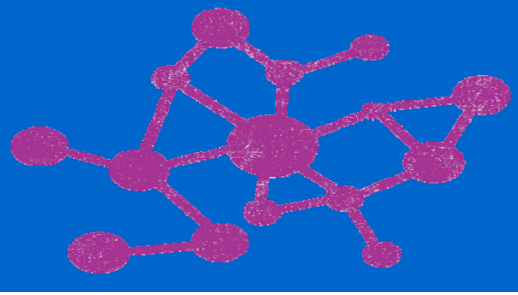
RSAConference2016

#RSAC

What Makes a "Leading Information Security Program?"



"We are on the verge of a revolution that is just as profound as the change in the economy that came with the industrial revolution. Soon electronic networks will allow people to transcend the barriers of time and distance and take advantage of global markets and business opportunities not even imaginable today, opening up a new world of economic possibility and progress."



- Vice President Al Gore, Jr., July 1997, A Framework for Global Electronic Commerce

1998 – "The Good Ol' Days"

No Face book

Phones

Wired

VCRs

No Ipods or IPad

No USB Sticks

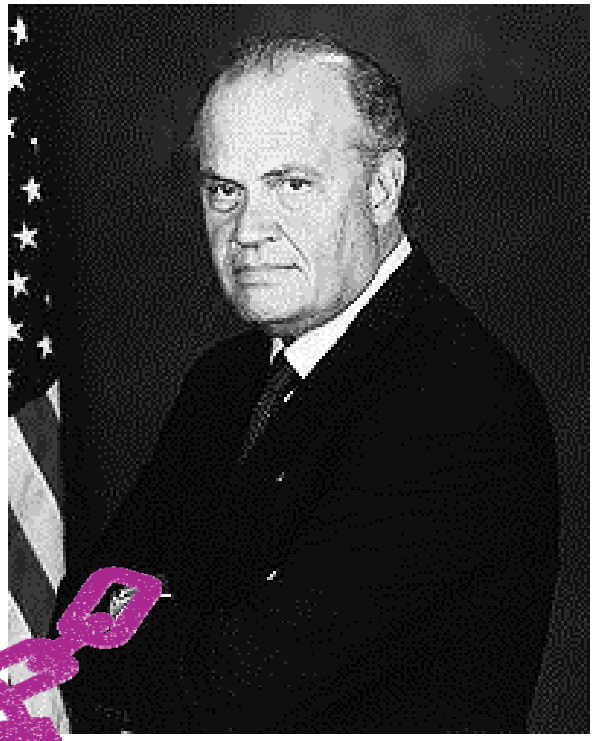
Blockbuster

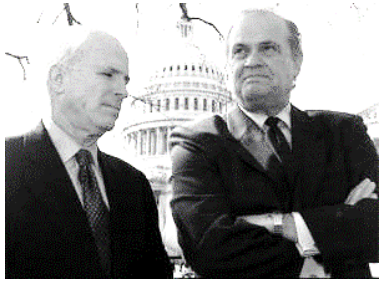
50 inch flat screen $9K

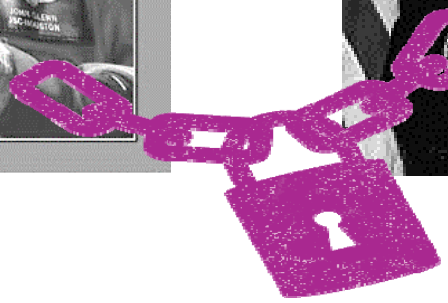
Y2k

Paper Maps

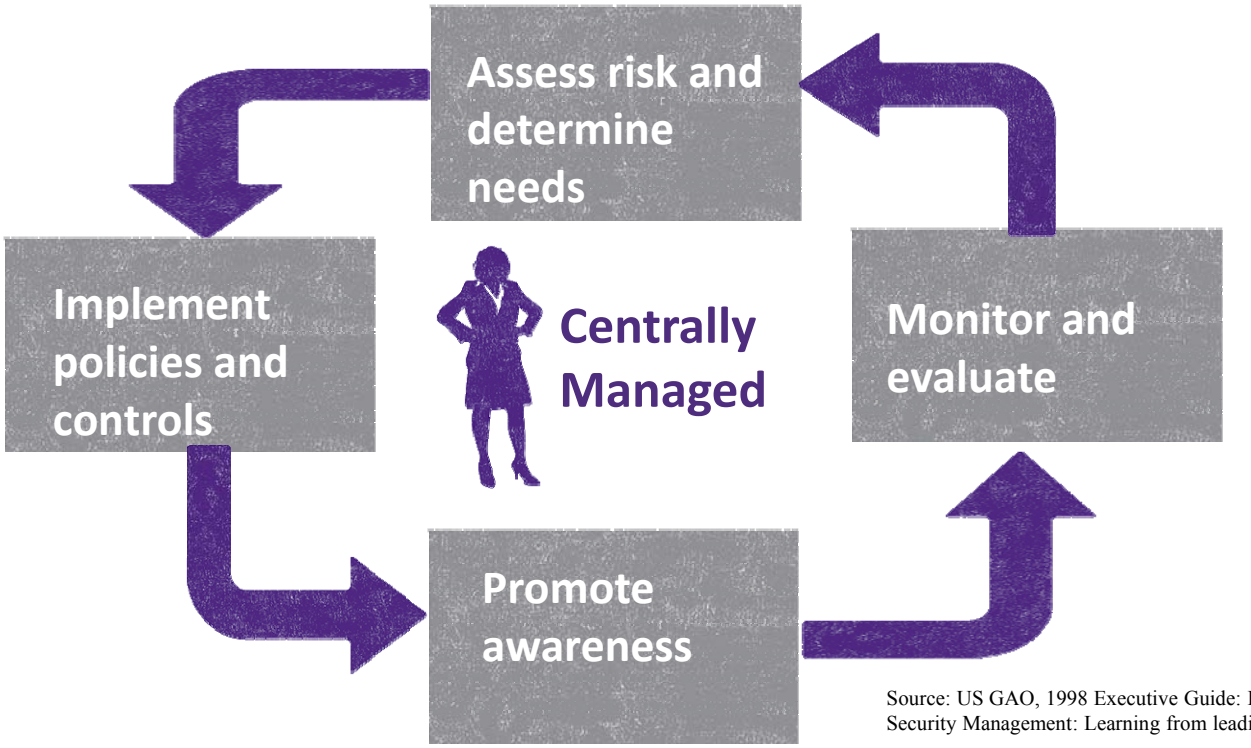
Circa 1997-1998, There These Two Men….







