# Economics of Security

**International Seminars on Planetary Emergencies**
**and Associated Meetings – 43rd Session**
**Erice, 19-25 August 2010**

Udo Helmbrecht

Executive Director
European Network & Information Security Agency - ENISA

# Agenda

- Introduction to ENISA
- Quantitative & Qualitative Data
- Economic Incentives & Barriers
- Economics of Security For Businesses
- Conclusions

# INTRODUCTION

# 500 Million people in 27 Countries

## 23 languages



## ENISA

## Heraklion, Crete

# ENISA Overview

- The European Network & Information Security Agency (ENISA) was formed in 2004, employs around 65 experts.
- Develop a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations of the European Union, thus contributing to the smooth functioning of the internal market.
- The Agency is a *Centre of Expertise* that supports the Commission and the EU Member States in the area of information security.
- We facilitate the exchange of information between EU institutions, the public sector and the privatesector.

# Activities

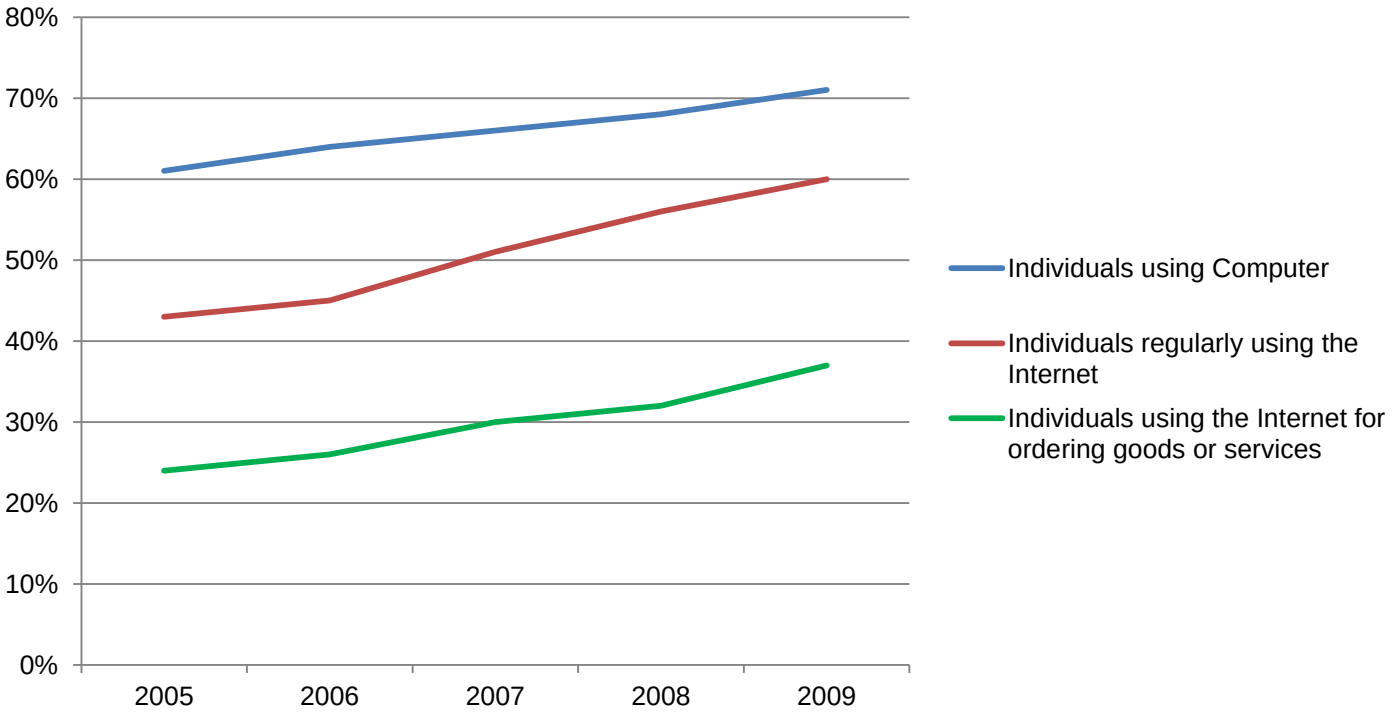
- The Agency's principal activities are as follows:
  - Advising and assisting the Commission and the Member States on information security.
  - Collecting and analysing data on security practices in Europe and emerging risks.
  - Promoting risk assessment and risk management methods.
  - Awareness-raising and co-operation between different actors in the information security field.
- recent published papers:
  - Priorities for Research on Current and Emerging Network Trends
  - Mobile Identity Management
  - Enabling automated air travel ...
  - Business Continuity for SMEs
  - Web 2.0 Security and Privacy
  - Cloud Computing

# QUANTITATIVE & QUALITATIVE DATA

## WHAT IT SAYS …WHAT IT DOESN'T SAY.

# The use of PC and Internet in the EU 27

- The importance of IT Security and its economical aspects increases year after year along with the increase in the use of IT by the European Citizens.




Source: Eurostat

# What Data Exists?

- There are many published sources of data on security:
  - Reports from consultancy firms.
  - Data published by CERT teams.
  - Ad hoc reports on specific subjects.
  - …
- Many of these reports are published at periodic intervals, which allows for the detection of trends in certain cases.
- The following slides provide key data and conclusions from these reports

# Limitations in Data Collection

- Due to the sensitive nature of the information, data collection is neither systematically tracked nor fully reliable
- Data source is often biased or has reasons to present a certain picture for reputation purposes depending on its role in the supply chain of Information Security
- OECD: “Although precise data on online criminal activity and the associated financial losses is difficult to collect, it is generally accepted that malware contributes significantly to these losses. Further, where data on cybercrime and its economic impact is available, businesses and governments are often reluctant to share it publicly.” [http://www.oecd.org/dataoecd/53/34/40724457.pdf]

# McAfee: Loss of $ 1 Trillion

- Between 2008 and 2009 American Businesses lost more that 1 trillion USD worth of intellectual property due to cyber attacks

- This amount does not include losses from:

- Theft of personally identifiable information (PII)
- System Inefficiency and Downtime
- Loss of Customers
- Negative impact on corporate share values

