Industry Best Practices for Personal Data Security

Dale Johnstone

Chief Information Security Officer
PCCW Limited

dale.johnstone@pccw.com

Communications
Technology
Information

26 March 2007

1

Those Were the Days - Centralised

2

These Are the Times – Distributed PII

3

Potential Security Threats

- **Insider Leakage**
  - Corporate Gain (Staff Turnover)
  - Personal Gain (Extra $)
- **External Leakage**
  - Opportunist (Falls into Lap)
  - Malicious (Hacking)
- **Data Corruption**
  - Malicious (Virus)
  - Uncontrolled (Power)

4

Information Security (IS)

- **Confidentiality**
  - Security Policies & Procedures
  - Access, Authentication & Privilege Controls
  - Encryption
  - Logging, Auditing and Archiving
- **Integrity**
  - Data and Malicious Code Filters
  - Reconciliation
- **Availability**
  - Real-Time Monitoring

5

Management System (MS)

- **Policy (Plan)**
  - Document Management Intentions
- **Baseline (Do)**
  - Implement Appropriate Controls
- **Monitoring (Check)**
  - Check for Deficiencies
- **Enforcement (Act)**
  - Security Compliance & Improvement

6

Key Considerations

- Corporate Culture & Policies
- Risk Management Approach
- Security Controls to Protect from Potential Risks
- End to End Solution & Services Delivery & On-Going Support:
  - Multiple Enterprise Communication Platforms
  - Variety of Data Infrastructures
  - Variety of Security Systems
  - Different Network Connectivity/Interfaces
- Compliance

7

Personal Identifiable Info Protection

- **Storage**
  - PII Can Reside in Many Locations
- **Creation**
  - PII Can be Sourced / Determined
- **Access**
  - PII Accessible by Multiple Persons/Systems
- **Transmission**
  - PII Can be Transmitted by Various Means

8

PII Visionary Direction & Goal

- **Evolution** – All kinds of methods are, and will continue to, emerge involving: Storage, Collection, Access, and Transmission of PII
- **IT Solution** – Affordable, easy-to-manage, easy-to-integrate solution encompassing company PII needs
- **Simplification** – Managing a single Solution for all voice, data and video PII, rather than three
- **Monitoring** – Accessing one location to find every PII source needed to ensure compliance

9

Emerging International Efforts / Standards

- **European Union on PII Protection**
- **ISO on PII Protection**
  - **27001 – ISMS – Requirements**
  - **27002 – Code of Practice for ISM**
  - **29100 – A Privacy Framework**
  - **29101 – A Privacy Reference Architecture**

10

PCCW

EU to Develop RFID Guidelines

RESULTS OF THE PUBLIC ONLINE CONSULTATION ON FUTURE RADIO FREQUENCY IDENTIFICATION TECHNOLOGY POLICY
"The RFID Revolution: Your voice on the Challenges, Opportunities and Threats"
http://ec.europa.eu/information_society/policy/rfid/doc/rfidswp_en.pdf

17 March 2007 http://www.dailytech.com/article.aspx?newsid=6443

The European Commission sets out to regulate RFID in terms of privacy and data security

The European Commission announced last week its plans to place guidelines on radio frequency identification, or RFID. The CeBit technology trade show in Hannover, Germany held the stage for the announcement to draft rules to modify the EU e-privacy legislation in order to specify on the existing RFID regulations.

Information society commissioner, Vivien Redding, stated that a stakeholder group with industry, consumers, and data protection groups would be formed at first to give recommendations to the Commission in order to handle data security and privacy. The group will report back in 2008 with all the information needed regarding EU laws that are necessary.

Redding also told reporters, "We should stimulate the use of RFID technology in Europe while safeguarding personal data and privacy." Also that the Commission would not tie up the use of RFID in the in regulations, Redding quoted, "We must not over regulate RFID, but we must provide the industry with legal certainty."

According to *CNET*, the Commission also published a strategy report on Thursday after consulting with interested partied. The report included that the RFID tags needed to be more secure, in aspects of encryption and authentication.

With RFID technology implemented in a wide range of uses such as on transportation and tracking cattle, the regulations on the technology become a necessity for the privacy and date security of consumers.

11

PCCW

ISO 27001 – ISMS - Requirements

- **Requirements for:**
  - **Establishing**
  - **Implementing**
  - **Operating**
  - **Monitoring**
  - **Reviewing**
  - **Maintaining**
  - **Improving**

- **Security Controls as Part of a Documented ISMS Within the Context of the Organisation's Overall Business Risks**
- **Customized to Needs of Individual Organizations or Parts Thereof**
- **Ensure the Selection of Adequate and Proportionate Security Controls to Protect Information Assets and Give Confidence to Interested Parties**

12

ISO 27002 – Code of Practice for ISM

- **Establishes guidelines and general principles for:**
  - **Initiating**
  - **Implementing**
  - **Maintaining**
  - **Improving**

  organizational security standards and effective information security management practices within an organization

Security Policy	Access Control
Organizing Information Security	Information Systems Acquisition, Development and Maintenance
Asset Management	Security Incident Management
Human Resources Security	Business Continuity Management
Physical and Environmental Security	Compliance
Communications and Operations Management	

- **Objectives provide guidance on commonly accepted goals of information security management**
- **Control objectives and controls implemented based on requirements identified by a risk assessment**
- **Assist to build confidence in inter-organizational activities**

13

ISO 29100 – A Privacy Framework

- **Defines privacy safeguarding requirements relating to PII processed by any information and communication system**
  - **Set Common Privacy Terminology**
  - **Define Privacy Principles When Processing PII**
  - **Categorize Privacy Features**
  - **Relate Described Privacy Aspects to Existing Security Guidelines**
  - **Basis for Desirable Additional Privacy Standardization Initiatives**
    - **Technical Reference Architecture**
    - **Use of Specific Privacy Technologies**
    - **Overall Privacy Management**
    - **Privacy Impact Assessments**
    - **Engineering Specifications**
- **Framework**
  - **General in Nature**
  - **Address System-specific Issues on a High-level**
  - **Closely linked to Existing Security Standards Implemented Into Practice**

14

ISO 29101 –Privacy Reference Architecture

- Describe best practices for a consistent, technical implementation of privacy requirements as they relate to the processing of PII in information and communication systems
  - Various Stages in Data Life Cycle Management
  - Required Privacy Functionalities for PI Data in Each Data Life Cycle
  - Positioning Roles and Responsibilities of all Involved Parties
  - Present a Target Architecture
  - Provide Guidance for Planning And Building System Architectures
  - Facilitate Proper Handling of PI Data Across System Platforms
  - Set Out Necessary Prerequisites to Allow
    - Categorization of Data
    - Control Over Specific Sets of Data Within Various Data Life Cycles
- Architecture
  - Closely linked to Existing Security Architecture Elements Compatible With Implemented System Practices

15

Industry Best Practices for Personal Data Security

Dale Johnstone

Chief Information Security Officer
PCCW Limited

dale.johnstone@pccw.com

26 March 2007

Communications
Technology
Information
Solutions

16