…Resulting in Security Leadership In Leading Organizations- 1998 Style



Source: US GAO, 1998 Executive Guide: Information Security Management: Learning from leading organizations

The Evolution of The Chief Information Security Officer (CISO) Role Pre-2000 to Present

Dimension	Pre-2000	2000-2003	2004-2008	2008-2016
Technology	Firewalls Anti-Virus	GRC Tools	Identity Management	Social Media Ipads/Tablets File sharing Virtualization
Organization	Data Center	Committee	CISO in IT	CISO outside IT
Laws/Regs	EU Directive	HIPAA, GLBA, PCI, FISMA	NIST Regs, ISO27001:05	Privacy Law Focus
Media Incidents	Infrequent	Breach Notification	Few companies, big attention	Many companies, large ones noticed
Security Issue	Technology	Technology Compliance	Risk	Vendor Consumer

Grant Thornton
An instinct for growth™

RSAConference2016

#RSAC

2016-2020 Information Security

WHAT WOULD WE PUT IN THESE BOXES IN 2016?

Assess risk and determine needs

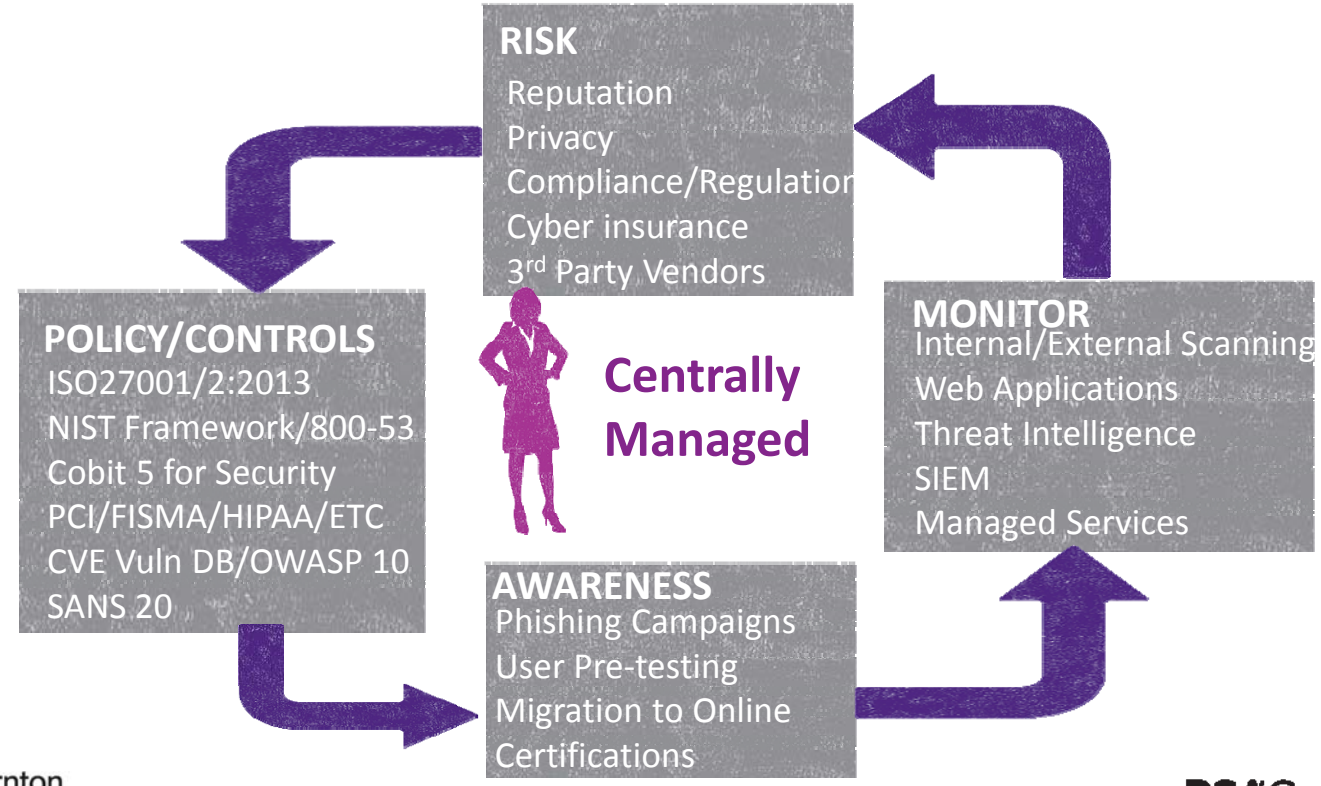
Implement policies and controls

Promote awareness

Monitor and evaluate

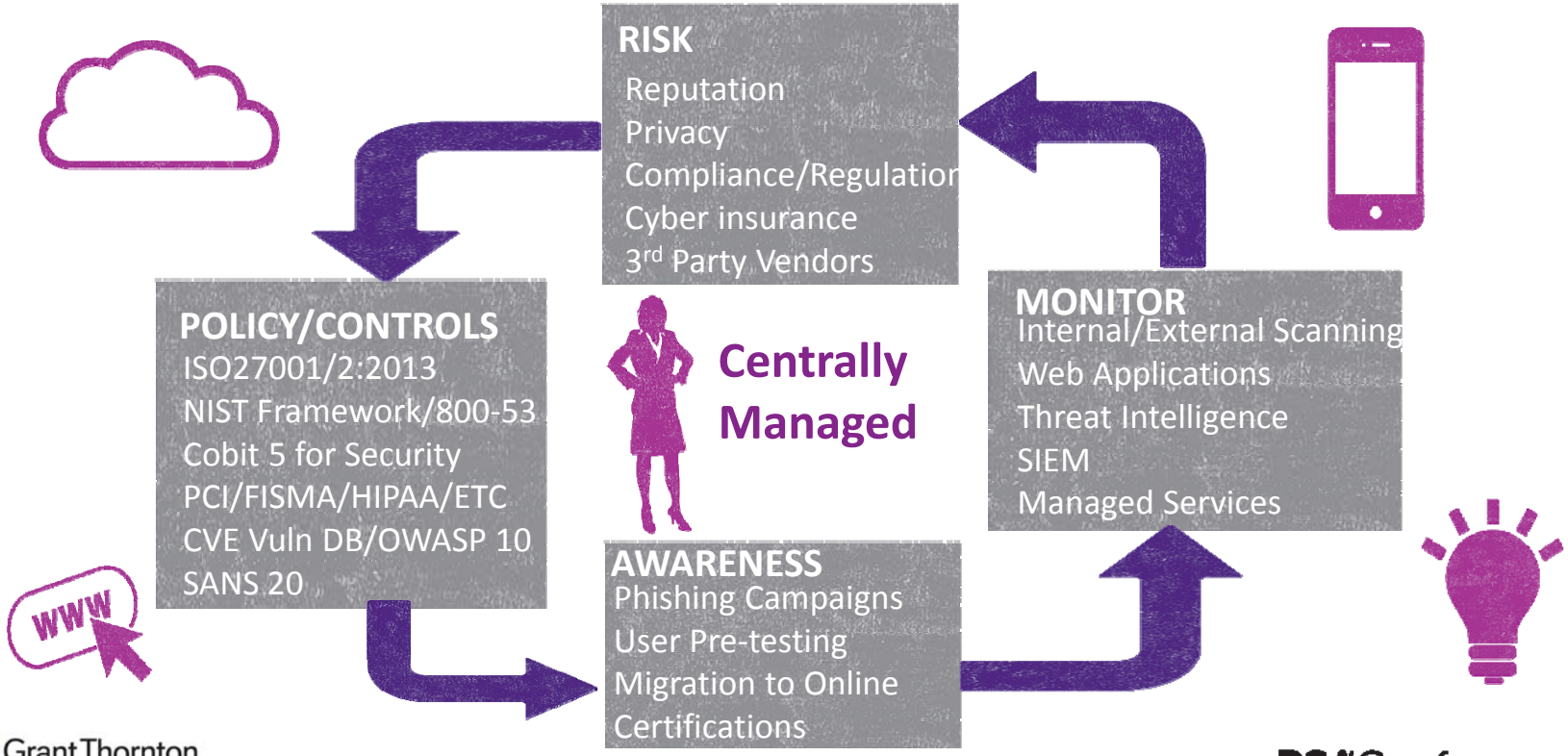
Grant Thornton
An instinct for growth™

Security Leadership In Leading Organizations- 2016 Style



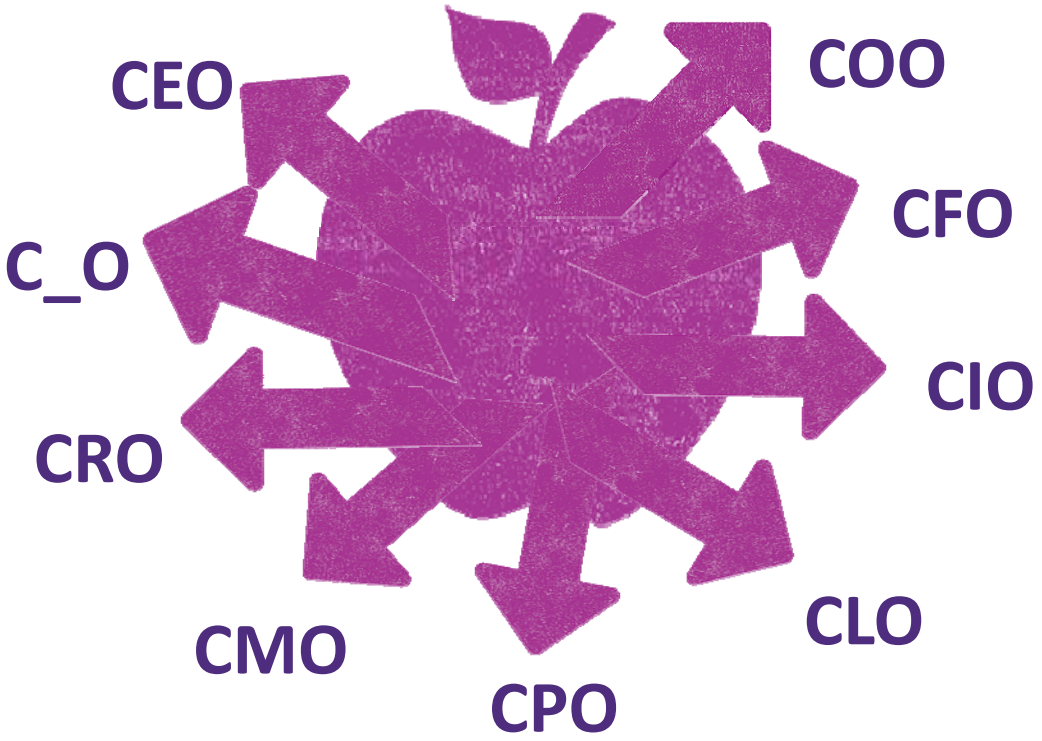
Grant Thornton
An instinct for growth™

Security Leadership In Leading Organizations- 2016 Style



Grant Thornton
An instinct for growth™

The 2016-2020 CISO Will Need to Balance The Needs of Multiple C-Level Stakeholders



Grant Thornton
An instinct for growth™

RSAConference2016

The "Security Language" May Not Be Easily Understood By The C-Suite and Board

Information Security Governance Benefits

Increase in share value for good governance

