IV Konferencja

SEMAFOR SECURITY • MANAGEMENT • AUDIT FORUM

Real Life Information Security

Embedding security in economic reality

pawel.krawczyk@hewitt.com

Hewitt Associates

- **Human Resources Outsourcing and Consulting**
- **~25’000 employees worldwide**
- **Highly sensitive client data**

Hewitt's Market

- **Not *purely* financial**
- **Mostly B2B**
- **Highly competitive**
  - Requirement to remain competitive
  - Requirement to be flexible

Security - Shepherds or policemen?

- **Very high pressure from business**
- **No „one size fits all” approach**
- **Lessons learnt**
  - Talk to business
  - Have real discussions
  - Continually talk to the business
- **Where do all these numbers come from?**

Learn from the past

ID: 2205: HSBC Life lost a CD containing the details of 180,000 policyholders

Date: 2009-07-22 Records Lost: 180,000 Source: Inside Accidental Submitted by: jjturner Location: Southampton Southampton, GB

Organizations: HSBC Life, HSBC Holdings plc

ID: 2206: HSBC Actuaries lost a floppy disk containing the personal information of 1,917 pension scheme members

Date: 2009-07-22 Records Lost: 1,917 Source: Inside Accidental Submitted by: jjturner Location: GB

Source: DatalossDB.org

Learn from market analytics

- **~$100 USD per record**
- **No actual abuse required**
- **„Losing control” is *the* greatest failing of security**
- **How much should we spend and where should we stop?**

Source: Ponemon Institute, „2008 Annual Study: Cost of Data Breach”

Learn from others' mistakes

HSBC firms fined over £3m for information security failings

FSA/PN/099/2009
22 July 2009

The Financial Services Authority (FSA) has fined three HSBC firms over £3 million for not having adequate systems and controls in place to protect their customers' confidential details from being lost or stolen. These failings contributed to customer data being lost in the post on two occasions.

Source: FSA, 22 July 2009

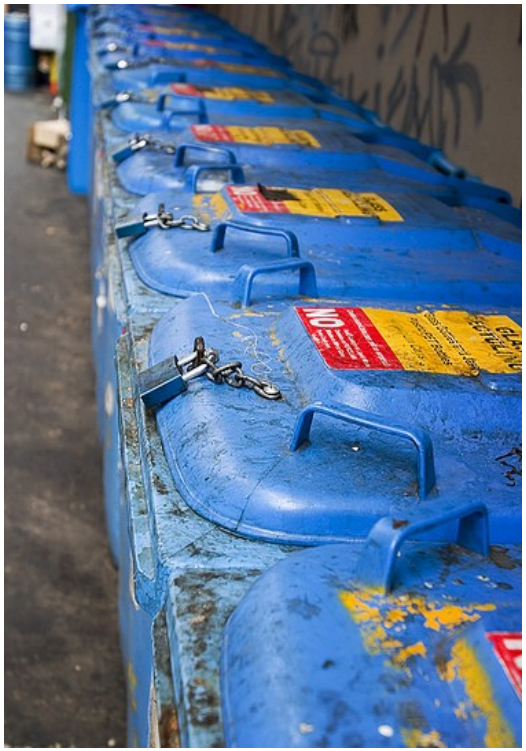
Learn from Your risk analysis

$$Risk = Impact \times Probability$$

Impact ~ Asset Cost, Brand Value...

When Risk Management makes sense?

Control Cost << Asset Cost



Source: Flickr (edouard)

What makes Control cost?

- **Roll-out cost**
  - Obvious
- **Change cost**
  - Not so obvious
- **Management cost**
  - Not so obvious
- **End-user usage cost**
  - Largely ignored
  - Especially if outside

Source: Flickr (daveme)

Wrong but common scenario...

Risk Analysis → Potential loss →
Control → Real loss

☺

Case studies

Qualified Certificate in ZUS*

- **ZUS costs**
  - Roll-out = ?
  - Administration = ?
- **Taxpayer costs (245’000 QC’s)**
  - 100-140 million PLN – one-time
  - ~40 million PLN – annual QC renewal
- **Future costs**
  - Attribute certificates (ZUS & taxpayers) = ?
  - „e-PUAP trusted profiles” (ZUS) = ?