Source: McAfee report “Unsecured Economies”
http://resources.mcafee.com/content/NAUnsecuredEconomiesReport

# InfoWorld: $3.8 Million

- A study of 45 U.S. organizations found that cyber crime - including Web attacks, malicious code, and rogue insiders - costs each one of them $3.8 million per year, on average, and results in about one successful attack each week

Source: http://www.infoworld.com/d/security-central/cybercrime-costs-businesses-each-38-million-year-732

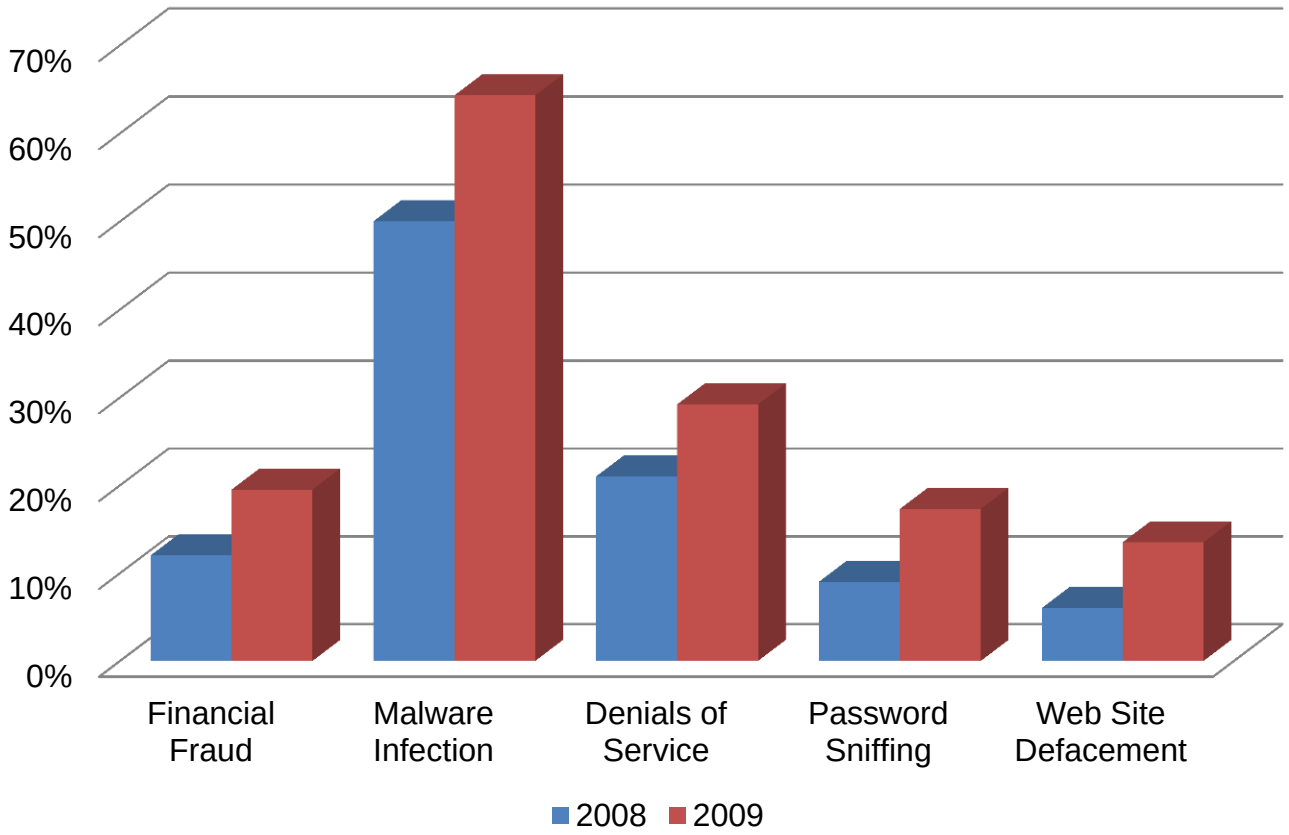
# 2009 Internet Crime Report

From January 1, 2009 through December 31, 2009, the Internet Crime Complaint Center (IC3) Web site received 336,655 complaint submissions.

| Year | Complaints Received | Dollar Loss |
|---|---|---|
| 2009 | 336,655 | $ 559.70 million |
| 2008 | 275,284 | $ 265.00 million |
| 2007 | 206,884 | $ 239.09 million |
| 2006 | 207,492 | $ 198.44 million |
| 2005 | 231,493 | $ 183.12 million |

