Privacy vs Data Protection

Eric A. Hibbard, CISSP, CISA
Hitachi Data Systems

Introduction

- The terms “privacy” and “data protection” are often used interchangeable
- In reality they can have very different meanings, depending on the jurisdiction, industry or market sector

2015 Data Storage Innovation Conference. © Hitachi Data Systems. All Rights Reserved.

Personal Information Angle

- Privacy

  The appropriate use of personal information under the circumstances. *What is appropriate will depend on context, law, and the individual's expectations; also, the right of an individual to control the collection, use and disclosure of information.*

  - Source: International Association of Privacy Professionals (IAPP) Glossary

- Data Protection

  The management of personal information. *In the United States, "privacy" is the term that is used in policies, laws and regulation. However, in the European Union and other countries, the term "data protection" often identifies privacy-related laws and regulations.*

  - Source: International Association of Privacy Professionals (IAPP) Glossary

2015 Data Storage Innovation Conference. © Hitachi Data Systems. All Rights Reserved.

Data Protection Alternatives

- Data Protection (Storage)

  Assurance that data is not corrupted, is accessible for authorized purposes only, and is in compliance with applicable requirements.

  - Source: Storage Networking Industry Association Dictionary

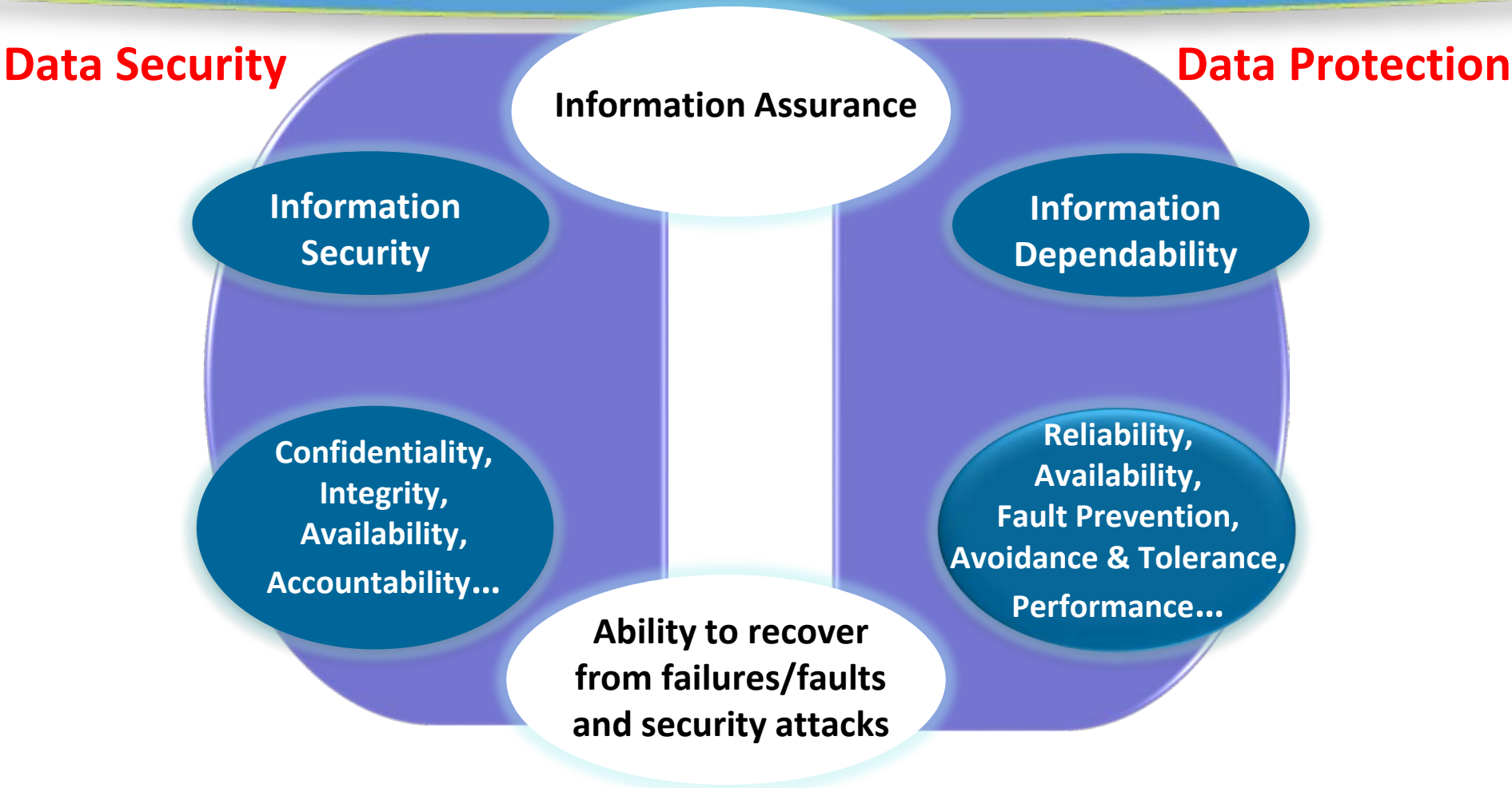
- Data Protection (Security)

