

RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: DSP-T08

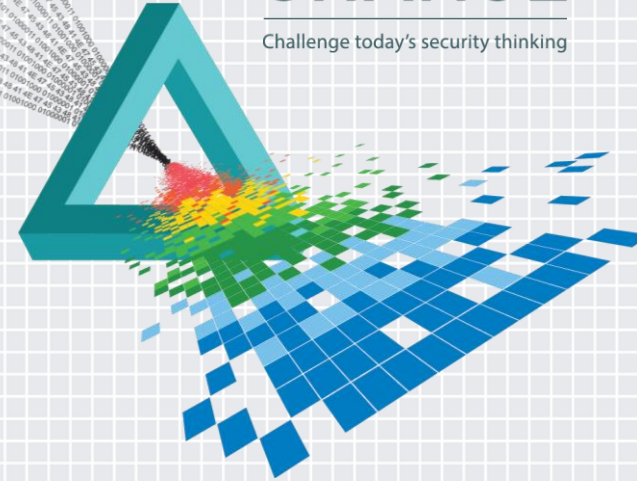
A Privacy Primer for Security Officers

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

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

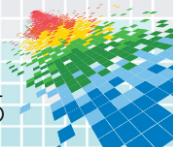
CHANGE

Challenge today's security thinking



For Our Time Together Today...

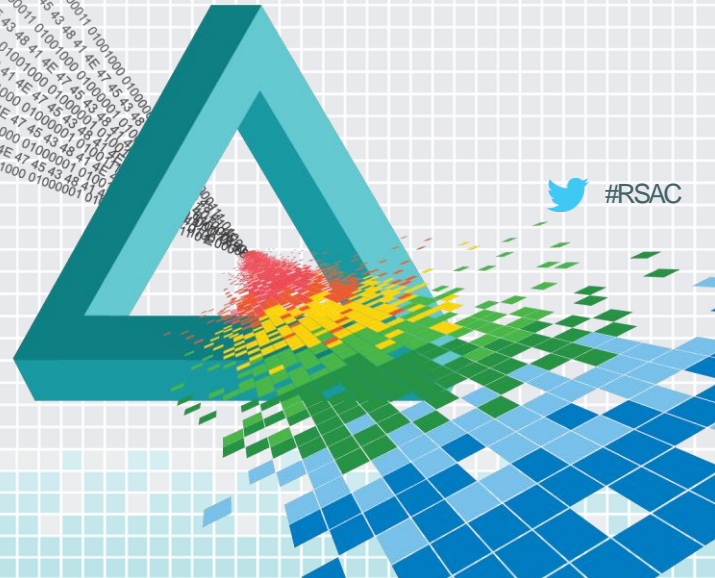
- ◆ Examine the CISO Privacy Landscape
- ◆ Review Privacy Laws and 8 Common Principles
- ◆ Present the Language of Privacy
- ◆ Final Thoughts



RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

The CISO Privacy Landscape

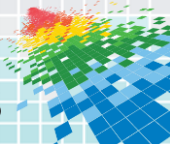


The CISO Job Description

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:

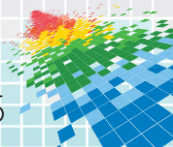
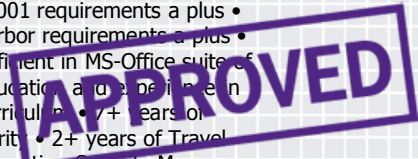
- Manage a cost-effective information security program for the Americas region; aligned with the global information security program, business goals and objectives
- Assist with RFP and Information Security responses for clients
- Implementing and maintaining documentation, policies, procedures, guidelines 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



...PAGE TWO!

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



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,

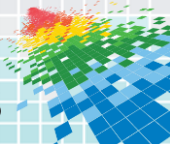
European Union

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 • **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 TWO!