http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf

# Global Trend of Incidences



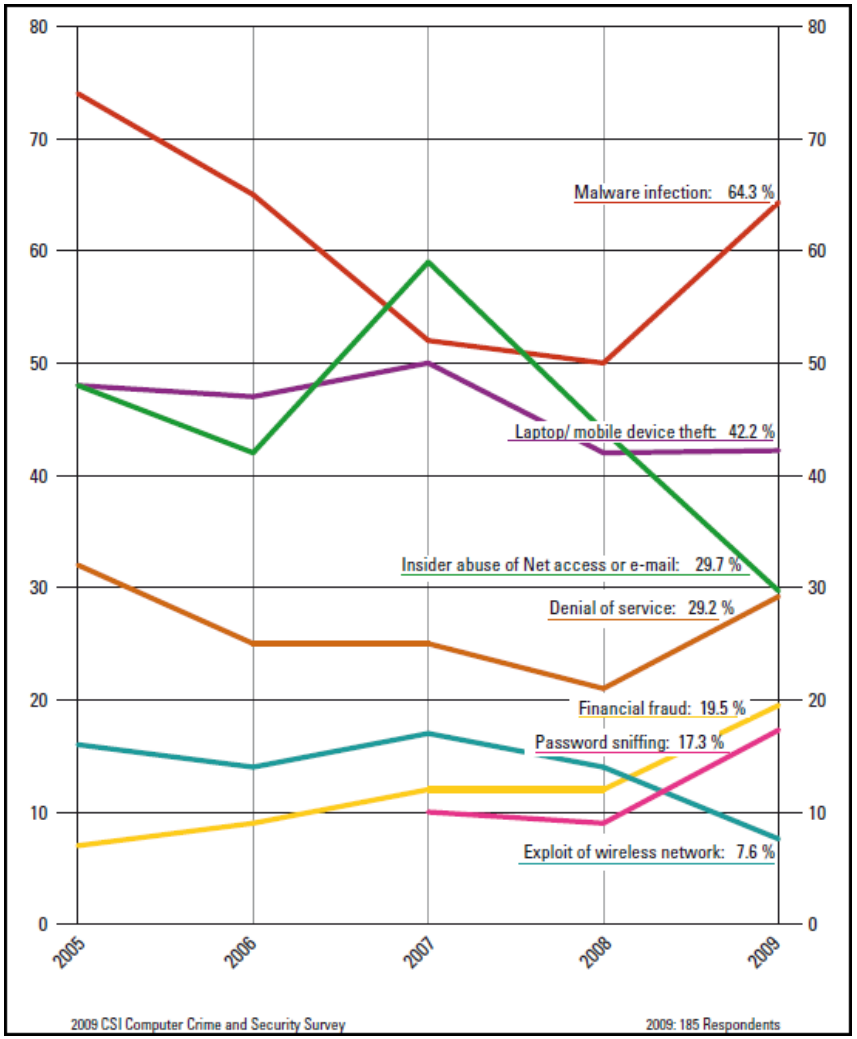

Source: CSI Report 2009

# Financial Fraud

- Financial fraud is a highly expensive attack, averaging almost $450,000 in losses, per organization that suffered fraud.
- Yet, in 2009 financial fraud is only number three on the most-expensive incident list, behind wireless exploits ($770,000) and theft of personally identifiable information ($710,000).

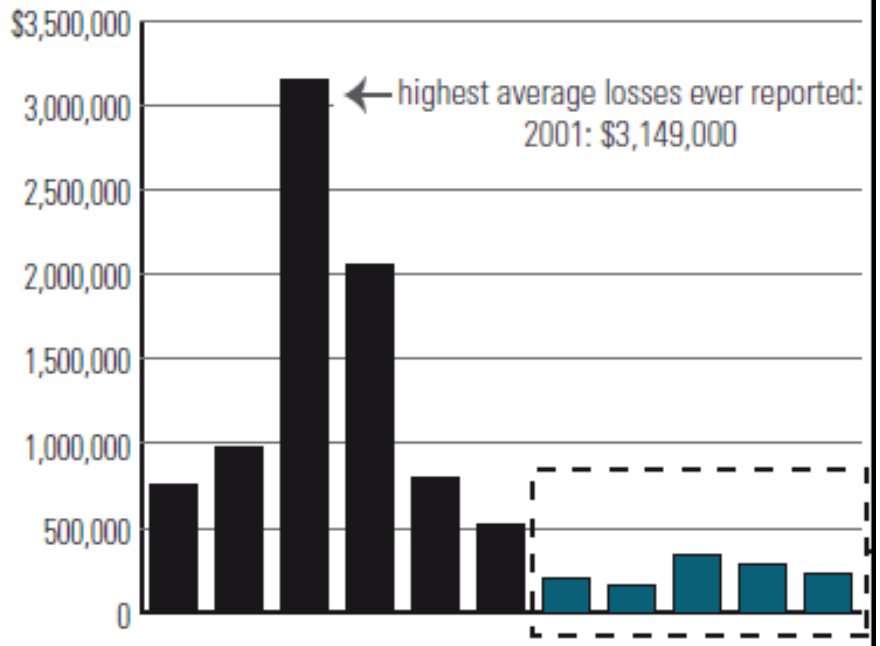
# Types of attacks experienced

- Most Frequent:
  - Malware Infection
  - Theft of laptop
- Less Frequent:
  - Exploit of wireless network
  - Password Sniffing



# Average Financial Losses (for the last decade)

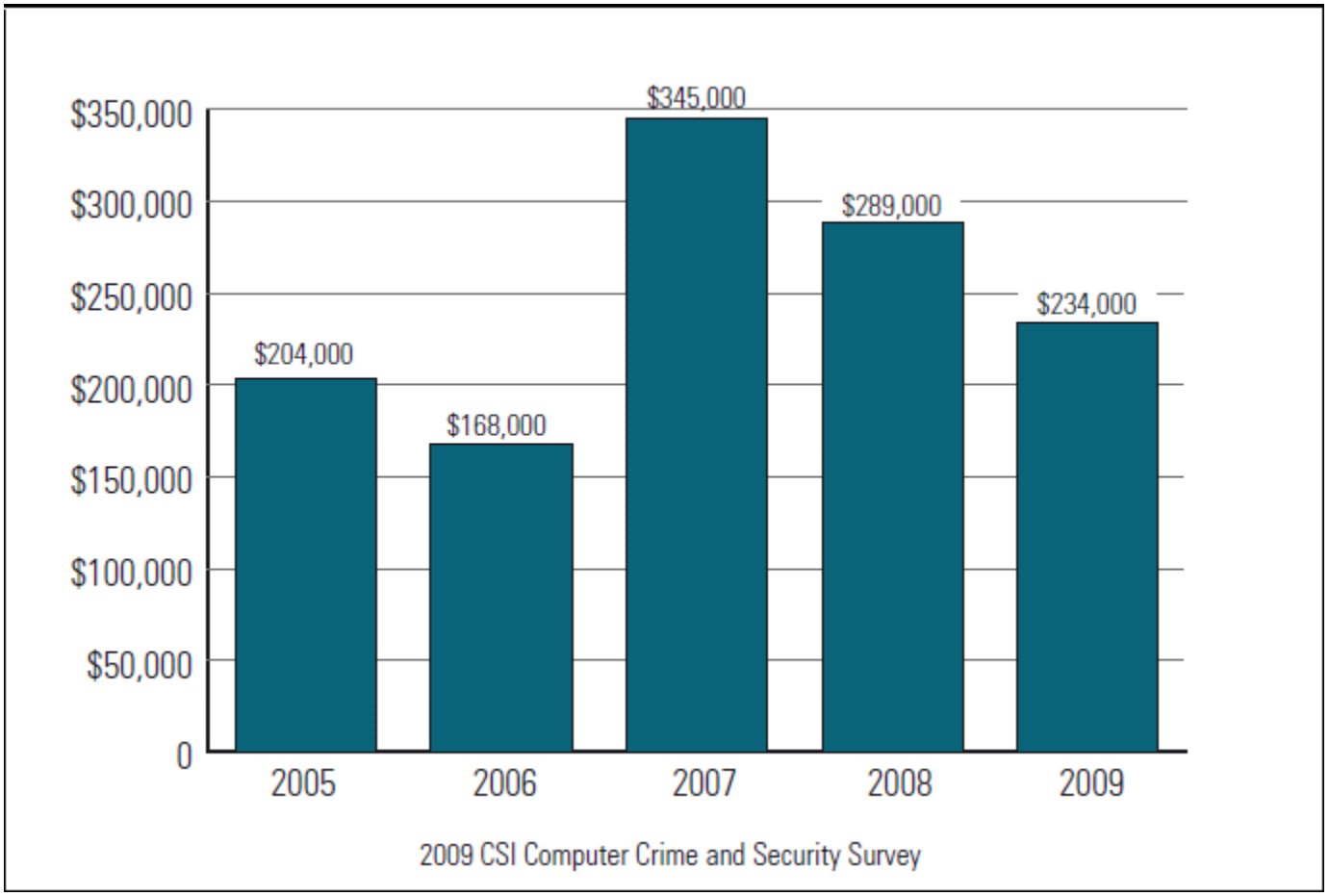
In 2005, respondents' reported losses dropped beneath the $500,000 mark. Losses haven't come anywhere near that amount, since then.




