## RSA\*Conference2016

San Francisco | February 29 – March 4 | Moscone Center



Connect **to** Protect

SESSION ID: PRV-T10

## **Privacy Primer for Security Officers**

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

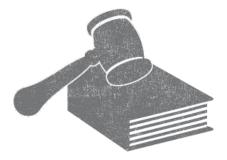


### Disclaimer



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" refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. [Member firm name'] is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's ages or emissions.



## **We Face Privacy Choices Daily**









## 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, quidelines 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 Technique V. Computer Science, Management Information Systems or similar curriculum • 7+ years of Information Technology or Inf dedicated to Information Security • 2+ years of Travel Industry experience preferred • Must be a Certifical normation 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



## **Contains Many Privacy References!**



#### 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 •





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 PTIVaCY

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 SAS-70 audit requirements a plus • Knowledge of SAS-70 audit requirements and concepts a plus • Knowledge of SA

9001 requirements a plus • Knowledge of ISO 27001 requirements a plus • Knowledge of ISO 27001 requirements a plus • Knowledge of COBIT requirements a plus • Knowledge of EU / Safe

#### • 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



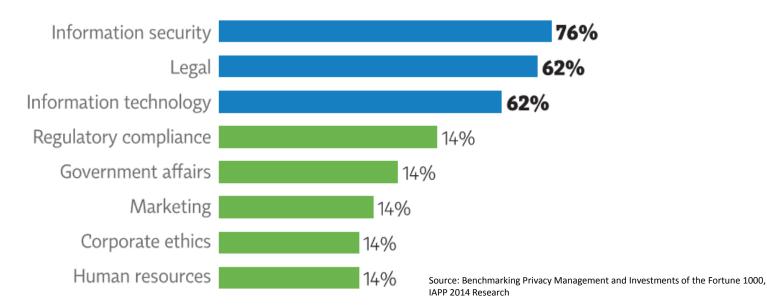
RS&Conference2016

## The Fortune 1000 Is Investing in Privacy and Values Relationships To Information Security



## Other Functions Seen as "Very Important" for Privacy Collaboration: Top Mentions

n=28





### 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



Build support network

 Create focus and attention of business leaders



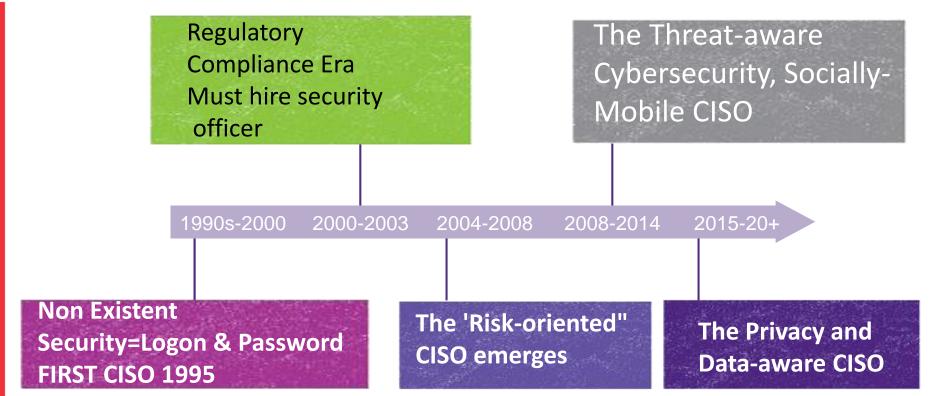