* ZUS = Polish public pensions provider

Source: Money.pl, ZUS

Invoicing

What's the cost of invoicing?

– People, paper, printing, postal, processing

– Average €1,4 per paper invoice

– Multiply by 1000, 10'000, 100'000... invoices

Ultimate solution

– Well, give up VAT…

When e-invoicing makes sense?

» Electronic invoice TCO << Paper invoice TCO

» Theory: €0,4 versus €1,4

» Key word: TCO

Sources: EU MEMO/00/85

E-Invoicing in Europe

Denmark

– OCES & others allowed
  - OCES: Quite simple origin & integrity authentication
  - OCES: Proportional to **e-invoicing risks**

Around 66% of all invoices are e-invoices

Poland

– Only QES & EDI allowed
  - EDI: supermarkets only
  - QES: Not designed for automatic signature
  - QES: More legal that real security

Around 5% of companies use e-invoicing

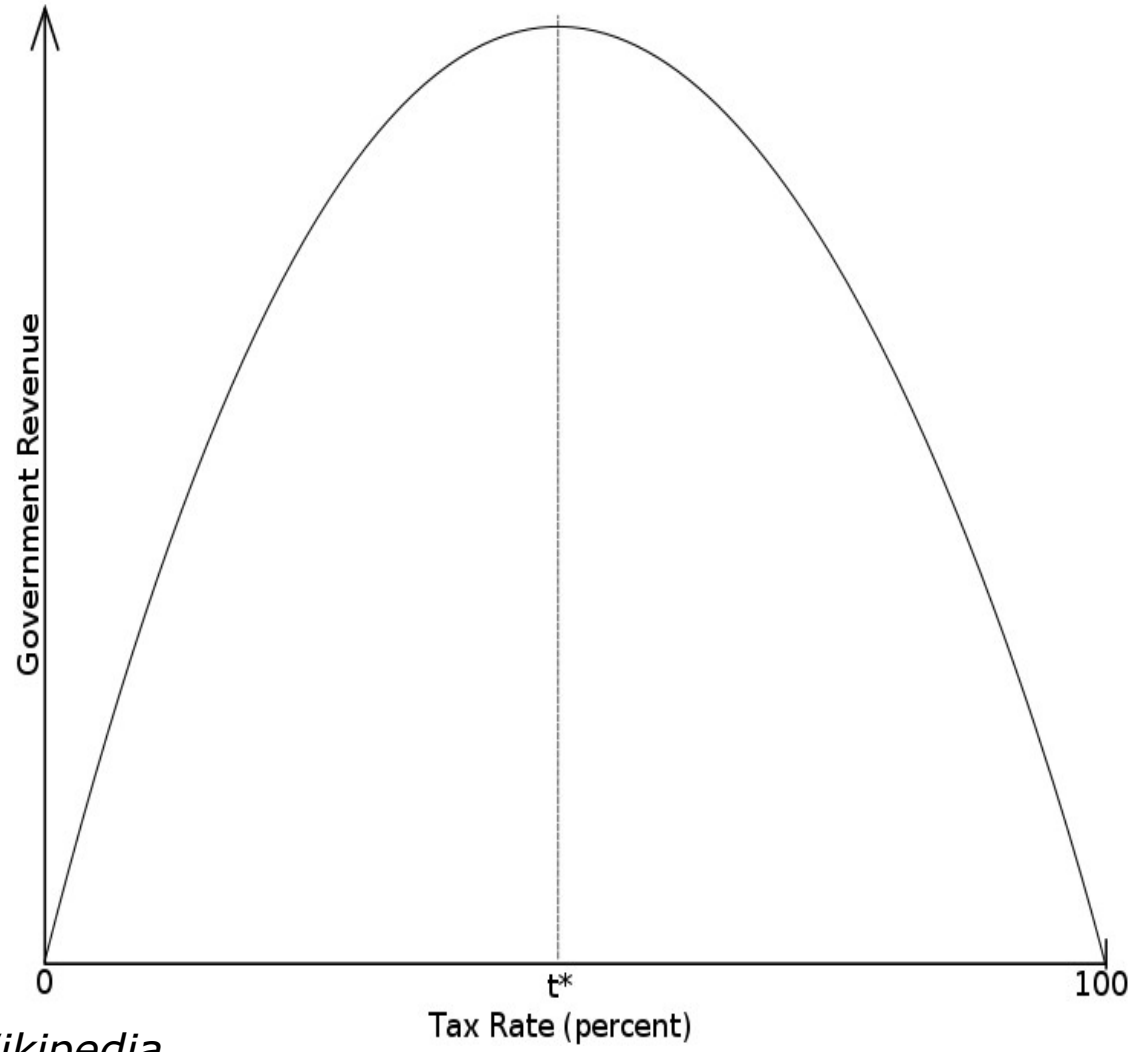
Sources: EEI 2007, ITST, OECD; GUS 2008

Risk Management in e-banking

Auth method	Number	Individual	Corporate
		Millions of clients	High non-repudiation needs
SMS	15	↑**Usable,** ↓**Big cost**	↓**Repudiation**
Token	11	↓**Big cost**	↓**Repudiation**
TAN	7	↓**Low security,** ↑ **Low cost**	↓**Repudiation**
Smart-card	2	↓**Not usable,** ↓**Big cost**	↑ **Non-repudiation**

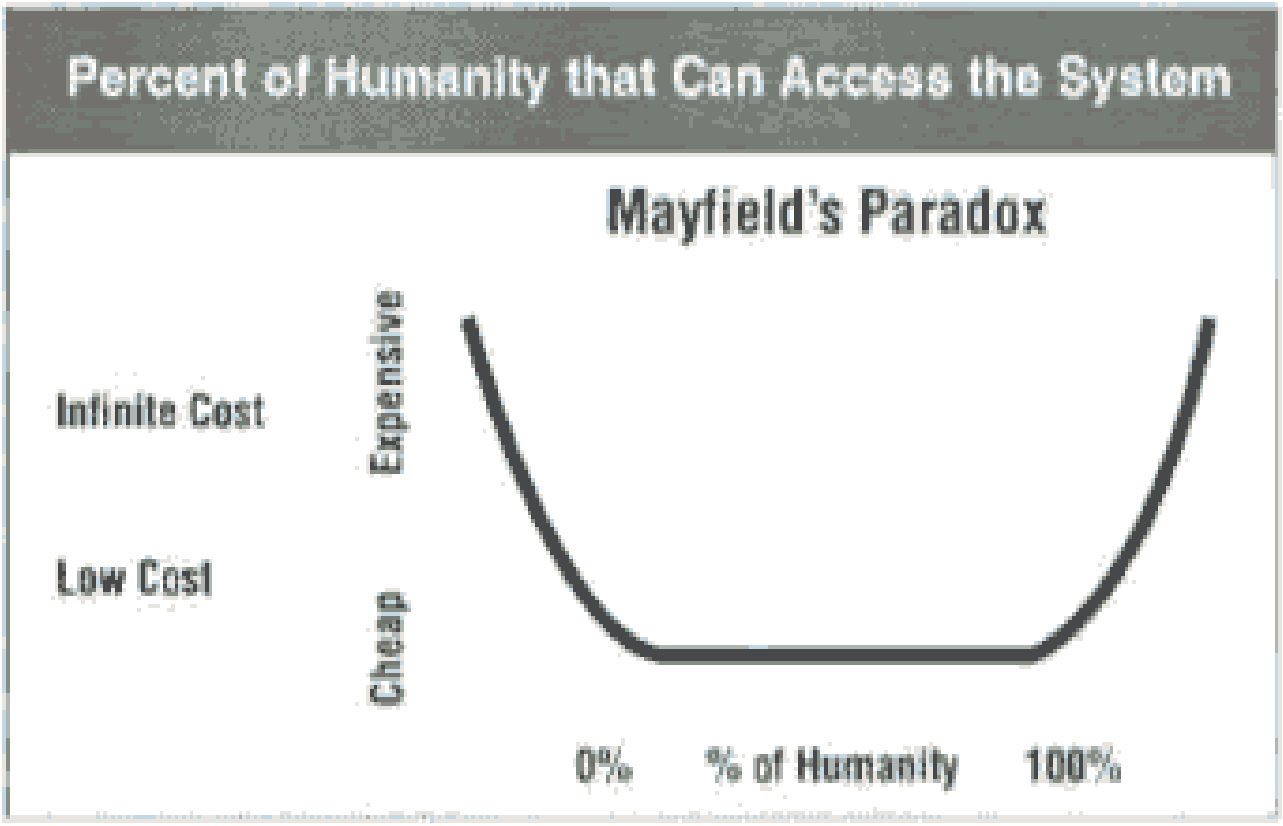
Source: Bankier.pl report, October 2009 (selected data only)