2009 CSI Computer Crime and Security Survey

2009: 102 Respondents

# Average Financial Losses (for the last five years)



# Situation in Europe (I)

- In comparison with the rest of the world, Europe reports the lowest impacts across a range of variables, from regulation and employee layoffs to supply chain.
- If true, that may be good news but it also raises the possibility that, while other regions continue to translate their concerns into even more robust security capabilities next year, Europe will continue to fall behind.

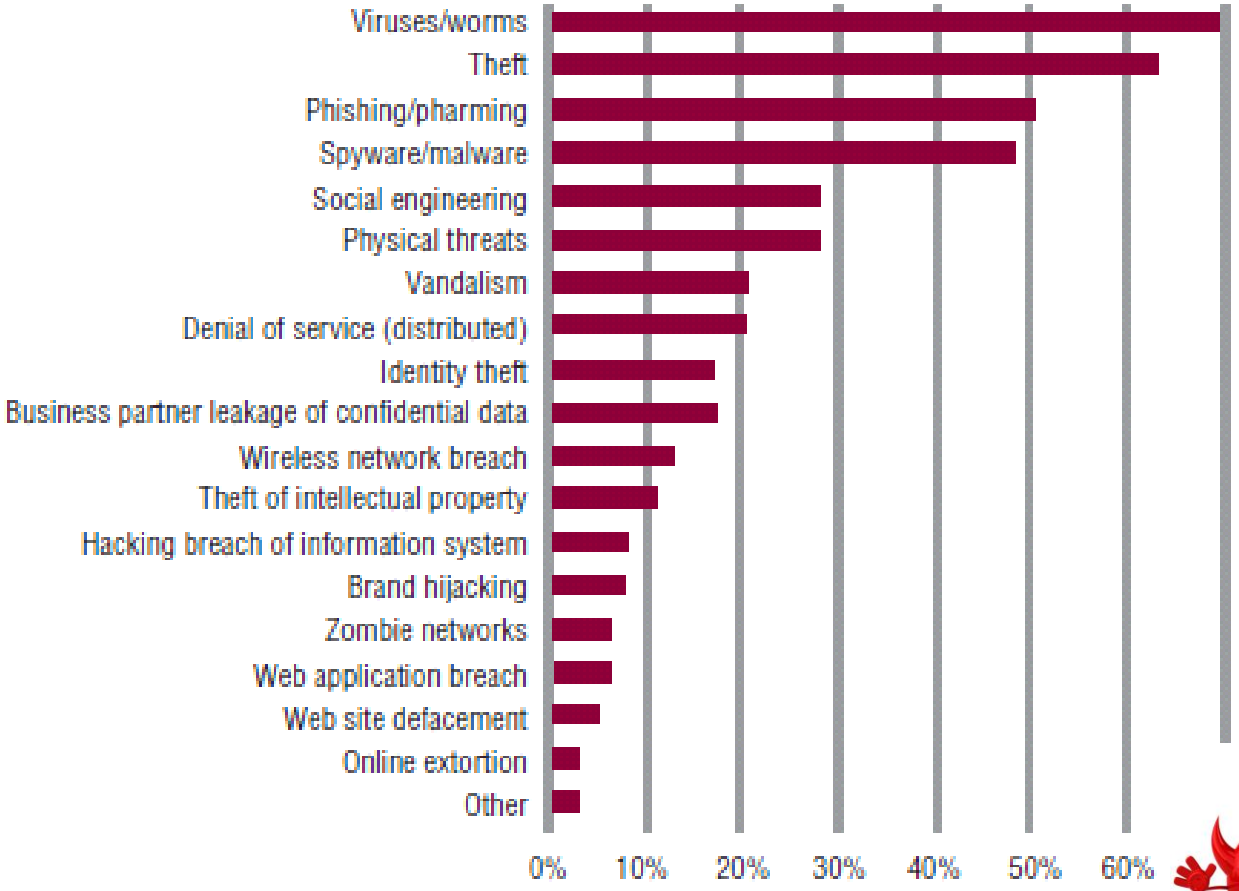
Source: PWC, Global State of Information Security Survey

# Situation in Europe (II)

- **Leadership and organisation:** Europeans report high gains in employing Chief Information Security Officers and Chief Security Officers.
- **Other security domains:** Europeans are least likely to have an identity management strategy (40% vs. 55% in North America) and to conduct threat and vulnerability assessments (39% vs. 55% in North America).
- **Compliance :** Europe trails behind North America in testing for compliance on a regular basis (39% vs. 57%).