Increased predictability of business operations

Protection from civil or legal liability as a result of absence of due care

Critical decisions not based on faulty information

To Whom Should The CISO Report?

GENERAL COUNSEL

- Compliance focused
- Legal Expertise Access
- Lack of technical understanding
- Underestimation of costs

CEO

- Lack of time for security
- Raises visibility of security
- May provide aid short-term
- Too many details for CEO

RISK OFFICER

- Risk advocate
- Security may not get attention
- Clout with senior management
- Lack of business metrics

PHYSICAL SECURITY

- Guns Guards vs IT culture
  Increased incident comms
- "Police Mentality"
- Law enforcement connections

Oh, yeah… we missed the CIO !!

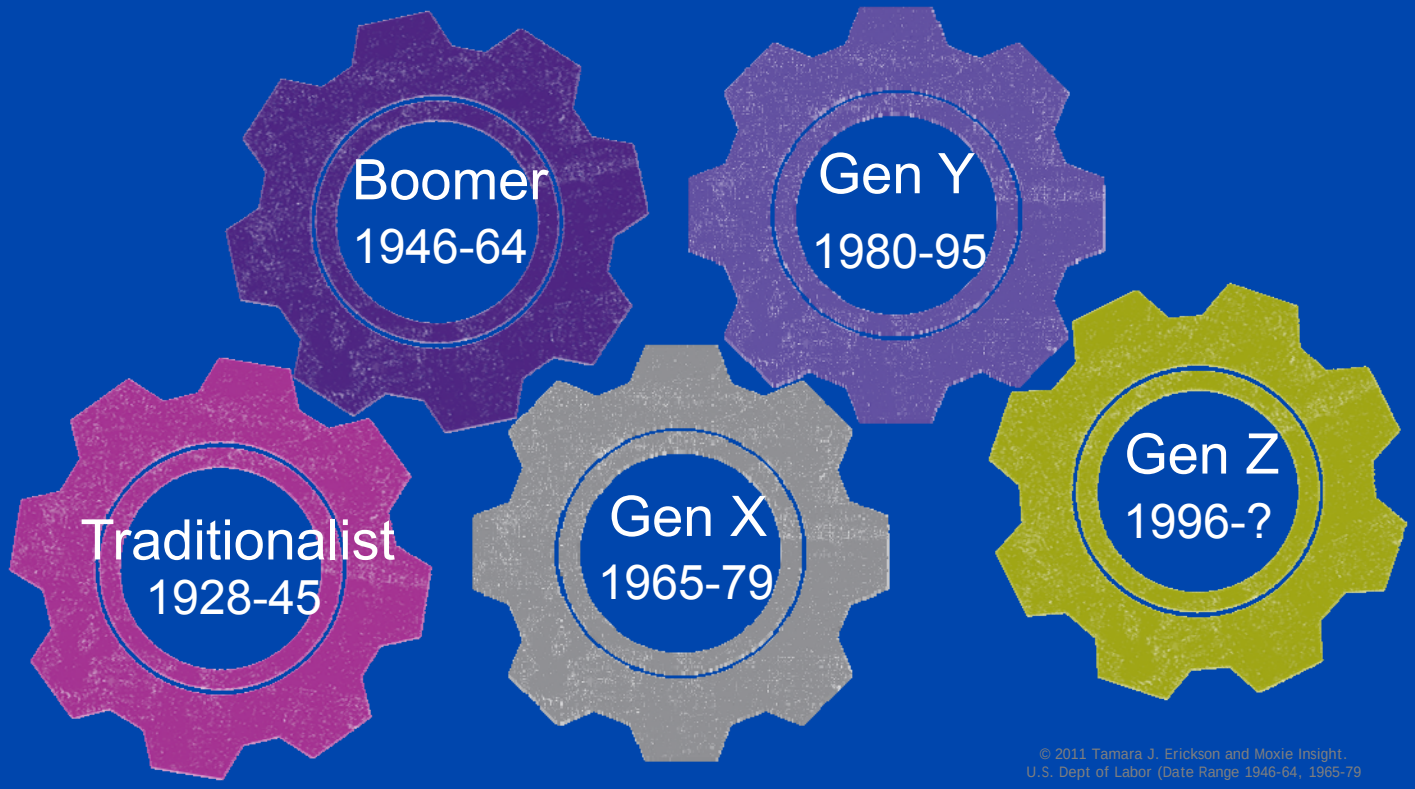
(Where 56% of CISOs report today…)