  The implementation of appropriate administrative, technical or physical means to guard against unauthorized intentional or accidental disclosure, modification, or destruction of data.

  - Source: ISO/IEC 2382-1:1993

2015 Data Storage Innovation Conference. © Hitachi Data Systems. All Rights Reserved.

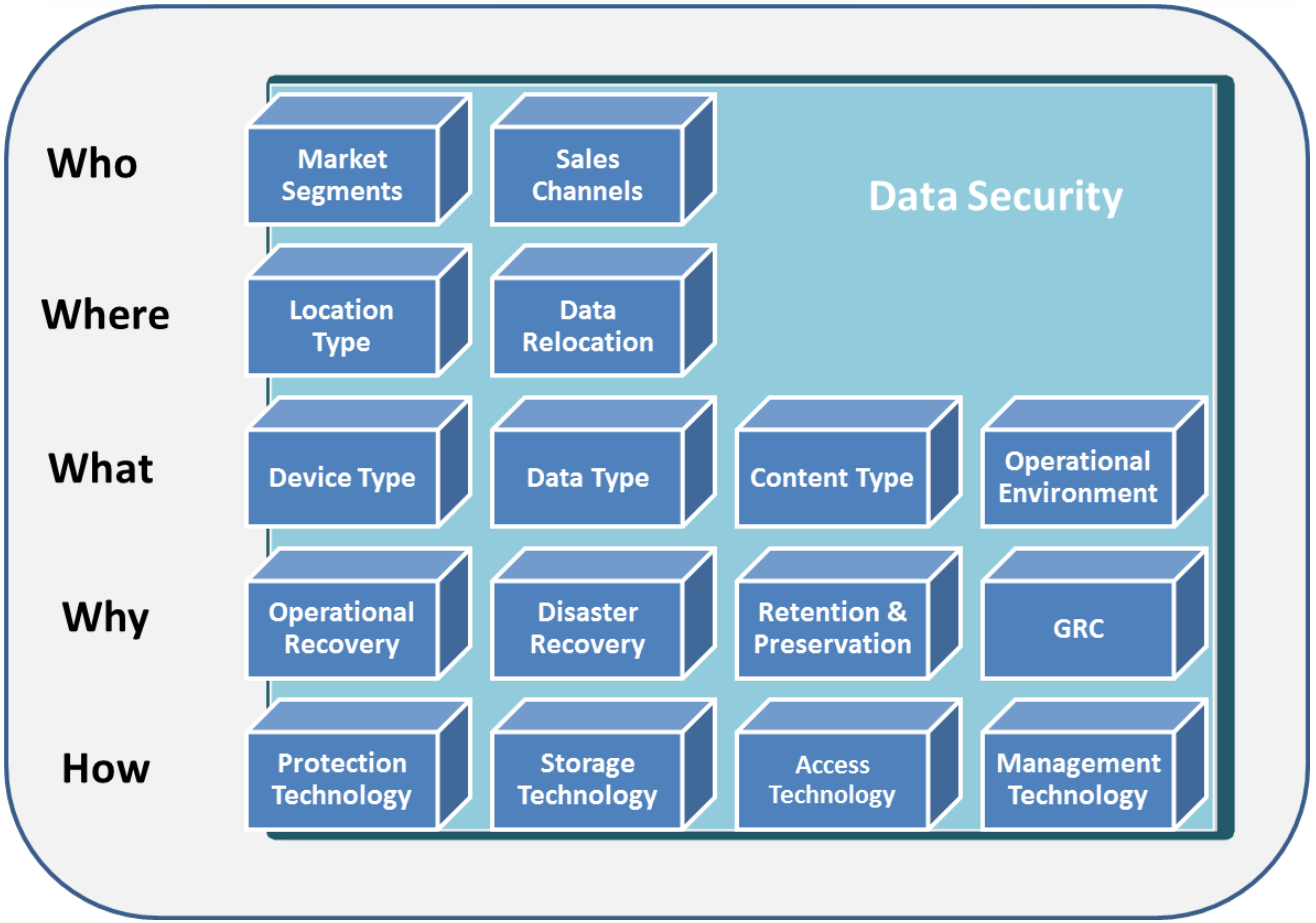
Information Security & Dependability