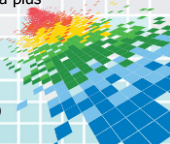
Direct senior security personnel in order to achieve the security initiatives • Participate in the information security steering and advisory committees to address organization-wide issues involving information security matters and concerns, establish objectives and set priorities for the information 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

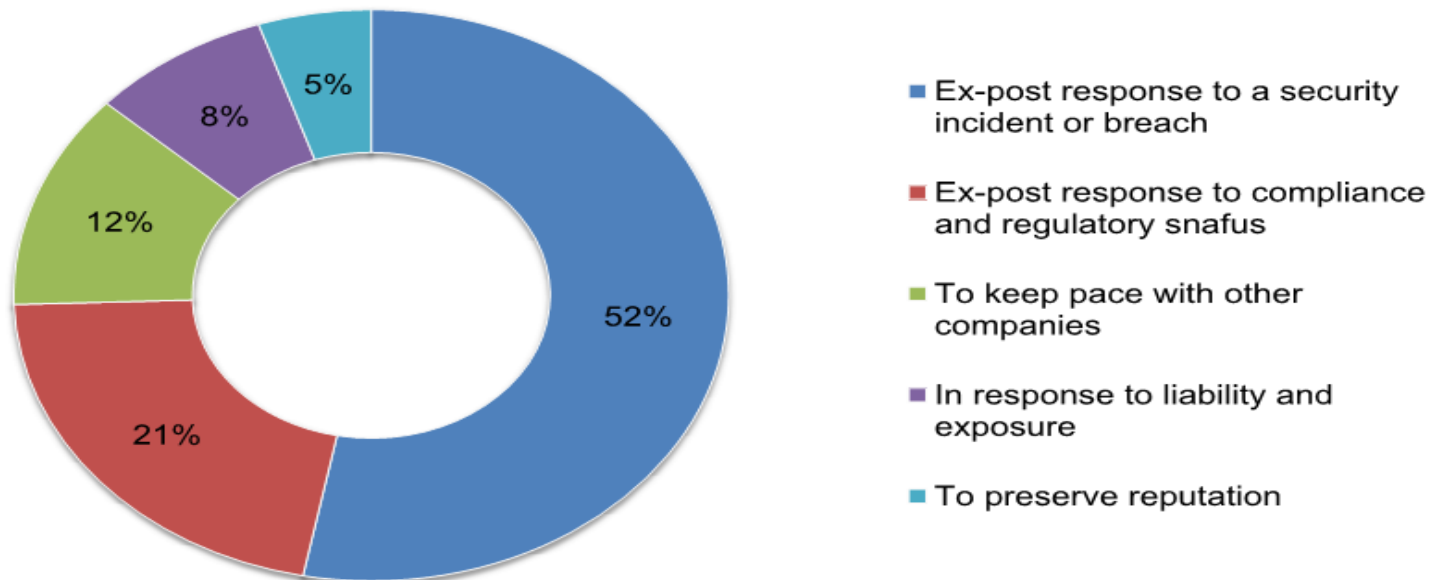
XP/2000/2003, Active Directory, and IT Infrastructure security and recovery methods and concepts • Working knowledge of Web-based application security and recovery methods and concepts • Working knowledge of AS400 security and recovery methods and concepts • Working knowledge of PeopleSoft security and 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 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

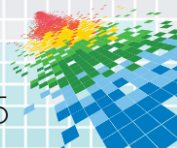


Why Are Organizations Employing Security Officers (CISOs) ?

Study of companies with 1,000 or more employees



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



The CISO 2015-2020... The 2018 CISO Evolution

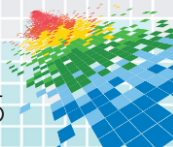
- Leadership
- Strategic Thinking
- Business Knowledge
- Risk Management
- Communication
- Relationship Management
- Security Expertise
- Technical Expertise



- 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



Source: Forrester Research: Evolve to become 2018 CISO or Face Extinction 9/6/13



The New CISO will Need to Know Privacy

Regulatory
Compliance Era
Must hire security
officer

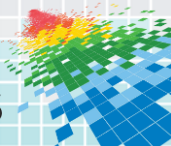
The Threat-aware
Cybersecurity, Socially-
Mobile CISO



Non Existent
Security=Logon & Password
FIRST CISO 1995

The 'Risk-oriented"
CISO emerges

The Privacy and
Data-aware CISO



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



Lack of global trust

Inconsistent application

Data Governance/location

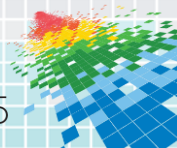
Controller/Processor responsibilities

Location of data

Regulatory fines for privacy notice violation

Location tracking

Retention, record correction, right to be forgotten

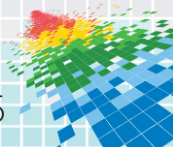


PRIVACY IS DEAD... OR IS IT ?