Source: CISO's Today: The good. bad and the ugly, CISO Summit, Larry Ponemon Dec 2013

+++ Reporting to Various Oversight Committees

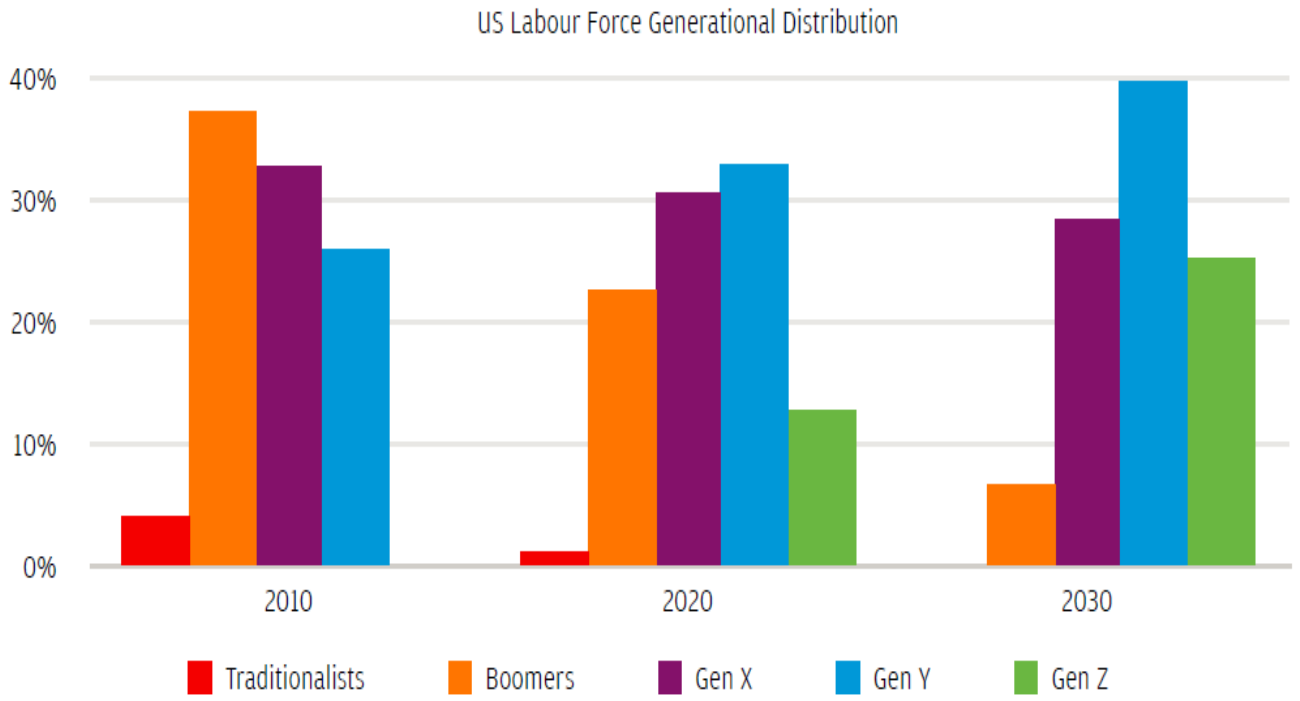
- LEGAL
- RISK
- COMPLIANCE
- HUMAN RESOURCES
- FINANCE
- PHYSICAL SECURITY/FACILITIES
- BUSINESS UNITS
- MARKETING
- INFORMATION TECHNOLOGY

Each generation approaches work differently, shaped by the economic, social and political forces of their time ultimately forming their individual preferences.