Laffer's curve in security



Source: Wikipedia

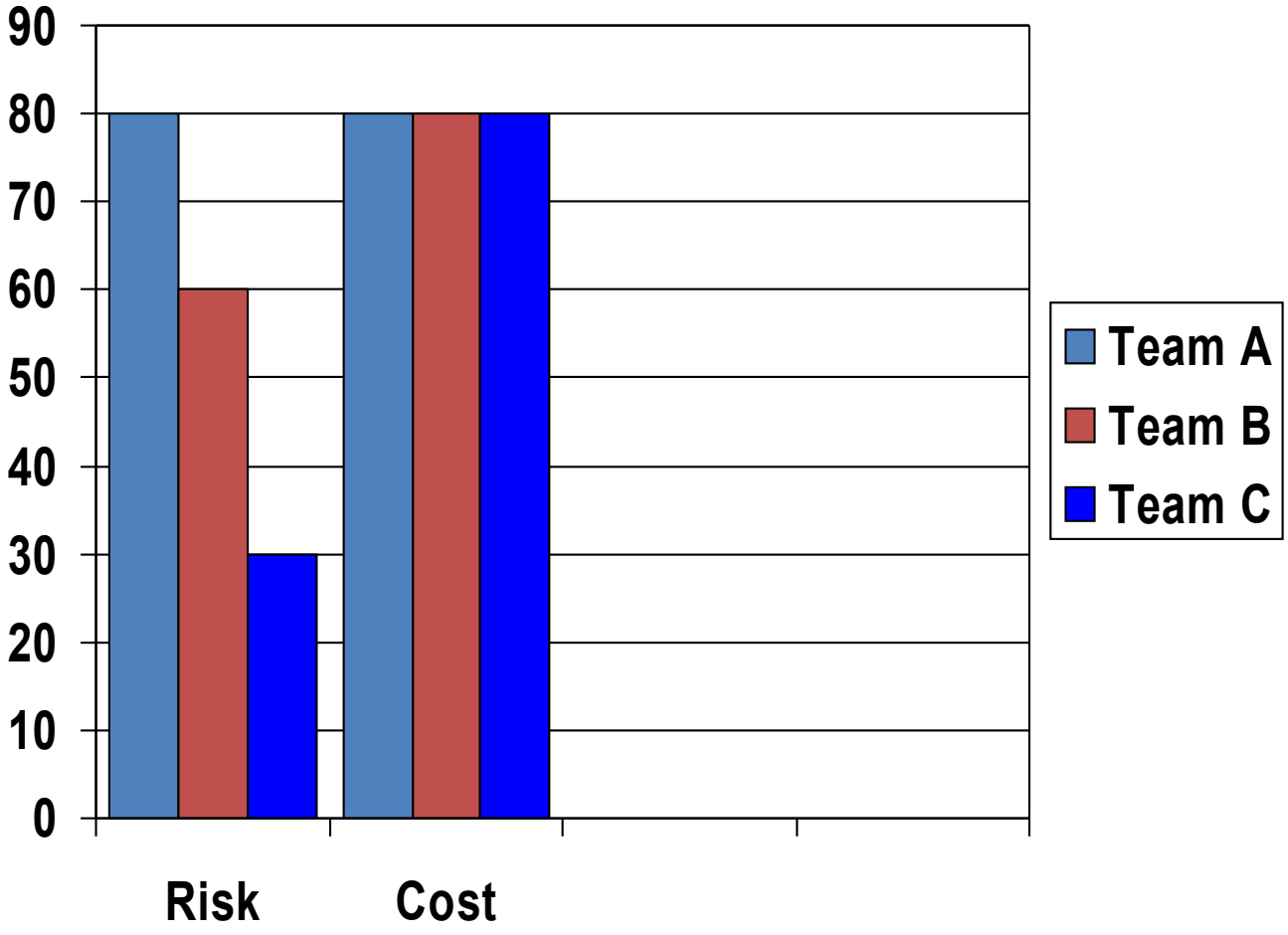
Mayfield's Paradox



Source: ISACA, „Mathematical Proofs of Mayfield's Paradox", 2001

How to?

Avoid „one-size fits all” approach



Control questions

Before deploying a new solution

– Do my controls help or do they hinder the business process?
– How do my controls help the business to do its work better?

Before asking for new funding

– What did we **learn from the** last project?
– What did the business earn/not lose as a result of previous security projects?

Is security a cost?

Security is an investment to prevent loss

– Spend $100k to prevent losing $1m = 10x benefit

– NOT: „Security again spent $100k”

– YES: „Security helped save $1M for just $100k”

How FDE* saves money

- **Office break-in**
- **Four laptops stolen**
- **All with full-disk encryption**
- **Cost of incident – <u>zero</u>**
  - Hardware – insurance
  - Data confidentality – able to prove to client
  - Data availability – backups & network drives
- **Where's ROI of FDE?**
  - No $$$ in fines
  - No $$ in breach notification
  - No $... in brand damage

** FDE = Full-Disk Encryption*

European Transportation Lane Study
Paris to Madrid

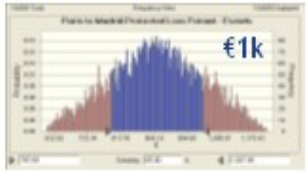
FIRST Advantage

Annual Lane Value: € 14,400,000
Shipment Frequency: 72 per year
Distance: 1,303 KM
Average Shipment Value: € 200,000

Average Annual Loss: € 75,000
Annual Security Escort Costs: € 101,634
Annual Telematics Costs: € 1,080

Security Countermeasure Analysis:
Escorts vs. Telematic Tracking

Protected Loss Forecast - Escorts



Unprotected Loss Forecast

Protected Loss Forecast - Telematics