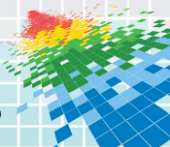
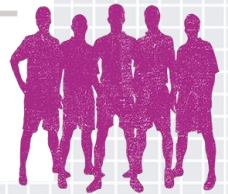
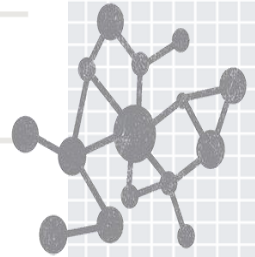
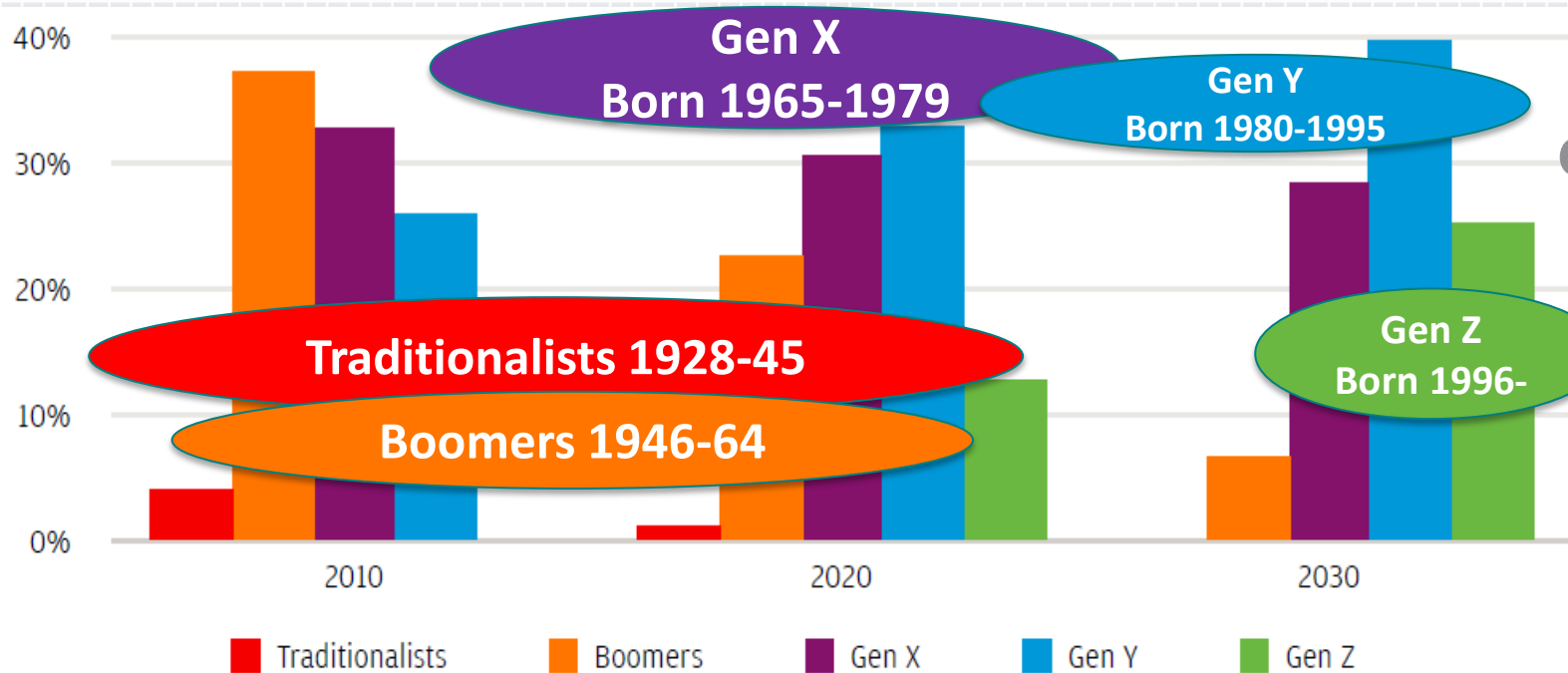
Privacy Is Dead, Harvard Professors Tell Davos Forum
- January 22, 2015

Why Privacy Is Actually Thriving Online
- Wired, May 2014

Privacy Is Completely And Utterly Dead, And We Killed It
- Forbes, August 19, 2014