U.S. Dept of Labor (Date Range 1946-64, 1965-79

The Workforce is Changing Dramatically



Source: Hot Spots Movement, 2011- The Future of Work

Grant Thornton
An instinct for growth™

CISOs Must Be Aware of Changes In the Way We Work

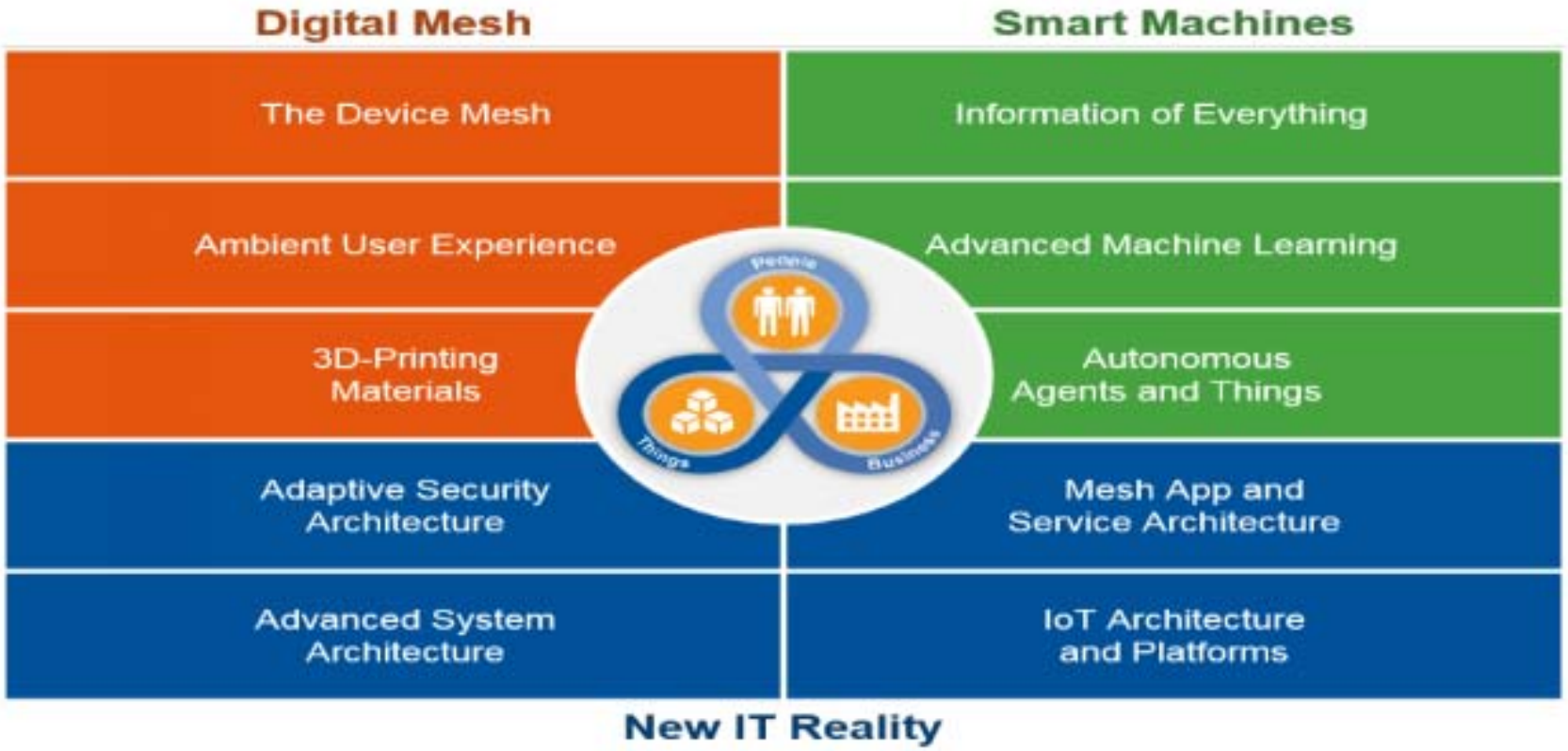
	Security Policy/Trend Influenced
	**Logon Id/Password** – Smartphone, biometric, near-field communication
	**Secure File Sharing** – Off premise working, cloud storage, large file collaboration
	**BYOD/BYOC/BYO?-** Want latest tech, recruiting tool

…and Also the "Behavioral" Trends

	Security Policy/Trend Influenced
	**Cloud Applications**– Risks need to be communicated, many will 'just try it'
	**Security Careers**– Multiple career paths, must be challenging, socially responsible, flexible
	**Awareness Training –**Interactive, bit-sized, game-based, relevant learning
	**Social Media** – Company information leaks, need to communicate regularly, value of privacy

Enterprise Security's Overlooked Factor: The End User's Age, T.Fitzgerald, Darkreading.com, Oct 2013

CISO Needs To Know What Is Coming: 2016 Top 10 Strategic Technology Trends (Gartner)



Top 2016 Information Security Trends

1. Unintended consequences of State Intervention
2. Big Data will lead to big problems
3. Mobile applications and IoT
4. Cybercrime causes perfect threat storm
5. Skills gaps becomes an abyss for information security

Source: CIO Magazine, ISF Forum, December 2015

The security officer is increasingly dealing with privacy concerns beyond the 'privacy principles'

Inconsistent application

Lack of global trust

Data Governance/location

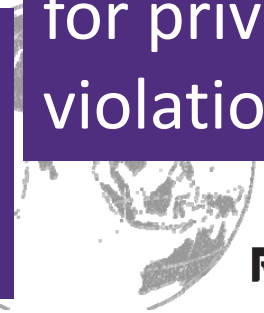
Controller/Processor responsibilities

Location tracking

Location of data

Retention, record correction, right to be forgotten

Regulatory fines for privacy notice violation



Grant Thornton
An instinct for growth™

The CISO 2016-2020… The 2018 CISO Evolution

Leadership
Strategic Thinking
Business Knowledge
Risk Management
Communication
Relationship Management
Security Expertise
Technical Expertise