Source: Forrester Research: Evolve to become 2018 CISO or Face Extinction



## The New CISO will Need to Know Privacy







# 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 of data

Retention, record correction, right to be forgotten

Location tracking

Regulatory fines for privacy notice violation



RS∧Conference2016

#### PRIVACY IS DEAD... OR IS IT?



Privacy Is Dead, Harvard Professors Tell Davos Forum

- January 22, 2015

Why Privacy Is Actually Thriving Online

- Wired, May 2014

**Privacy Is Dead: What You Still Can Do to Protect Yourself** 

- Huffington Post, 08/27/15

Privacy Is Dead, Says M. Zuckerberg, Even for his Unborn Daughter

Privacy Is Completely And Utterly Dead, And We Killed It

- Forbes, 8/19/14

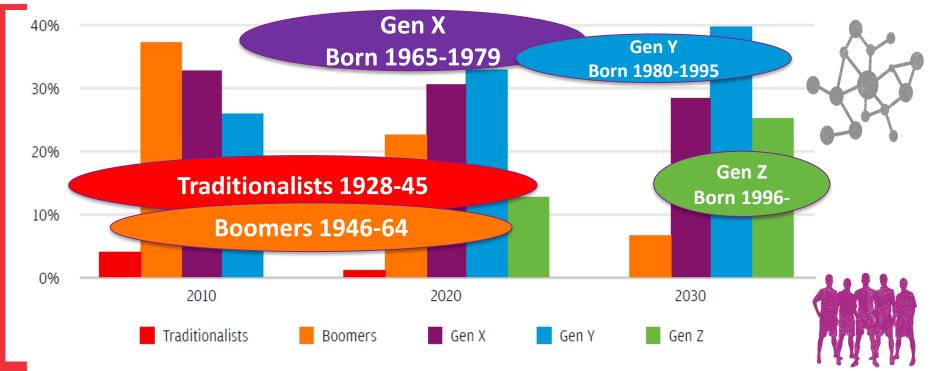


Grant Thornton

An instinct for growth

## **Privacy Concern Differs By Generation**





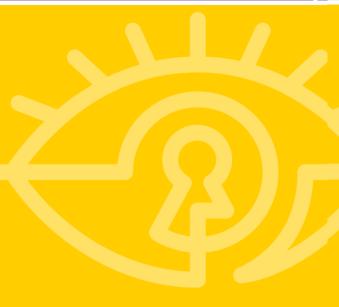




## RSAConference2016



**Privacy Laws and Common Principles** 



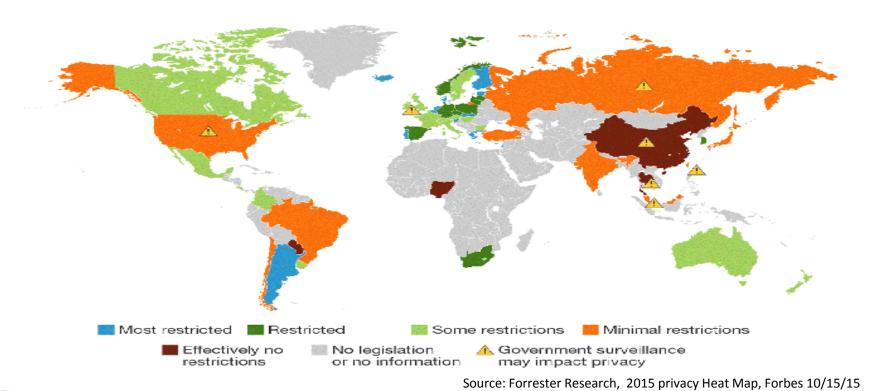
## **Early Privacy Laws and Regulations**



<b>63</b>	Year	Milestone
Warren  Brandeis	1890	"The Right to Privacy" Warren and Brandeis
	1947	Article 12 of Universal Declaration of Human Rights
	1966	US Freedom of Information Act
	1970	Fair Credit Reporting Act
	1974	US Privacy Act
	1978	France Data Protection Act
	1980	Organization for Economic Cooperation and Development (OECD)
	1981	Council of Europe Convention on the Protection of Personal Data

## **Privacy Coverage Varies Across Countries**







## **Current Privacy Laws**



## Sectoral Laws (US) PIPEDA (Canada)



Fair Credit Reporting Act HIPAA/HITECH/State laws Gramm-Leach-Bliley Act Children's Online Privacy Protection Act (COPPA) 1974 Privacy Act /FOIA

### Comprehensive (EU)



1995 EU Data Protection
Directive
e-Privacy Directive
Data retention directive
Article 29 working party



### Co-Regulatory (AU)

Australia Federal Privacy Act (amended in 2000) China- No comprehensive policy Hong Kong- 1996 Personal Data Ordinance