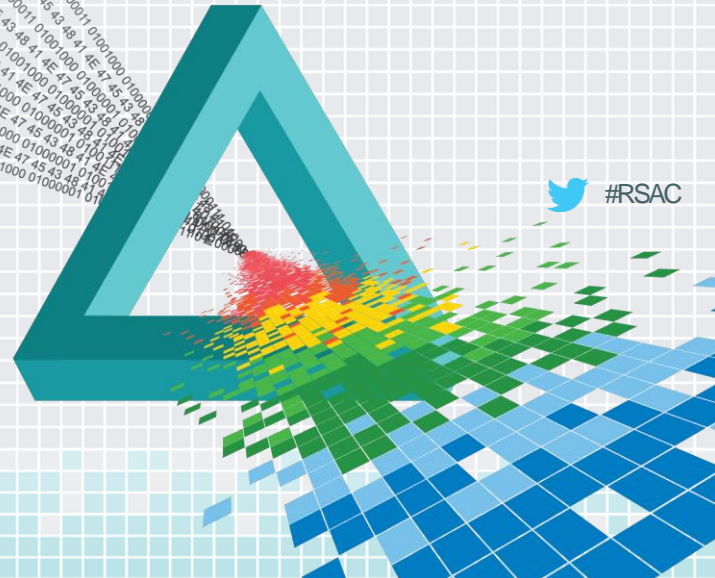
Privacy Concern Differs By Generation



RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

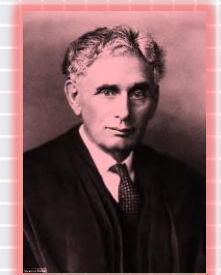
Privacy Laws and Common Principles



Early Privacy Laws and Regulations

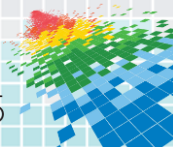


Warren



Brandeis

Year	Milestone
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



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)

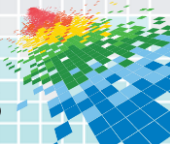


1995 EU Data Protection
Directive
e-Privacy Directive
Data retention directive
Article 29 working party

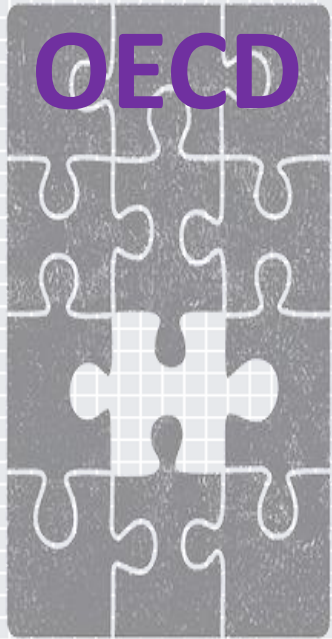


Co-Regulatory (AU)

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



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




 Collection Limitation


 Data Quality

 Purpose Specification

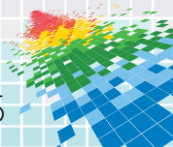
 Use Limitation

 Security Safeguards

 Openness

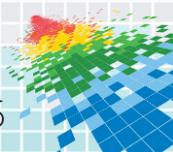
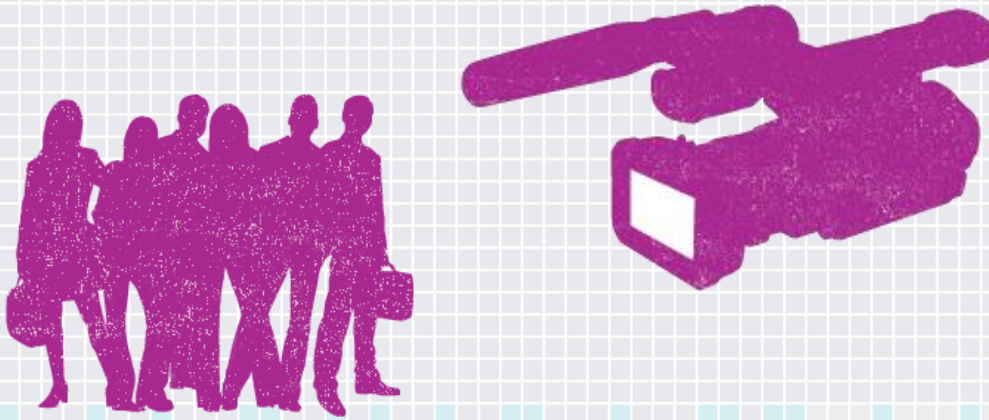
 Individual Participation

 Accountability



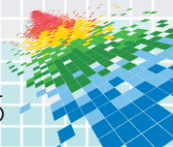
OECD- 1. Collection Limitation Principle

- ◆ 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.