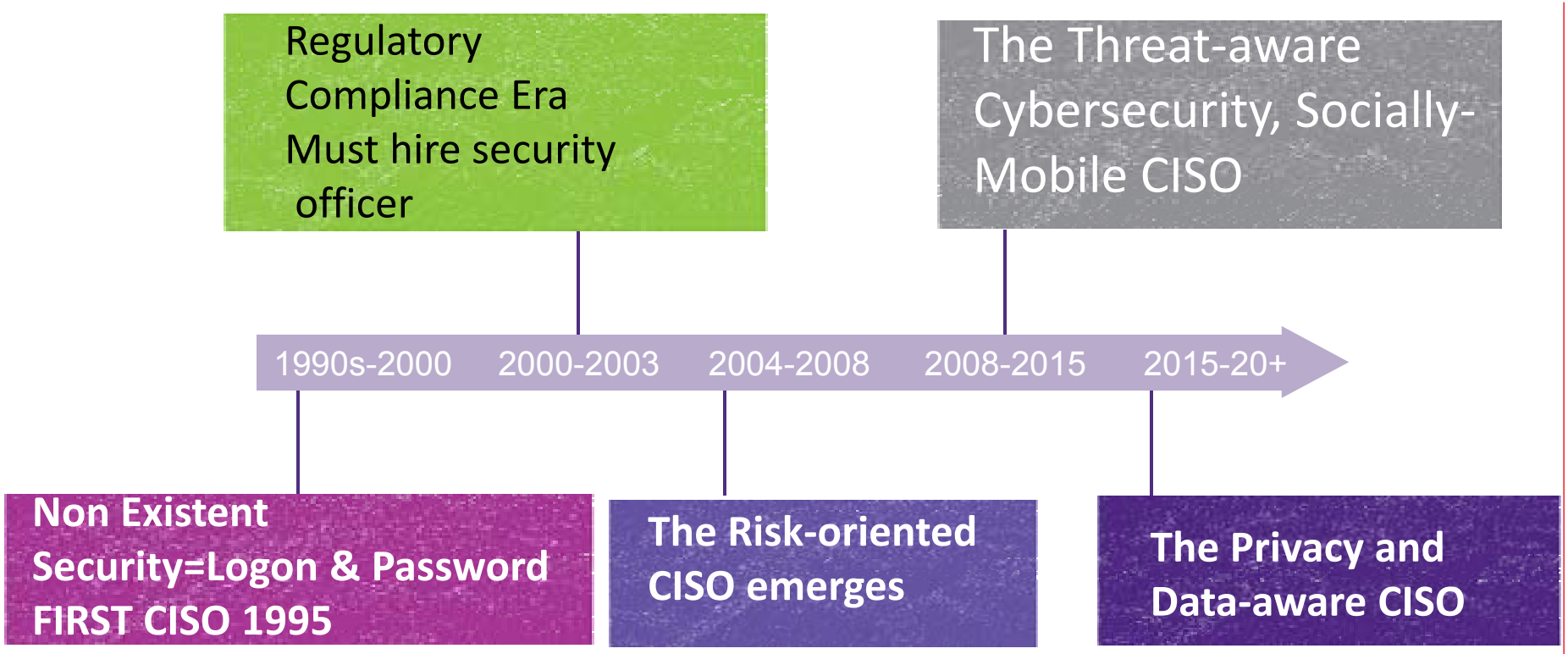
- Plan path away from operations
- Refine **risk management** processes to **business language**
- Widen vision to privacy, data management and compliance
- Build support network
- Create focus and **attention of business leaders**

Grant Thornton
An instinct for growth™

Source: Forrester Research: Evolve to become 2018 CISO or Face Extinction

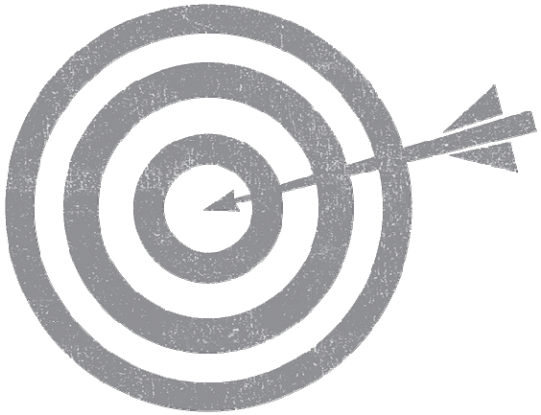
Grant Thornton
An instinct for growth™

The 25 year CISO Profession Evolution 1995-2020



Are You Prepared for 2020 ? Let's Take a Test…

- ☑ Security Risk Management
- ☑ Global Privacy Knowledge
- ☑ Managed Security Services/Remote Teams
- ☑ Boardroom Acumen/Building Strategies
- ☑ Threat Intelligence/Analytics
- ☑ Data Governance
- ☑ Knowing how IOT, Mobile, Social, Cloud, 3D printing fits *your* business



Grant Thornton
An instinct for growth™

Final Thoughts

… A sign on a taxicab credit card device…

Do You have a Disclaimer on Your Security Program ?

Will it prevent the CISO Pink slip Process ?