SOURCE: *Information Assurance – Dependability and Security in Networked Systems*, Qian, Joshi, Tipper, Krishnamurthy, 2008, New York, ISBN: 978-0-12-373566-9.

2015 Data Storage Innovation Conference. © Hitachi Data Systems. All Rights Reserved.

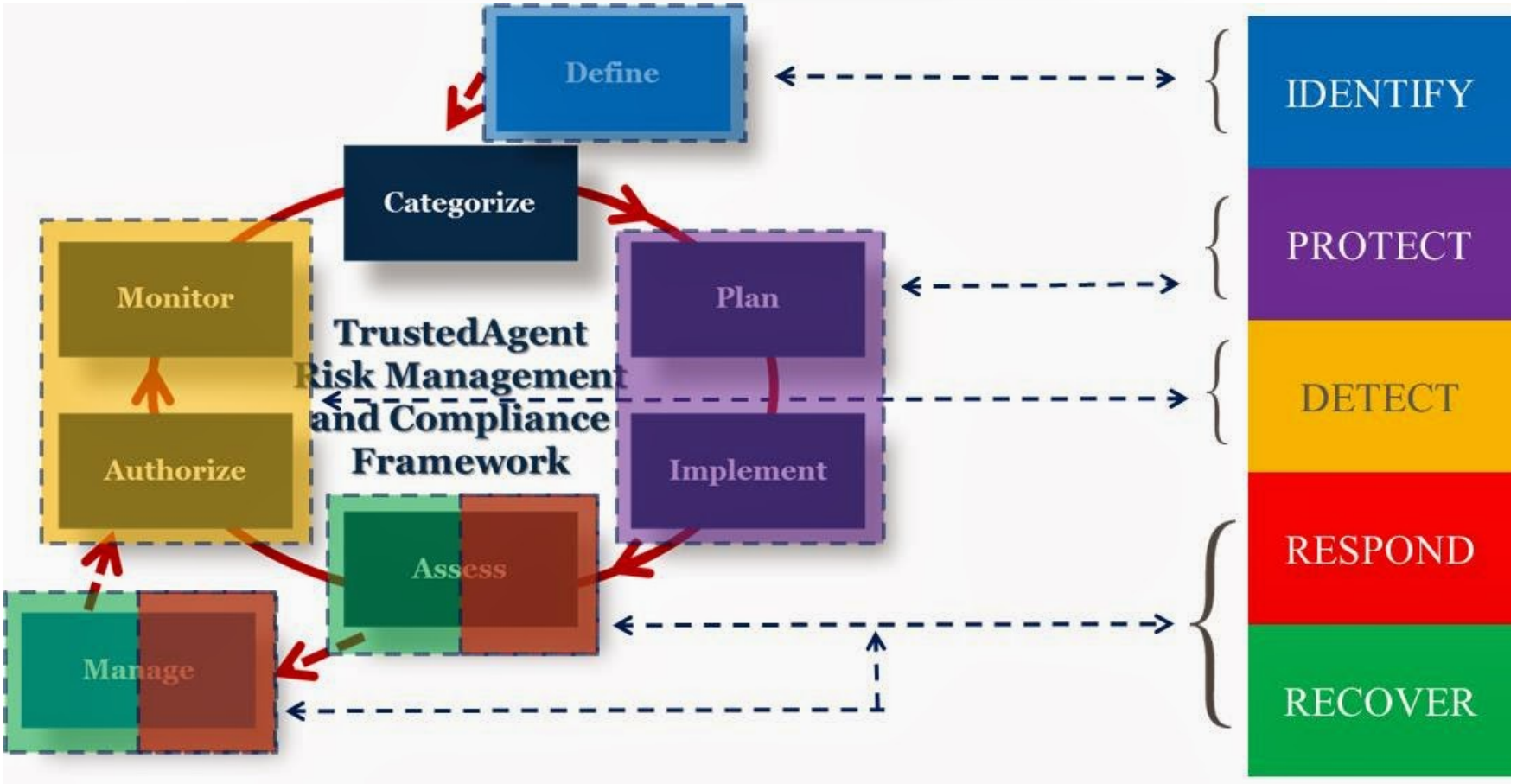
Data Protection – Storage Angle



Source: Based on SNIA DPCO – *A Data Protection Taxonomy* whitepaper (Jun-2010)