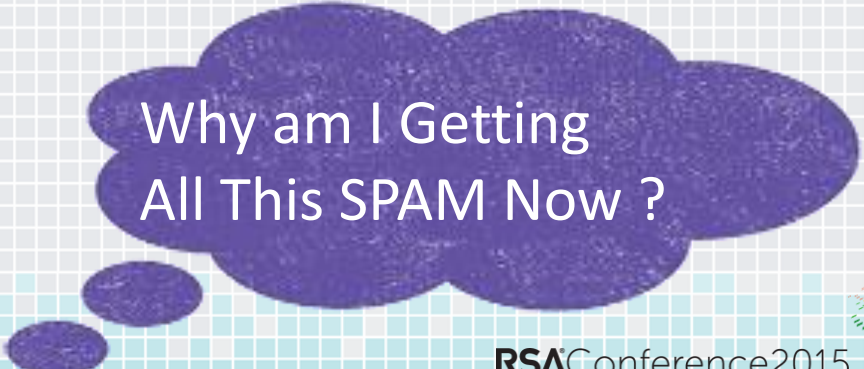
OECD- 2. Data Quality Principle

- ◆ 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

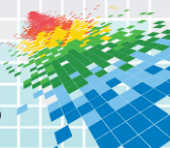
- ◆ The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.



Why am I Getting
All This SPAM Now ?

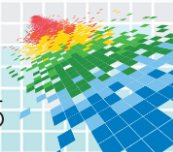
OECD- 4. Use Limitation Principle

- ◆ 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.



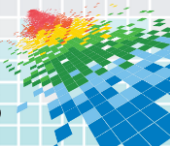
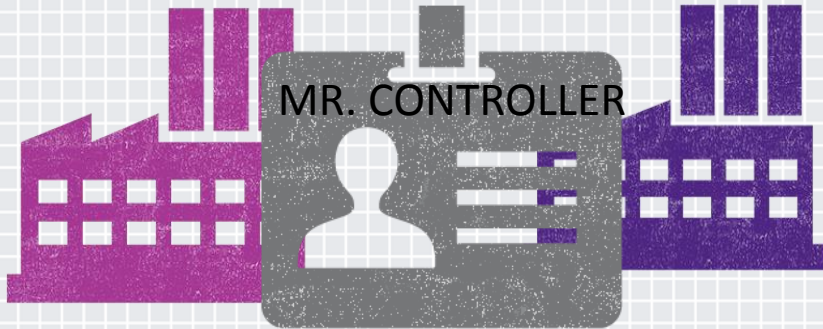
OECD- 5. Security Safeguards Principle

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



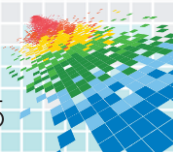
OECD- 6. Openness Principle

- ◆ 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

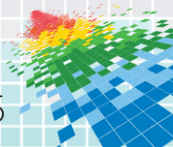
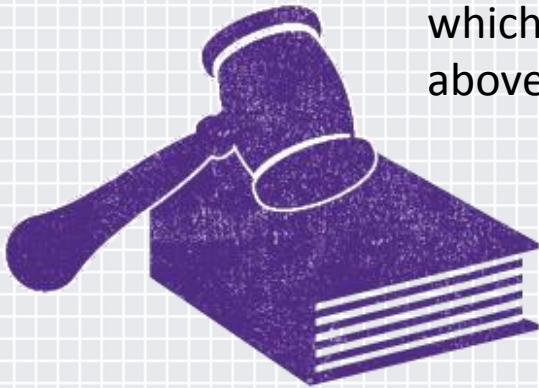
- ◆ Individuals should have the right:
 - ◆ a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;
 - ◆ b) to have communicated to them, data relating to them
 - i. within a reasonable time;
 - ii. at a charge, if any, that is not excessive;
 - iii. in a reasonable manner; and
 - iv. in a form that is readily intelligible to them;
 - ◆ c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
 - ◆ d) to challenge data relating to them and, if the challenge is successful
 - ◆ to have the data erased, rectified, completed or amended.



