

**How to enable security in large corporation without strict enforcement?**

---

# Real Life Information Security

To protect the confidential and proprietary information included in this material, it may not be disclosed or provided to any third parties without the approval of Hewitt Associates LLC.

**Hewitt**

# What is Hewitt?

## Human Resources Outsourcing company

- Pensions, payroll, benefits for thousands of companies worldwide

## From security perspective

- 90% work is on personal and highly sensitive data
- ~25'000 associates worldwide
- Large number of jurisdictions and legal systems
- Hundreds of bussiness teams with VERY different characteristics

## What Hewitt is not?

### Not in banking industry

- ▣ Not globally bound by financial regulations
- ▣ People don't have feeling that they work for financial institution

### Advantages and disadvantages

- (+) We (Hewitt) have less pressure and more choice
- (-) We (Security) have less powers and more choices

# Most important regulations

## Personal information privacy laws

- 27 of them in Europe
- All different (even if they stem from one EU Directive)
- Most strict in France

## Financial regulations

- Some teams are FSA regulated

## Client requirements

- Frequent requests for 3rd party auditing
- SOX, SAS-70

## Shepherd or policemen

### Very strong pressure from bussiness

- Highly competitive, global market

### You can't just say „you have to” in many cases

- If there's no strict legal or client requirement
- „Best practice” theory needs to pass through reality check

### Need for well prepared argument with clear cost-benefit analysis

**Welcome to „sell your security services internally” world!**

# Cost and Benefit in Security

## Simple Risk Analysis

- $Risk = Asset\ Cost * Threat\ Probability$
- Then establish Controls to prevent risks

## Cost of controls

- Not only direct cost of roll-out (license, installation)
- Employee's burden to use control is also Cost
- If  $Control\ Cost > Asset\ Cost$  then it doesn't make much sense!

**Pretty obvious for Business folks**

**Not so obvious for Security folks**

## Case studies: Web application security

### We write many web applications for clients

- Security through education, penetration testing, source code auditing, web application firewalls etc.
- Many 3rd party penetration testing of our applications

### **Case study #1 – „*you don't use httpOnly/disable Autocomplete!*”**

- Minor, non-standard features introduced in 2008 by Microsoft
- Slowly adopted by most web application frameworks

### **Case study #2 – „*you used RC4-MD5 in SSL!*”**

- Penetration testing company is completely wrong
- Ok, now explain that to client!

# Security as a cost?

## This is how it's often seen by Business

- Security = „Necessary evil, required by Regulators, waste of our hardly earned money”

## Security folks know the truth here

- Often they can't properly express it

## Security is not a cost

## Security is an investment to prevent losses

- Spend \$100k to prevent losing \$1m = 10x benefit
- It's not: „Security spent \$100k”
- It's: „Security helped saving \$1m for just \$100k”

# Successful security in competitive world

## So even if you have powers...

- Try to understand your client needs as much as possible
  - Client = your Sales dept, Citizens, National business
- Perform as much **real life** risk analysis (including cost & benefit)
- Make sure your controls **help things** instead of **breaking things**
- Periodically perform a reality check – how does my security **help** business?
- Otherwise you may destroy your organisation's flexibility and competitive advantage
  - And lose your job – and make hundreds other people lose job as well

## Ponemon Report (2006)

### Direct cost to handle data breach incidents

- On average **4,8 milion USD** – from 226'000 to 22'000'000

### Cost of controls implemented after the breach

- On average **180'000 USD** for one incident

### Data loss caused by organization internal factors

- **70%** cases caused by lack of data ownership, ignoring procedures and negligence

### Data loss during electronic data processing

- **90%** incidents caused by loss of laptop or electronic media

## Case study: Lost laptop

### Real life incident from 2005

- Still remembered by some senior management

### One laptop was lost by associate on way home

- Laptop was unencrypted, contained ~6000 client records
- Ponemon's estimate from 2008 is \$100-200 **per record**

### How much this single incident costed us at the end of the day?

- We use this example in every internal presentation
- Close hit, real people, real money

*Note: You have to pay even if no abuse was confirmed!*

## Case study: FSA fines HSBC

### FSA fined HSBC Group for £3m, June 2009

- Public report on FSA website
- How close was the hit to our industry?
  - Very close
  - So we immediately used that in internal newsletter
- FSA published list of issues found
  - „How many of these issues you recognize in your team?”

## Case study: Successful controls

### We deployed full-disk encryption (FDE)

- All laptops covered company-wide

### Office break-in in 2009

- 4 laptops stolen

### Cost for organisation at the end of the day – close to ZERO

- Hardware was covered by insurance
- Data was backed up
- Whole operating system was encrypted
- You can prove this to client, because all laptops are encrypted by policy

# Things we learned when talking to business

## **Avoid „weasel talk” and buzzwords**

- Blacklist wording like: „some attacks exist that might pose a risk”

## **Use as much facts and numbers as possible**

- Do use industry reports
- But always filter them through your company’s context
- Learn from historic incidents in YOUR organisation
  - Single such incident is worth 10 industry reports

## **Perform periodic reality checks on your arguments**

- If necessary drill down to a single specific incident
- Build cause-reason trees
- Make sure at the end the threat is still there!

# Questions?

Questions, comments

<http://www.linkedin.com/in/pawelkrawczyk>