2015 Data Storage Innovation Conference. © Hitachi Data Systems. All Rights Reserved.

Data Protection – Security Angle



Source: Based on NIST *Framework for Improving Critical Infrastructure Cybersecurity*, (Feb-2014) and NIST SP 800-53r4 (Apr-2013)

2015 Data Storage Innovation Conference. © Hitachi Data Systems. All Rights Reserved.

What is a Data Breach?

- A ***breach*** is the unauthorized acquisition, access, use, or disclosure of protected health information, which compromises the security or privacy of such information.

  – U.S. HITECH (HIPAA) Act

- A ***personal data breach*** "means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community".

  – EU ePrivacy Directive (EC Proposal)

2015 Data Storage Innovation Conference. © Hitachi Data Systems. All Rights Reserved.

Exploring the Poster-child for Privacy/Data Protection

PROPOSED REFORM OF THE EU DATA PROTECTION DIRECTIVE

2015 Data Storage Innovation Conference. © Hitachi Data Systems. All Rights Reserved.

EU Directive Versus Regulation

- ***Directive***
  - Specific objectives that must be reached and Member States need to adopt national implementation legislation
  - Member States left with the choice of form and method of implementation
  - Language in Directives tend to be more general to allow Member States to adapt into their legislation

- ***Regulation***
  - Directly applicable to all Member States
  - Do not require any additional implementation in national legislation
  - Apply in all Member States in the same wording and scope
  - Law across ***all*** Member States as written

2015 Data Storage Innovation Conference. © Hitachi Data Systems. All Rights Reserved.

New EU Data Protection Regime

- ***Regulation*** (replacing Directive 95/46/EC) "*General Data Protection Regulation (GDPR)*"
  - To set out a general EU framework for data protection
  - Would make limited technical adjustments to the e-Privacy Directive (2002/58/EC)
  - Total of 91 Articles in the Proposed Regulation

- ***Directive*** (replacing Framework Decision 2008/977/JHA)
  - To set out rules on the protection of personal data processed for the purposes of prevention, detention, investigation, or prosecution of criminal offences and related judicial activities

2015 Data Storage Innovation Conference. © Hitachi Data Systems. All Rights Reserved.

“Personal Data” Redefined

- Expansion of “***Personal Data***” Definition
  - ***Any information relating to a data subject***
  - Independent of whether it relates to ones private/professional/public life
  - Can be anything from a name, a photo, an email address, your bank details, your posts on social networking websites, your medical information, or your computer’s IP address

- “***Data subject***” definition broadened
  - Identified by means reasonably likely to be used by the data controller or by any other natural or legal person
  - By reference to not just an identification number but also to things like:
    - location data and online identifiers
    - Genetic identity
    - Mental identity
    - Others…

2015 Data Storage Innovation Conference. © Hitachi Data Systems. All Rights Reserved.

EU - GDPR Summary (1 of 5)

- Express Consent
  - Covered businesses are required to obtain (and not assume) the ***express consent*** of the data subject
  - The data subject may withdraw the consent at anytime; ***the right to be forgotten (the right to erasure)***
  - Consent is essentially not valid where there is an "*imbalance*" between the position of the data subject and the business

- Breach Notification Requirement
  - Businesses must notify the ***supervisory authority person***, of a personal data breach after becoming aware of the breach
  - Companies must also notify the ***affected data subject*** of a personal security breach

2015 Data Storage Innovation Conference. © Hitachi Data Systems. All Rights Reserved.

EU - GDPR Summary (2 of 5)