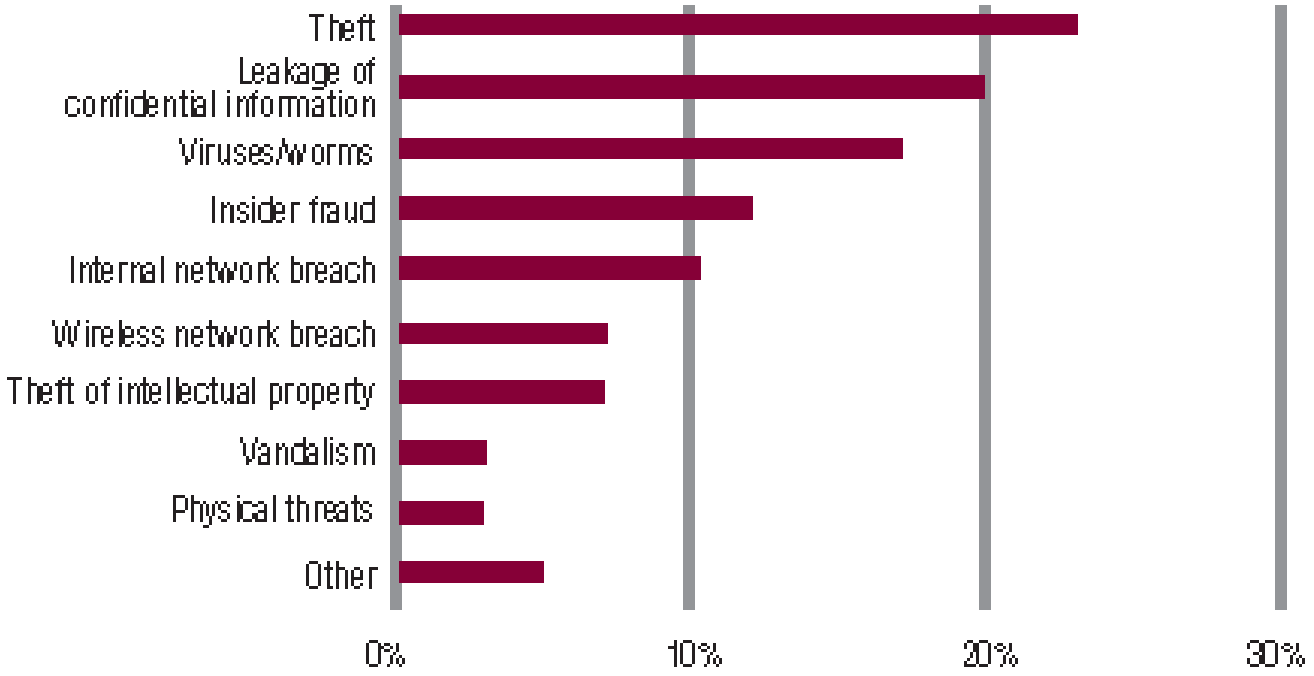
Source: PWC, Global State of Information Security Survey

# The Key External Threats




Results may not total 100 percent as respondents were allowed to select more than one answer.

# The Key Internal Threats




Results may not total 100 percent as respondents were allowed to select more than one answer.

# The Key Cost Elements

- Direct Financial Losses
- Customer attrition/decline in market share
- Brand / Reputation damage
- Legal costs
- Regulatory costs
- Audit costs
- Lost productivity
- Opportunity cost of expenditure on Security
- Cost on employee pride, morale and retention

Source: Deloitte, The Convergence of Physical and Information Security in the Context of Enterprise Risk Management

# Gaps in Economic Data

- Currently, economic data relating to information security is highly fragmented and difficult to verify.
- There are a number of global studies that provide information on key threats and trends, but the information reported is at the discretion of the provider.
- As only a few countries make security incident reporting obligatory, there is no real incentive for companies to provide such data.

- Example: The German Federal Criminal Police Office publishes only cases, no financial data.
  [http://www.bka.de/pks/pks2009/download/pks2009_imk_kurzbericht.pdf]

# Issues on Security Economics

Examining the economics of security requires an understanding of certain particularities such as:

- Political aspects
- National Sensitivity
- National Sovereignty and Defence
- High Market Competition in the ICT sector

# Data Collection & Analysis - Issues

- A significant part of current data is provided by commercial companies.
  - This may well have an influence on which data is published and how it is presented.
  - Lack of standardisation makes comparison between different reports difficult.
- Collection of data by Member States also has problems:
  - No incentive to comply for voluntary schemes.
  - Regulatory approach may be seen as 'heavy handed'.
- Consolidation of data at the European level would have to be in line with the principle of subsidiarity and respect MS wishes to keep certain data confidential.

# ENISA's Role

- The European Council resolution of December 2009 calls upon ENISA to '*Work in collaboration with Member States, the Commission and statistical bodies, on the development of a framework of statistical data on the state of Network and Information Security in Europe*'.
- As a neutral third party, ENISA is well positioned to collect data from the Member States and to analyse this data for pan-European trends.
- Article 13a of the Telecommunications Directive (2009/140/EC) already requires National Regulatory Authorities to inform ENISA about security breaches under certain conditions.

# Way Forward

- There is a clear need to continually improve the quality and quantity of data on security issues and incidents.
- Commercial reports should be supplemented by data that is collected and verified at national level.
- This data, in a suitably aggregated form, could be used to identify trends and issues at the pan-European level.
- ENISA is ideally positioned to serve Member States by collecting and analysing security data provided by Member States at the pan-European level.