## 2016 Emerging EU/US Privacy Laws



General Data Protection Regulation

- Regulation vs Directive
- Reach beyond EU
- Fines 4% revenue
- 72 hour data
   breach notification

EU/US Privacy Shield

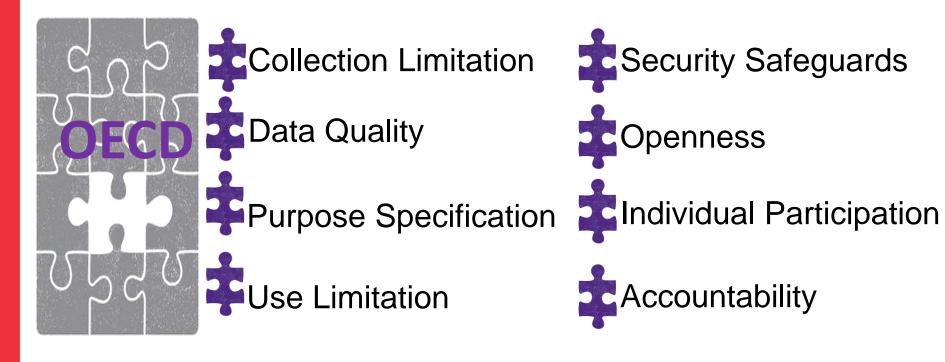
- Strongobligations forUS Companies
- Government accesstransparency
- Redress





# Organization for Economic Co-operation and Development (OECD) Privacy Principles







## **OECD- 1. Collection Limitation Principle**



There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.







## **OECD- 2. Data Quality Principle**



Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.





## **OECD- 3. Purpose Specification Principle**



■ The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Why am I Getting All This SPAM Now?





## **OECD- 4. Use Limitation Principle**



Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9

- except:
  - a) with the consent of the data subject; or
  - b) by the authority of law.





## **OECD- 5. Security Safeguards Principle**



Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.



## **OECD- 6. Openness Principle**



■ There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.



## **OECD-** 7. Individual Participation Principle



Right to obtain confirmation DATA STORED

REASONABLE MANNER, COST and FORM

Ability to challenge denials

REASONABLE TIME If denied, be provided a reason

Right to erase, rectify complete, or amend information



## **OECD-8. Accountability Principle**



A data controller should be accountable for complying with measures which give effect to the principles stated above.





## **RS**∧°Conference2016







### **EU Defines Personal Data**



- "Personal data shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."
- Sensitive Personal Data or 'special categories of personal data' are generally prohibited from processing (some exemptions).
- **De-Identified (non-personal) data** laws generally do not apply after identifying elements removed.

### **Personal Information Elements**





Name

Gender

Age

DOB

Marital Status

Citizenship

Nationality

Languages Spoken

**Veteran Status** 

Disabled Status

**IP Address** 

Demographics

### **Sources of Personal Information**



#### **Public Records**

- Real estate
- Criminal
- VariesState/National/Local level

#### **Publicly Available**

- Names and addresses
- Newspapers
- Search engines
- Facebook/Twitter



#### Nonpublic

- Medical records
- Financial information
- Adoption Records
- Company customers
- Employee database



### **Sensitive Personal Information**



# EUROPE UNITED STATES

- Racial or Ethic Origin
- Political opinion
- Religious or philosophical beliefs
- Trade-union membership
- Health or sex life
- Offenses or criminal convictions

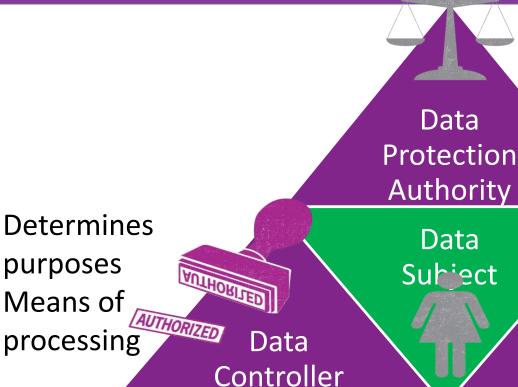
- Social Security Number
- Financial Information
- Driver's License Number
- Medical Records