OECD- 8. Accountability Principle

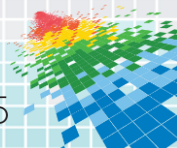
- ◆ A data controller should be accountable for complying with measures which give effect to the principles stated above.

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



EU Defines Personal Data

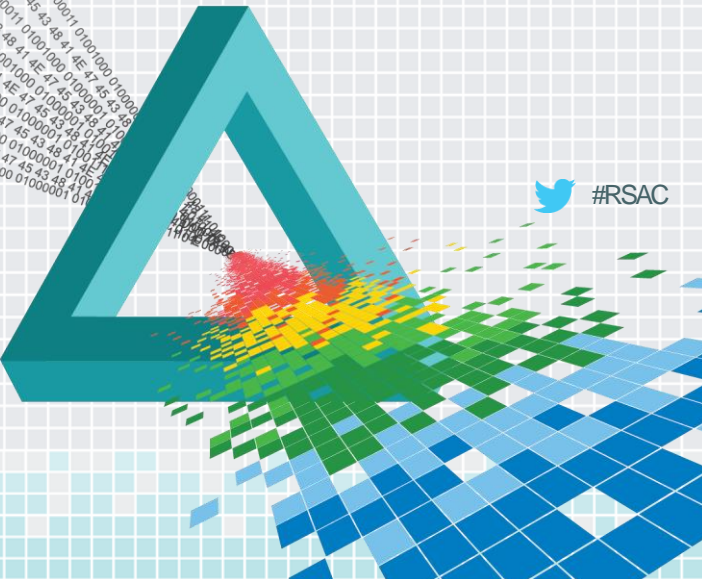
- ◆ "Personal data shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular reference to an identification number or to one or more factors specific to his physical, 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.



RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

The Language of Privacy



Personal Information Elements



Name

Gender

Age

DOB

Marital Status

Citizenship

Nationality

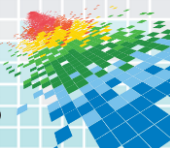
Languages
Spoken

Veteran Status

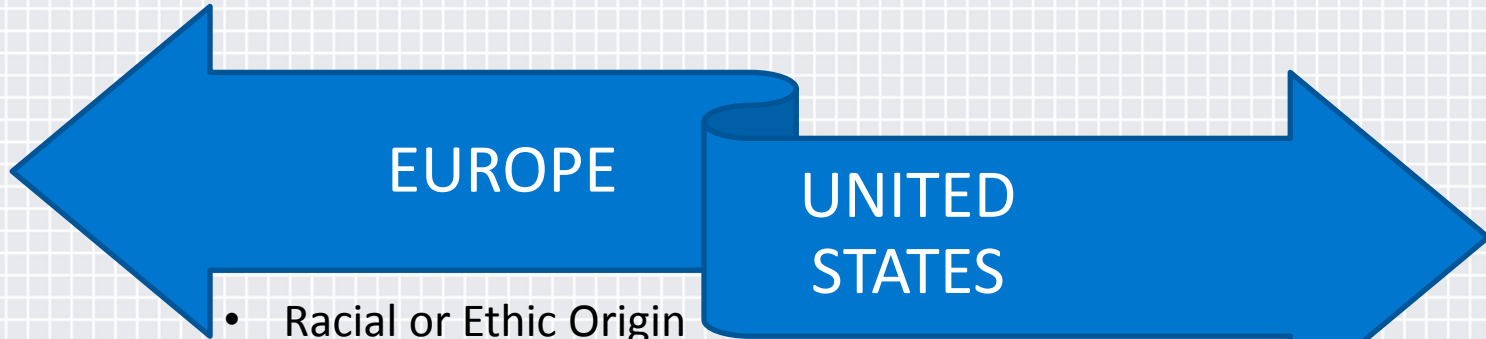
Disabled
Status

IP Address

Demographics

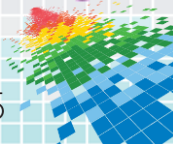
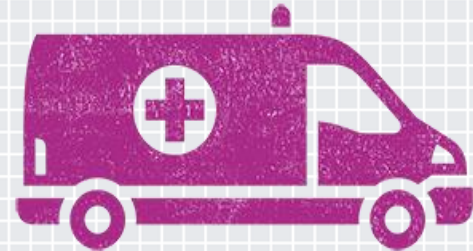


Sensitive Personal Information



- 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



Sources of Personal Information



Public Records

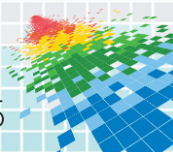
- Real estate
- Criminal
- Varies
State/National/Local
level