One Security Officer's Prediction (Mine!) for the CISO of 2020

1. Must have a 2-3 year roadmap tied to new business opportunities/technologies
2. Incidents expected, controlled response expected
3. Controls compliance with control framework expected – pick one and go, all industry-mapped
4. Reports outside of IT, 'IT security' resides under infrastructure group
5. SIEM, threat intelligence performed by cloud-providers
6. More CISOs sourced from the business
7. Focus on risk, where the data is and knows country-specific privacy laws

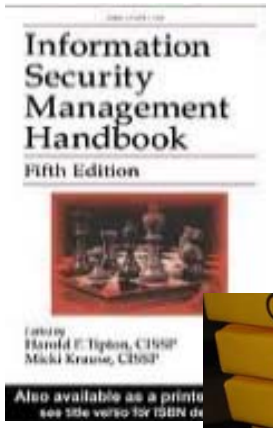
Apply What You Have Learned Today

- Next week you should:
  - Identify stakeholders with whom you have a limited relationship
- In the first three months following this presentation you should:
  - Build stronger relationships with legal, risk, IT, compliance, HR, marketing, etc.
  - Identify the emerging trends impacting your company/industry
  - Pursue a certification of at least one new skill area each year
- Within six months you should:
  - Complete independent study/training/certification in a leadership, business, risk, or privacy area
  - Draft a 2016-2020 security plan for the organization

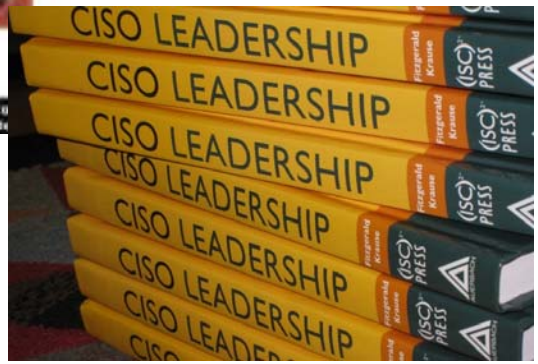
Today We Explored…

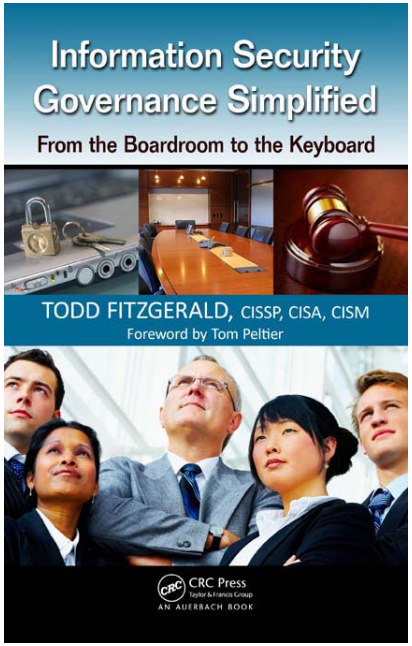
- The breadth of the CISO Job
- What makes a "Leading Information Security Program"
- The historical view of the CISO leader
- Trends impacting 2016-2020 Information Security
- Soft skill areas, relationships, technologies, approaches to be successful

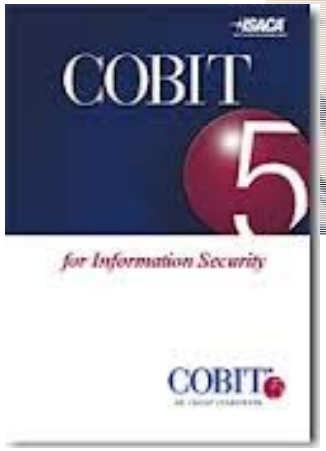
Resources Contributed To By Presenter (Books Available in RSA Bookstore)



Information Security Handbook Series Since 2004



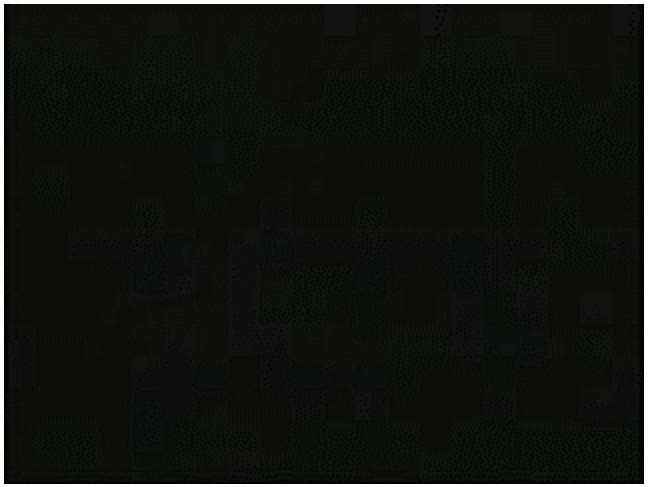




CSX CYBERSECURITY NEXUS

Grant Thornton
An instinct for growth™

I Leave You With This Final 60 Second View of Your Next Few Years as a CISO…



Thank You For Your Participation!

Grant Thornton
An instinct for growth™
Top 50 World's Most Attractive Employers

Winner 2015
International Accounting Bulletin
Winner
Employer of the year 2015

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

Todd_fitzgerald@yahoo.com

linkedin.com/in/toddfitzgerald