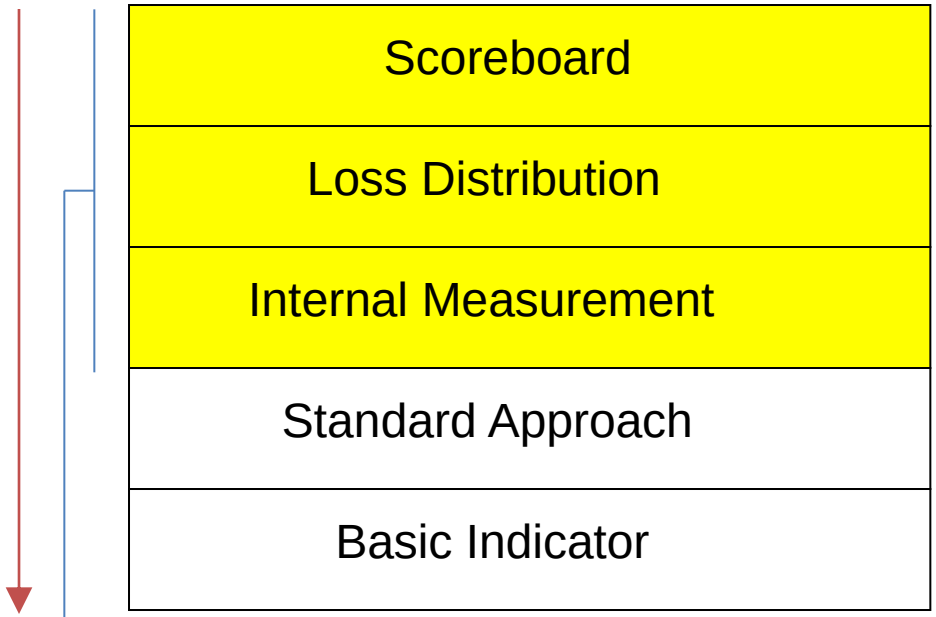
# ECONOMIC INCENTIVES & BARRIERS FOR INFORMATION SECURITY

# The Role of Regulation

- Regulations that exploit economic incentives could be a powerful way of ensuring that the private sector adopts appropriate security measures.
- The Basel II Agreement is an example of how this can be achieved in practice.
  - The basic idea is to require companies to put aside money to cover their exposure to security-related risk.
  - The more sophisticated the risk analysis carried out, the less money that has to be put aside...
- An alternative approach would be to reduce insurance premiums for companies that can demonstrate high levels of security.

# Basel II – Calculating Capital Charges

Increasing expected Capital allocation




Increasing sophistication of model

Advanced Measurement Approaches (AMA)

# Regulation versus Soft Law

- Regulation is a powerful instrument, but changing regulation takes time – it is a slow moving instrument.
- Problems and issues in information security evolve rapidly.
- Regulation is a useful instrument for resolving fundamental issues that the market cannot resolve by itself.
- Soft law and notably good practice is a good alternative to regulation in many cases – particularly when a quick response is needed.
- In general, the soft law approach is expected to be more economically efficient – it gives companies more flexibility in obtaining a reasonable trade-off between opportunity and risk.

# Underground Economy

- Malware is generated in and fuels a sizeable underground economy.
- Such illegal activities include the herding and renting out of botnets, different forms of fraud, and cybercrime.
- Some of the revenues generated in this underground economy are laundered and injected in the legal economy.

# Gray Zone

- It is not always easy to draw the line between Legal and Illegal activities.
- Malware has also spawned operations in a legally gray zone in which a legal and illegal economy overlap.
- Such semi-legal activities include spam-induced sales, bullet-proof Internet hosting, or pump and dump stock schemes.
- This mesh of legal, semi-legal and illegal activities creates mixed and even conflicting incentives for individual stakeholders. Furthermore, it complicates coherent policy responses to the problem.

# Economics of Supply Chains

- Security products are not usually designed to work in a stand-alone mode.
  - Most products run on top of an established operating system.
  - There is a cooperation between the OS and the product.
- Similarly, the people who produce the software may not be the people who install and configure it.
- In all cases, someone has to use the software.
- These are examples of supply chains.
- For the security model to work correctly, roles & responsibilities and liabilities within the supply chain need to be clearly established.

# Liability in a Global World

- The classical model of defining liability does not translate well to a globally connected environment.
  - Dependencies between actors are extremely complex.
  - Legal juristictions are aligned with national boundaries – we do not have an established Internet Law.
  - Potential losses could be enormous – the tendency will probably be to move towards Limited Liability Companies in such an environment.
- A better approach is to concentrate on defining clear roles and responsibilities and to exploit the effect that good or bad incidents have on the reputation of a supplier.

# Importance of Reputation

- Reputation has always played an important role in risk analysis and management.
  - A negative impact on the reputation of a company is often regarded as one of the most significant risks.
- This can be exploited in two ways:
  - Enterprises that follow sound security practices should be rewarded by some form of recognition – Certification Schemes are an example of this.
  - Enterprises that take undue risks should be penalised for not protecting their customers and shareholder base. In this respect, we can view Negative Publicity as an existing market mechanism.

# Vendor Push versus User Pull

- A market in which vendors take the lead is economically inefficient.
- In such a market, buyers are not sufficiently aware of their needs and cannot therefore coherently exploit product differences to obtain lower prices.
- The solution to this problem involves many steps:
  - Users need to develop a more thorough understanding of their own security requirements.
  - By forming communities with common security requirements, users can increase their economic leverage.
  - Products should be judged on what they deliver in an operational environment rather than on paper specifications.

# Sectorial Considerations

Each sector of the economy has its own peculiarities on Security

- Public Sector has better means to address Security issues
- Banks are traditionally stronger
- Telecomms are more regulated
- Healthcare involve high risks related to life or death
- SME usually lack resources to invest on Security