### **Data Protection Roles**





- Enforcement
  - Reporting

• Processes on behalf of data controller

Data Processor





## **Privacy Policy and Notice**





### **PRIVACY NOTICE**

- Initially, periodically
- Clear and conspicuous
- Accurate and complete
- Readable, plain language

- Privacy Policy Internal statement directing employees
- Privacy Notice- statement to data subject for collection, use, retention and disclosure of information
- Contracts, application forms, web pages, terms of use, Icons, signs, brochures

## **Privacy Consent**





## **OPT-OUT**

- Processed unless data subject objects
- Box pre-checked to accept or check box to opt-out

## **OPT-IN**

- Information processed only if data subject agrees
- Active affirmation

#### **OPT-IN or OPT-OUT?**



- A. DO YOU WANT TO RECEIVE ADDITIONAL INFORMATION?

  ☑ YES □ NO
- B. 

  CHECK BOX IF YOU DO NOT WANT TO RECEIVE MORE INFORMATION
- C. DO YOU WANT TO RECEIVE ADDITIONAL INFORMATION?
  - ☐ YES ☐ NO
- D. 

  PLEASE SEND MORE INFORMATION ABOUT YOUR PRODUCTS



## **RS**∧°Conference2016







## **Privacy Information Life Cycle**



#### Collection

#### Use

#### Retention

#### Disclosure

- Limits
- Lawful and fair means
- Consent
- Identified purpose
- Proportionate

- Purposes identified in notice
- Implicit or explicit consent
- Retain only as long as necessary for purpose
- Securely dispose, destroy, return
- Rights maintained on transfer of data
- New purposes subject to consent

Grant Thornton

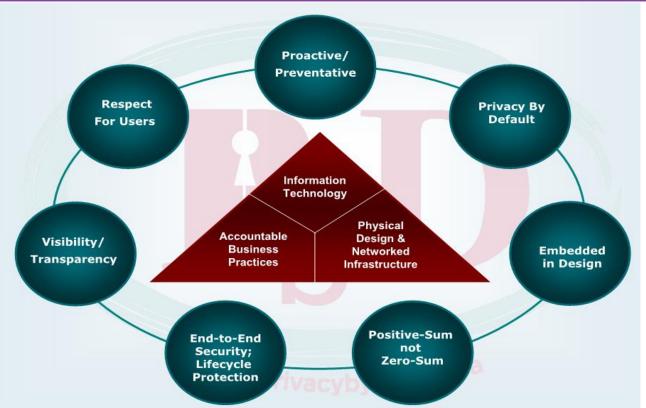
An instinct for growth

RS∧Conference2016

### **Privacy By Design – 7 Principles**



Originated by
Information
and Privacy
Commissioner
of Ontario,
Canada in
mid-1990's



