PRIVACY IS 80% INFORMATION SECURITY
- HOW TO MANAGE PRIVACY IN YOUR ORGANIZATION

NISlecture 2014/06
Sept. 26, 2014
Hans Dahlquist
OUTLINE

Privacy Different Perspectives of:

1. Legal compliance
2. Brand and reputation
3. Cost

What to do?
10 Arrested in Theft of Web Data

By BRIAN X. CHEN and JOHN H. CUSHMAN Jr.
Published: December 12, 2012

International authorities, with some help from Facebook, have arrested 10 people accused of operating a network of infected computers that stole personal information from millions of victims.

TD Bank says 260K customers exposed in data breach

December 14, 2012

California leaks Social Security numbers for second time this year

Department of Health Care Services downplays latest incident, in which 14,000 Medi-Cal providers’ Social Security numbers were posted online

By Ted Samson | InfoWorld

TD Bank has begun notifying about 260,000 customers from Maine to Florida that the company says may have been affected by a data breach.

Company spokesman Rebecca Acevedo confirmed in emails Friday to The Associated Press that unencrypted backup data tapes were misplaced in transport in March.

She said the tapes contained personal information, including account information and Social Security numbers, but the company is not aware of any misuse of customer information. Still, TD Bank has not ruled out the possibility and is monitoring the situation.
“... the loss of an external hard drive that contained the personal information for 583,000 Canada Student Loan borrowers. The unencrypted hard drive was found to be missing on Nov. 5, but department security was not notified until Nov. 28 ... data, which included names, birthdays, and social insurance numbers ...”

Vodafone Hacker Accesses 2 Million Customers’ Banking Data
Bloomberg (09/12/13) Weiss, Richard

........... According to Vodafone spokesman Kuzey Esener, the attack was carried out by a person with insider knowledge who stole data including the names, addresses, birth dates, and bank account information of 2 million customers. He added that the hacker had no access to credit-card information, passwords, PIN numbers or mobile-phone numbers.
As computer experts peel back the layers of Target’s massive data breach, federal and state law enforcement agencies are running parallel investigations to find the cyber criminals who infiltrated the retailer’s computers.

Target reported Friday that the cyber thieves compromised the credit card data and personal information of as many as 110 million customers. That data includes phone numbers, email and home addresses, credit and debit card numbers, PINs, expiration dates and magnetic strip information.

“The Secret Service will confirm that it is looking into it,” said a Target spokesperson.

The investigation is also expected to examine the possibility that multiple individuals were behind the attack.

Investigators have been working over the weekend to understand how the data was compromised.
43 Percent of Companies Had a Data Breach in the Past Year

USA Today (09/24/14) Weise, Elizabeth

According to a recent Ponemon Institute report, 43 percent of companies have experienced a data breach in the last year, up 10 percent from a year ago. "He noted that more than 80 percent of the breaches his firm works with "had a root cause in employee negligence," such as giving out passwords, spear phishing, lost USBs, and mishandled files."
CONCLUSIONS

1. Information and IT security are too weak in almost all countries, all areas and all businesses in relation to the threat
2. Rare with sophisticated cyber attacks – it not needed
3. Unacceptable situation from a consumer/customer perspective
4. Privacy breach very offending, difficult to handle for the customer and has a very negative effect on the brand
5. Privacy related fraud crime is the fastest growing crime
6. Personal Identifiable Information (PII) data records has a value and can be purchased on the Internet
7. Privacy legislation is lagging behind in all countries
8. Self regulation of Privacy is growing in the private sector
PII as Currency

Sam Pfeifle

Privacy Perspectives | Sep 3, 2014
HOW CAN IT HAPPEN?
We analyzed the result when visiting svd.se (Svenska Dagbladet), 13 connections was found, 2 encrypted.

Also check encrypted connections:
- Mobile Broadband connection
- Webmail
OTHER TYPICAL CAUSES FOR LEAKAGE

1. Lack of security for Third Party Connections (TPC) – Target Corporation sub contractor
2. Loss of hardware as laptops, Hard Discs etc – no HD encryption
3. Weak passwords, insiders, corruption, late patching

• Rare with sophisticated cyber attacks – it is not needed
IMPORTANT REQUIREMENTS IN THE EU DATA PROTECTION REGULATION

1. A ‘right to be forgotten’ will help people better manage data-protection risks online. When they no longer want their data to be processed and there are no legitimate grounds for retaining it, the data will be deleted. *(Erasure of selected customer records, very costly)*

2. Whenever consent is required for data processing, it will have to be given explicitly, rather than be assumed. *(In General terms and Conditions)*

3. Companies and organizations will have to notify serious data breaches without undue delay, where feasible within 24 hours. *(Incident Management to customer and authorities)*

4. Increased responsibility and accountability for those processing personal data. *(data protection, availability, access management, encryption, classification of privacy records and assignments of ownership, CPO (Chief Privacy officer) with Privacy Governance)*