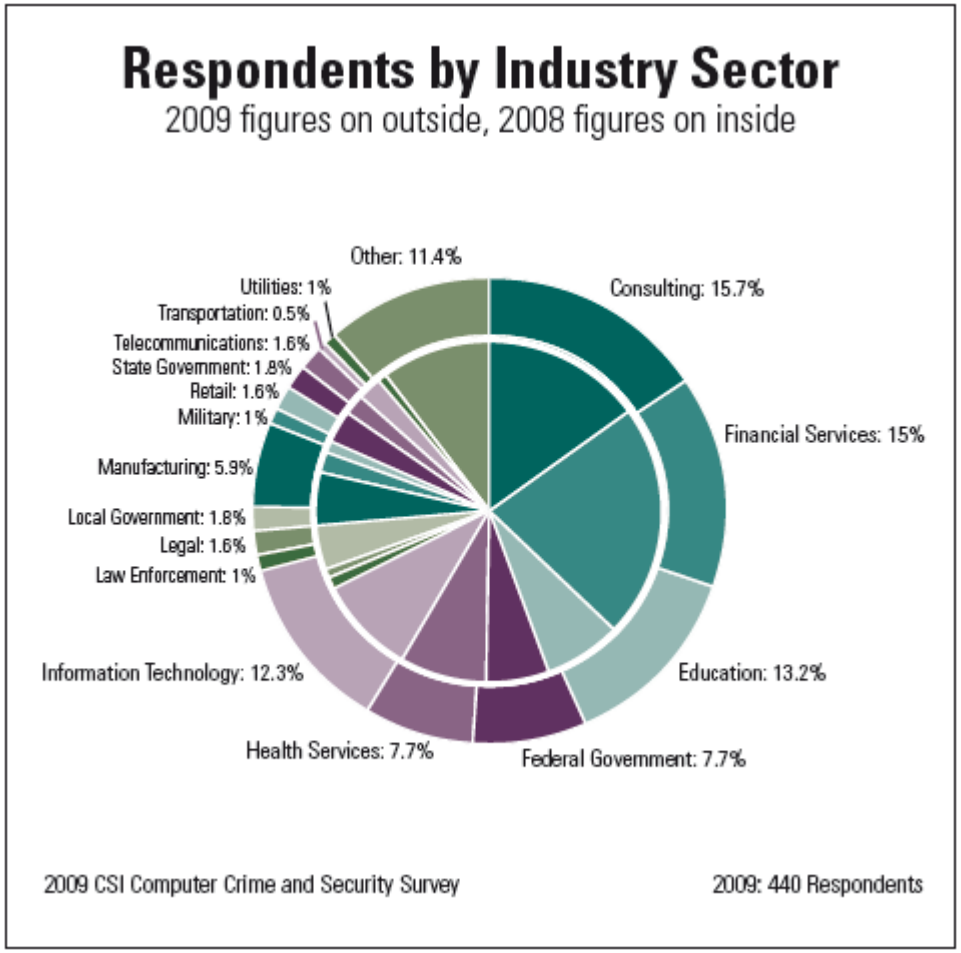
# Sectorial analysis of the 2009 CSI Report

- ★ More respondents from:

- IT sector
- Education

- ★ Less respondents from:

- Financial Services
- Health Services



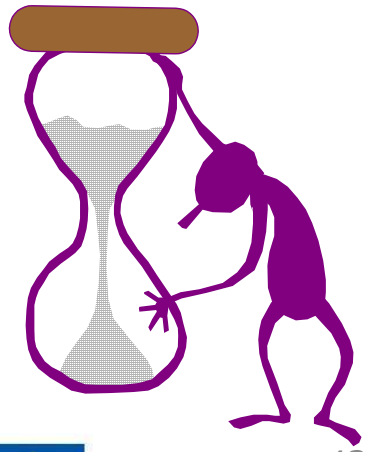
# Recommendations

- ENISA intends to study these aspects of the economics of security
- An initial work package is foreseen in the 2011 work plan
- Further activities can be deployed based on the emerging needs

# ECONOMICS OF SECURITY FOR BUSINESSES

# The Management Challenge

Modern enterprises have to secure more complex environments, faster, using less resources.



# A Risk Based Approach

- The primary objective of the information security process is to reduce information security-related risk to an acceptable level.
- Individual organisations have the right to define the level of risk that they are prepared to accept, as long as legal and regulatory requirements are respected.
- By focussing on opportunity and risk, enterprises retain the possibility to take account of contextual information when taking security-related decisions.
- The key to implementing a successful approach to information security within the enterprise is to ensure that this approach is economically viable.

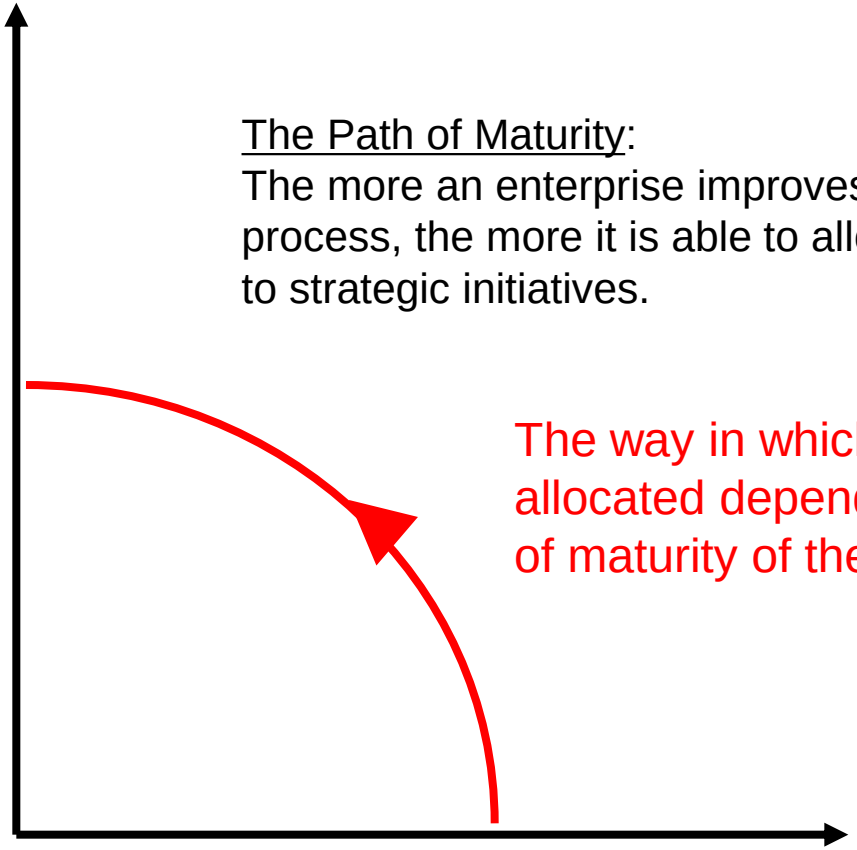
# Using Resources Effectively

- We need an approach that will allow us to react rapidly to satisfy punctual requirements without sacrificing strategic initiatives.
- The policy, standards and operational procedures collectively constitute the control framework. Strategic initiatives aim to improve this framework.
- Tactical initiatives require decisions to be made quickly and are best supported by Fast Risk Analysis (FRA) techniques.
- The optimal approach to security is a division of resources between these two tasks that reflects the level of maturity of the enterprise.

# A Proactive Approach

Strategic Initiatives

Contribute to Long-term stability.