Publicly Available

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

Nonpublic

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



Data Protection Roles



Data Protection Authority

- Enforcement
- Reporting

Data Subject

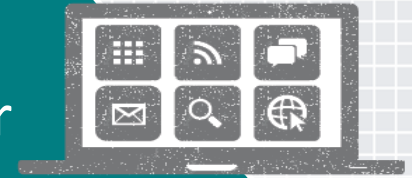


- Processes on behalf of data controller

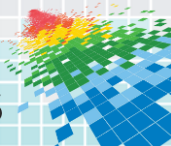


Data Controller

Data Processor



- Determines purposes
- Means of processing



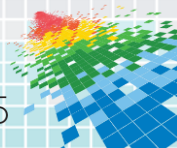
Privacy Policy and Notice



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

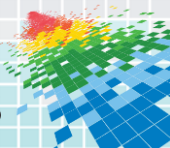


OPT-
OUT

- 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?

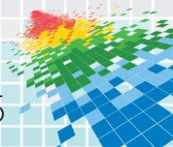
YES NO

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



Privacy Information Life Cycle

Collection

Use

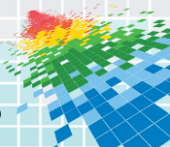
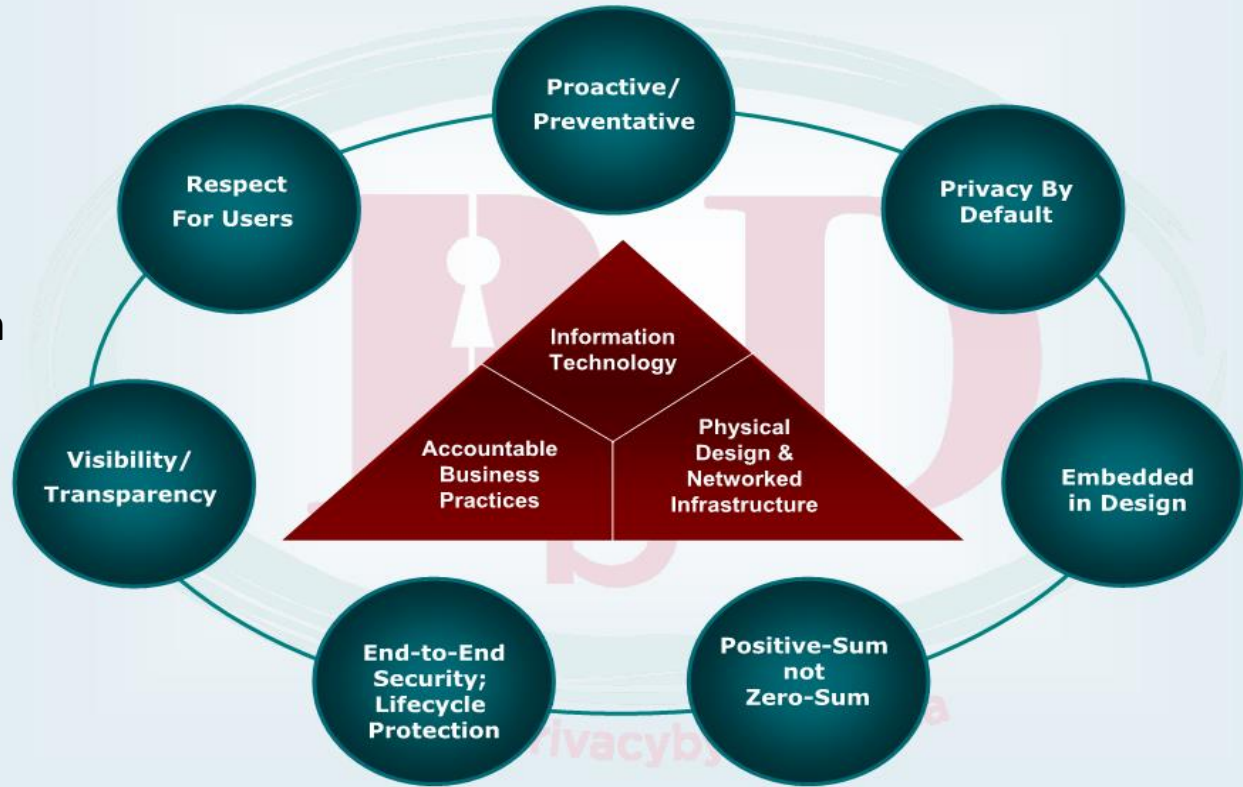
Retention