5. Companies will only have to deal with a single national data protection authority – in the EU country where they have their main establishment. *(One-Stop-Shop)*
1. PRIVACY LEGAL COMPLIANCE PERSPECTIVE

- Different legislation in all countries, from non existing to very extensive
- New Privacy legislation is coming in many countries
- US legislation very fragmented
- EU Data Protection Regulation (DPR) will be decided in April (?) 2015 and in force 2017/18?
- To be EU DPR compliant in 2017/18 – start now!
- Difficult to handle Privacy for international companies
- Data Transfer Agreements (DTA) needed when outsourcing Privacy data
- Binding Corporate Rules (BCR) a growing international arrangement for cross-border transfer of data
2. BRAND AND REPUTATIONAL PERSPECTIVE

- Highest risk exposure; loss of privacy records
- International companies handling Privacy data should have one Privacy Policy covering the legislation in all countries
- One brand – one policy – one treatment of the customer
- Investments in Privacy is a business decision based on risk, legal compliance, potential fines (EU) and market perspective (Brand etc.)
INPUT TO THE PRIVACY POLICY

1. Legal and contractual/license requirements in force

2. Coming legal requirements (EU)

3. Customer care, branding, risk reduction

4. Signed commitments (Global Reach initiative, UN human rights etc.)

Self regulation

Privacy Policy
3. PRIVACY COST PERSPECTIVE

- Most costly requirement is purging of privacy records (at least one MSEK/database)
- Almost no information system/database is designed to remove specific data records
- Not unusual with 20-60 databases or more with Privacy data in an organization
- Updated asset and information content management is first step
- Information architecture must be documented
- Lack of “one-stop-shop” will drive audit cost for international companies
- **Privacy by design** is an urgent requirement in ICT sourcing
- Potential fines up to 2 or 5% of global annual turnover if non compliance to EU Data Protection Regulation
INFORMATION ARCHITECTURE MISSING - DIFFICULT WITH DATA PURGING
WHAT TO DO?

Based on previous experience from almost 3 years of global Privacy Policy implementation
STANDARD FOR PRIVACY; ISO/IEC 29100 PRIVACY FRAMEWORK

1. Framework for handling of PII
2. Certification not possible
3. No Management System
4. Content:
   - Terms and definitions
   - Roles for handling PII
   - PII security requirements and risk management
   - References for known principles for Privacy
PII = PERSONAL IDENTIFIABLE INFORMATION

- Name
- Home address
- Phone number
- E-mail
- Pictures
- Position
- Social security number
- Credit card data
- Bank account
- IP address
  - Etc according to ISO 29100

“Or any personal information relating to an individual, whether it relates to his or her private, professional or public life”
1. Clear and decided vision on purpose; why are we doing this and what do we want to achieve?

2. How to reach the vision (project or line activity etc)?

3. Who is responsible and accountable?

4. What are the main processes?

5. What support, routines, activites and controls do we need?
"If you don't know where you are and where you want to go it is difficult to describe the way to your destination"
PRIVACY MANAGEMENT SYSTEM:

1. **Steering and guiding documents**
   - Legislation, Standards, agreements, Policy, Directives, Instructions, guidelines and decisions

2. **Processes:**
   - Continuous improvements (PLAN – DO – CHECK – ACT)
   - Controls, compliance, reporting and KPI:S
   - Management commitment and decisions
   - Training and communication
   - Implementation and maintenance
   - Privacy risk management etc.

3. **Organization** with clear roles (Chief Privacy Officer, CPO), responsibility, authority and knowledge in an operational description (Privacy Governance)
INFORMATION LIFE CYCLE MANAGEMENT – A MUST

Information lifecycle

Capture

Processing

Transmission

Presentation

Storage

Backup

Access rights

Encryption?

Disposal

Purging

New customer

VPN?

CRM

Access rights

VPN?
IMPLEMENTATION SUMMARY:

• Create and anchor a Privacy policy and a change management strategy

• Start with a rather deep GAP-analysis before implementation

• Use Management System as an implementation and maintenance strategy

• Integrate the Privacy MS as a component in ISO 27001 if implemented (Privacy is 80 % Information Security)

• Use ISO 29100 as a framework for support

• Make sure ”Privacy by Design” is implemented with priority for all new procurement of ICT

• Decisions must be based on risk assessment in order to reduce the exposure
CONCLUSIONS AND SUMMARY

• Loss of privacy data is will hurt your brand, reputation and profit, over 100 million data records lost so far during 2014 in the US
• Privacy related fraud is increasing rapidly
• Your personal preferences and behavior on Internet is spread and stored without your knowledge and consent
• The legal requirements are increasing
• Self-regulation is more important than pure legal compliance in the private sector
• Privacy has moved from a legal compliance problem to a business enabler
• Most costly is data purging. A “one-top-shop” and “Privacy by Design” will lower cost
• Implement a Privacy Management System for effective maintenance and improvements in Privacy
Questions and comments?

hans.dahlquist@rote.se

+46 733 687795

www.rote.se