The Path of Maturity:
The more an enterprise improves its control process, the more it is able to allocate resources to strategic initiatives.

The way in which resources are allocated depends on the level of maturity of the current process.

Tactical Initiatives

Establishes confidence and
Responds to short-term requirements

# Return on Investment

- ROI is usually used to refer to measures of how effectively capital is being used to generate profit.
- Detailed technical definitions of ROI vary considerably and tend to reflect the requirements of the target audience.
  - Investorwords.com provides a definition of ROI in terms of income, stock equity and long-term debt.
  - The Whatis?.com definition is phrased in terms of use of money, profit and cost saving.
- The problem with using classical definitions such as these in the area of information security is that they take insufficient account of risk.

# The TROI Formula

- We would like to be able to calculate a value for the ROI of an initiative that includes the risk component in addition to financial gains and losses.
- If we call this the Total Return On Investment (TROI), then:

$$\text{Total Return On Investment} = \frac{\text{Generated Revenue} + \text{Generated Cost Savings} - \text{Value of Change in Risk}}{\text{Investment}}$$

In reality, this would be expressed in terms of financial metrics such as Net Present Value (NPV) and Internal Rate of return (IRR).

# Measuring ROI

- Commonly used methods for measuring the ROI of security-related initiatives include Annual Loss Expectancy (ALE) and Cost-Benefit Analysis (CBA).
- Both methods involve considerable analysis and their effectiveness is often limited by a lack of empirical data.
- Neither of these methods measures risk directly.
- In general, there is  no standard method of measuring Value of Change in Risk, as used in the preceding formula.

# ROI: Malicious Code Protection

| Investment: | | k€ | k€ |
|---|---|---|---|
| Various software licences | @ 30 k € year$^{-1}$ = | 150 | |
| Hardware costs | = | 200 | |
| Yearly HW maintenance costs * 5 | = | 135 | |
| Staff & service provider costs | = | 400 | |
| | | | 885 |
| Generated revenue | | | 0 |
| Generated cost savings | | | 0 |
| | | | 885 |
| Value of change in risk: | | | |
| Estimated average yearly cost Of virus infections * 5 | = | 5 000 | |

You need to have this data, or to estimate it from global statistics!

Gross underestimate:
No. days downtime * turnover day$^{-1}$

Doesn't take account of claims etc., but still gives positive ROI

TROI = 0 + 0 – (– 5000) / 885 = 5,64.

# Problems With ROI Driven Approaches

- If you badly needed to have brain surgery, would you calculate the ROI of the operation?
- ROI calculations can sometimes be a useful way of justifying an initiative, but should be used carefully.
- Methods of calculating ROI involving risk are difficult to perform and may put the emphasis on the wrong aspects of the problem.

# Other Methods of Investment Appraisal

- **NPV**: **N**et **P**resent **V**alue

  - Calculates the present value of an investment decision in monetary value

  Advantage: It calculates the actual additional wealth

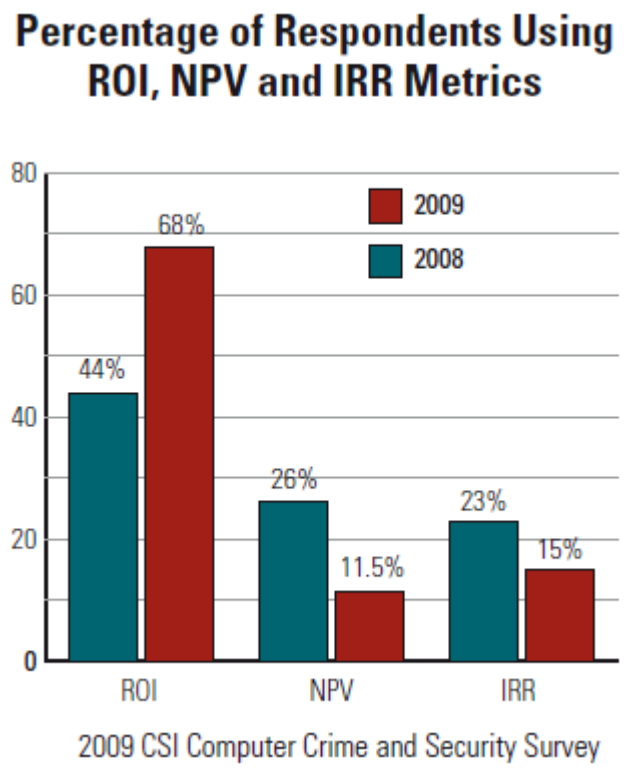
- **IRR**: **I**nternal **R**ate of **R**eturn

  - Calculates the return of an investment decision in the form of percentage

  Advantage: Easier understood by managers

# ROI Preferred Security Metric

- More and more companies use ROI as the most appropriate security metric
- NPV and IRR are seen as less relevant security metrics



# ROSI: Return on Security Investment

- A specialised method used by IT management to measure the value of a security solution is Return on Security Investment (ROSI)

$$ROSI = \frac{(\text{Risk Exposure} \bullet \%\ \text{Risk Mitigated}) - \text{Solution Cost}}{\text{Solution Cost}}$$

Risk Exposure = cost in damages and lost productivity per year

%Risk Mitigated = % of malware detected and resolved

Solution Cost = cost for implementing security tools

# Conclusions

# Key Points

- The more Information Society gets into our daily life, the more Network and Information Security is becoming a crucial success factor for individuals and organisations.
- There is a clear need to continually improve the quality and quantity of data on security issues, incidents and financial impacts.
- IT-security must be seen as a competitive advantage (instead of a cost factor) and a common model for ROSI has to developed
- Enterprises and public institutions can improve the economic efficiency of their approach to information security
- Build in IT-security by design

# ENISA's Role

- ENISA can assist enterprises and public institutions getting a better understanding of the economic aspects of Information Security by:
  - Studying new theories and methods
  - Publishing and promoting best practice guides.
  - Sharing and disseminating its expertise
  - Coordinating the work of the various actors at European level
  - Promoting a new culture on information security

# Contact

European Network and Information Security Agency

Science and Technology Park of Crete (ITE)
P.O. Box 1309
71001 Heraklion - Crete – Greece

http://www.enisa.europa.eu