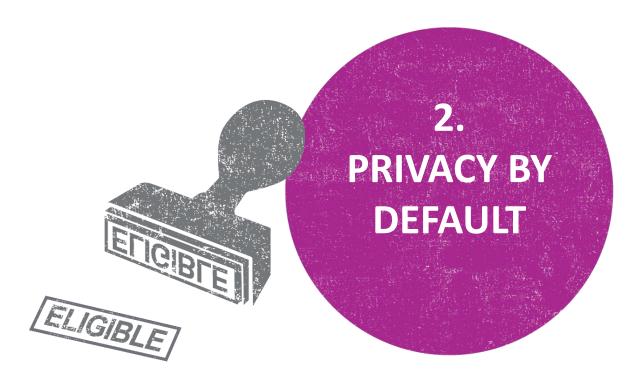






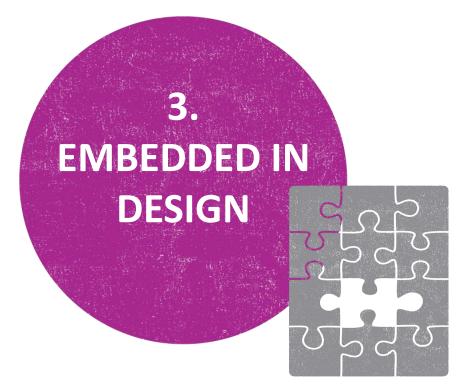


































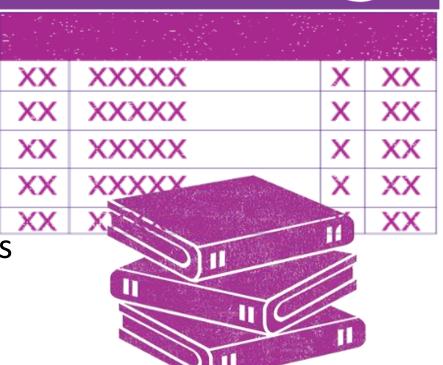




## **Privacy Impact Assessment (PIA)**



- Checklists to ensure systems evaluated for privacy risks
- New systems
- Changes to existing systems
- Legal/Regulatory requirements
- Policy/Practice consistency





# RSA Conference 2016

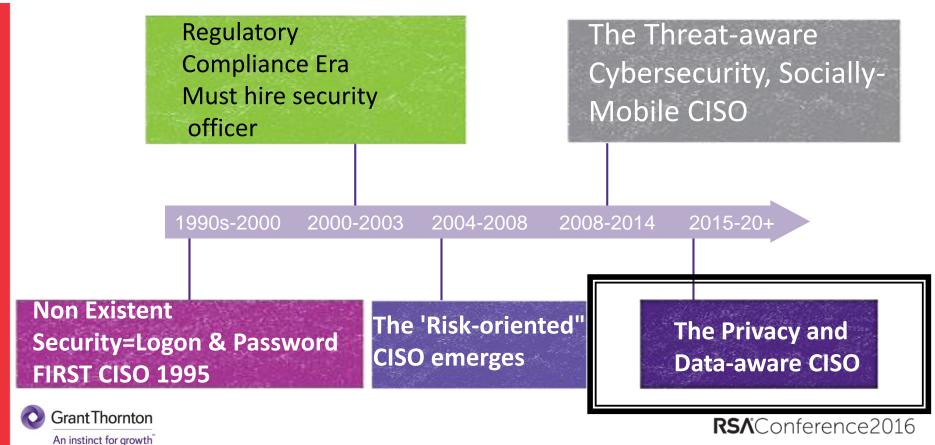




**Final Thoughts** 

### Data+Privacy+Security+Risk= New Focus





### **Apply What You Have Learned Today**



- Next week you should:
  - Schedule a meet n greet with the privacy officer or legal dept.
- In the first three months following this presentation you should:
  - Read the EU Data Protection Directive and any local laws
  - Visit the International Association of Privacy Professionals (IAPP) website at www.privacyassociation.org
  - Examine your organization's privacy policies
- Within six months you should:
  - Go forward with a privacy certification
  - Drive an assessment project (with the privacy officer) to determine where the privacy gaps are
  - Begin educating the workforce on privacy principles through regional meetings

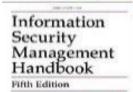
#### **Today We Explored...**



- Why Privacy should be Important to the security officer
- 8 information OECD Privacy Principles
- Global laws impacting privacy
- Building a program through Privacy By Design Principles
- Understanding the data elements and language of privacy

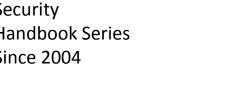
## **Resources Contributed To By Presenter** (Books In RSA Bookstore)

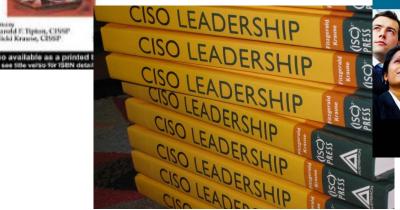




Harold F. Tipton, CISSP Micki Krause, CISSP

Information Security Handbook Series Since 2004





Information Security Governance Simplified

From the Boardroom to the Keyboard



Foreword by Tom Peltier









**EC-Council Certified** 

CCCC Sury of Encylphysia



### Thank You For Your Participation!









Winner Employer of the year 2015



**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