Disclosure

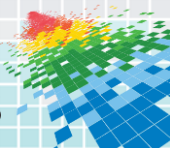
- Limits
 - Lawful and fair means
 - Consent
 - Identified purpose
 - Proportionate
- Purposes identified in notice
 - Implicit or explicit consent
- Retain only as long as necessary for purpose
 - Securely dispose, destroy, return
- Rights maintained on transfer of data
 - New purposes subject to consent

Privacy By Design – 7 Principles

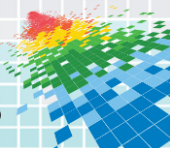
- Originated by Information and Privacy Commissioner of Ontario, Canada in mid-1990's



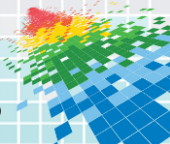
1. PROACTIVE PREVENTATIVE



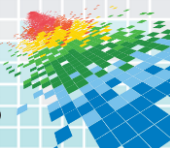
2. PRIVACY BY DEFAULT



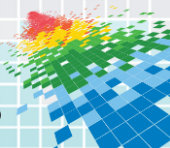
3.
EMBEDDED IN
DESIGN



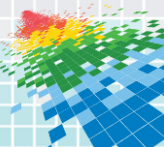
4.
POSITIVE SUM
NOT ZERO-SUM



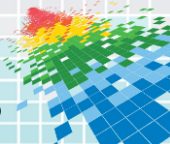
5.
END-TO-END
SECURITY;
LIFECYCLE
PROTECTION



6. VISIBILITY TRANSPARENCY

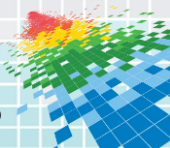


7. RESPECT FOR USERS



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[®]Conference2015

San Francisco | April 20-24 | Moscone Center

Final Thoughts



The New CISO will Need to Know Privacy

Regulatory
Compliance Era
Must hire security
officer

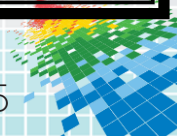
The Threat-aware
Cybersecurity, Socially-
Mobile CISO



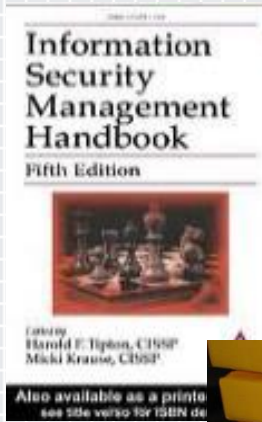
Non Existent
Security=Logon & Password
FIRST CISO 1995

The 'Risk-oriented'
CISO emerges

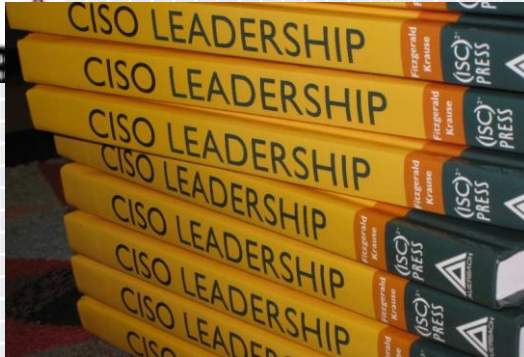
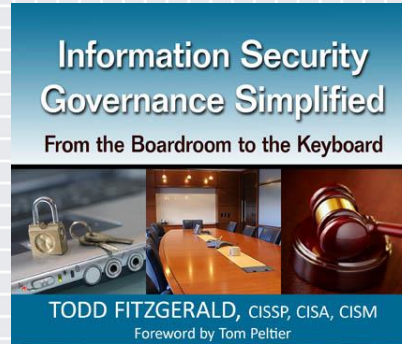
The Privacy and
Data-aware CISO



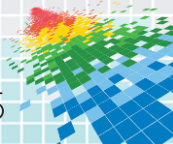
Some Resources Contributed To By Presenter



Information Security Handbook Series (2004-Present) & others



Source: Amazon.Com, Barnes & Noble, ISC2, EC Council, ISACA Websites (2003-2014)



THANKS MUCH FOR YOUR PARTICIPATION!



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