GE imagination at work

GE Equipment Services
Asset Intelligence

Source: Willem Duiff, GE (SASMA 2009)

Building a consistent security policy #1

- **Should people take their laptops home?**
  - Isn't that increasing risk of theft?
- **Laptop theft**
  - Lose laptop ($)
  - Lose data ($$$)

Source: Flickr (aresnick)

Building a consistent security policy #2

- **Benefits of laptop at home**
  - Disaster Recovery
- **Work from home**
  - Examples: UK snow (2009), London flood (2009), Hemel Hempstead explosion (2005)
- **Need to prevent the other risks**

Source: Wikipedia

Building a consistent security policy #3

- **Perform risk analysis and cost-benefits balancing**
- **Deliver proper controls & evidence**
  - FDE is standard, non-optional proces
- **Deliver simple end-user message**
  - *„Always take your laptop home”*

Things we learned when talking to business

Avoid „weasel talk" and buzzwords

– *„Some attacks exist that might pose a significant risk..."*

Talk facts, numbers and money

– **Do** use industry reports

– Be careful with **vendor** reports

  • *„How spam filtering helps preventing global warming"*

– **Filter** them through your company's reality check

– **Learn** from historic incidents in your organisation

Perform periodic review of your controls

– Make sure at the old threat is still there

– Make sure no new threats appeared

SEMAFOR

IV Konferencja

SECURITY • MANAGEMENT • AUDIT FORUM

ISSA

www.issa.org.pl

Paweł Krawczyk

- pawel.krawczyk@hewitt.com
- http://www.linkedin.com/in/pawelkrawczyk

COMPUTERWORLD Polska

www.computerworld.pl

prezentacja dostępna
będzie na stronie konferencji
semafor2010.computerworld.pl