- Policies and Measures
  - Businesses are required to ***implement appropriate technical and organizational measures***
  - ***Privacy by design*** (and ***privacy by default***) principle
  - ***Right to data access, correction, and erasure***
  - ***Right to transfer data***
  - ***Special protections for children*** and their personal data
- Binding Corporate Rules (BCRs)
  - BCRs are the tool used by companies with global operations to transfer personal data of EU residents within their corporate group to entities located in countries which do not have an adequate level of data protection
  - ***BCRs will no longer need to be approved by each Data Protection Authority in each applicable EU Member State***

2015 Data Storage Innovation Conference. © Hitachi Data Systems. All Rights Reserved.

EU - GDPR Summary (3 of 5)

Data Protection Impact Assessment

- Required for businesses with processing operations that "***present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes***"
- Must describe the processing foreseen, risks to data subject rights and freedoms, means of addressing these and those designed to protect personal data, and demonstrate compliance with the Rules
- The views of the data subjects on the processing must also be sought
- Accomplished by or on behalf of the data controller (i.e., at its expense)
- Examples of these activities include (but not limited to):
  - Monitoring publicly accessible areas
  - Use of personal data of children
  - Use of genetic data or biometric data
  - Processing information on an individual's sex life
  - The use of information regarding health or race
  - An evaluation having the effect of profiling or predicting behaviors

2015 Data Storage Innovation Conference. © Hitachi Data Systems. All Rights Reserved.

EU - GDPR Summary (4 of 5)

Data Protection Officer (DPO)

- Requirement for organizations to appoint a DPO with expertise in privacy regulations if it processes data related to about 5,000 or more "data-subject" individuals in some way
- Responsible for monitoring data processing activities
- **Significant shortages are anticipated for these privacy experts**

Transfers of Data to Third Countries

- Restrictions on the transfer of personal data to third countries that do not offer an adequate level of protection remain in place
- International data transfers are possible if one of the following items are in place:
  - Binding Corporate Rules (BCRs)
  - "*Standard data protection clauses*" approved by the EC
  - Standard data protection clauses adopted by a DPA in accordance with the consistency mechanism
  - "Ad hoc" contractual clauses authorized by a DPA
  - Other appropriate safeguards "not provided for in a legally finding instrument"

2015 Data Storage Innovation Conference. © Hitachi Data Systems. All Rights Reserved.

EU - GDPR Summary (5 of 5)

Significant Penalties

- Introduces the ability of each supervisory authority to impose fines
- Penalties for violations of the Regulation range from a written warning to fines for intentional or negligent conduct of anywhere from ***€1,000,000*** or ***5% of the annual worldwide turnover*** of a company
- ***Severe Offenses include*** (among others):
  - Not adopting internal policies or does not implement appropriate measures for ensuring and demonstrating compliance
  - Not alerting on, or failing to do a data breach notification in a timely manner
  - Not carrying out a data protection impact assessment
  - Not designating a Data Protection Officer (DPO)
  - Carrying out a data transfer to a third country not allowed by an adequacy decision
- The administrative sanction "***shall be in each individual case effective, proportionate and dissuasive***"

2015 Data Storage Innovation Conference. © Hitachi Data Systems. All Rights Reserved.

WRAP UP

2015 Data Storage Innovation Conference. © Hitachi Data Systems. All Rights Reserved.

Summary

- ***The protection of personal data is a fundamental right for all Europeans*** (Article 8 of the EU's Charter of Fundamental Rights and by the Lisbon Treaty)
- When the rules are ultimately approved (est. early 2016), there will be a transition period (24 months) before enforcement starts (est. early 2018)
- Elements of the Regulation may be adopted early (e.g., the court case decided the right to be forgotten issue)
- There are indications that the existing **U.S.-EU Safe Harbor** may still have some value

2015 Data Storage Innovation Conference. © Hitachi Data Systems. All Rights Reserved.

Conclusions

- Until the Snowden adventure there were signs of softening of the Rules, the LIBE committee's revised draft has given indications that this is less likely going forward

- According to the ABA Business Law Section, don't wait until the Rules are approved:
  - *Put the General Data Protection Rules on Your Radar*
  - *Audit Risks for Potential Data Protection Violations*
  - *Incorporate Data Protection into Compliance Programs*
  - *Make Sure Proper Consent is Obtained*
  - *Prepare for Data Breaches*

2015 Data Storage Innovation Conference. © Hitachi Data Systems. All Rights Reserved.

THANK YOU

2015 Data Storage Innovation Conference. © Hitachi Data Systems. All Rights Reserved.