How much security does an SME need?

iTEC08. 6th November 2008.

Dr Jeremy Ward. Symantec Europe.

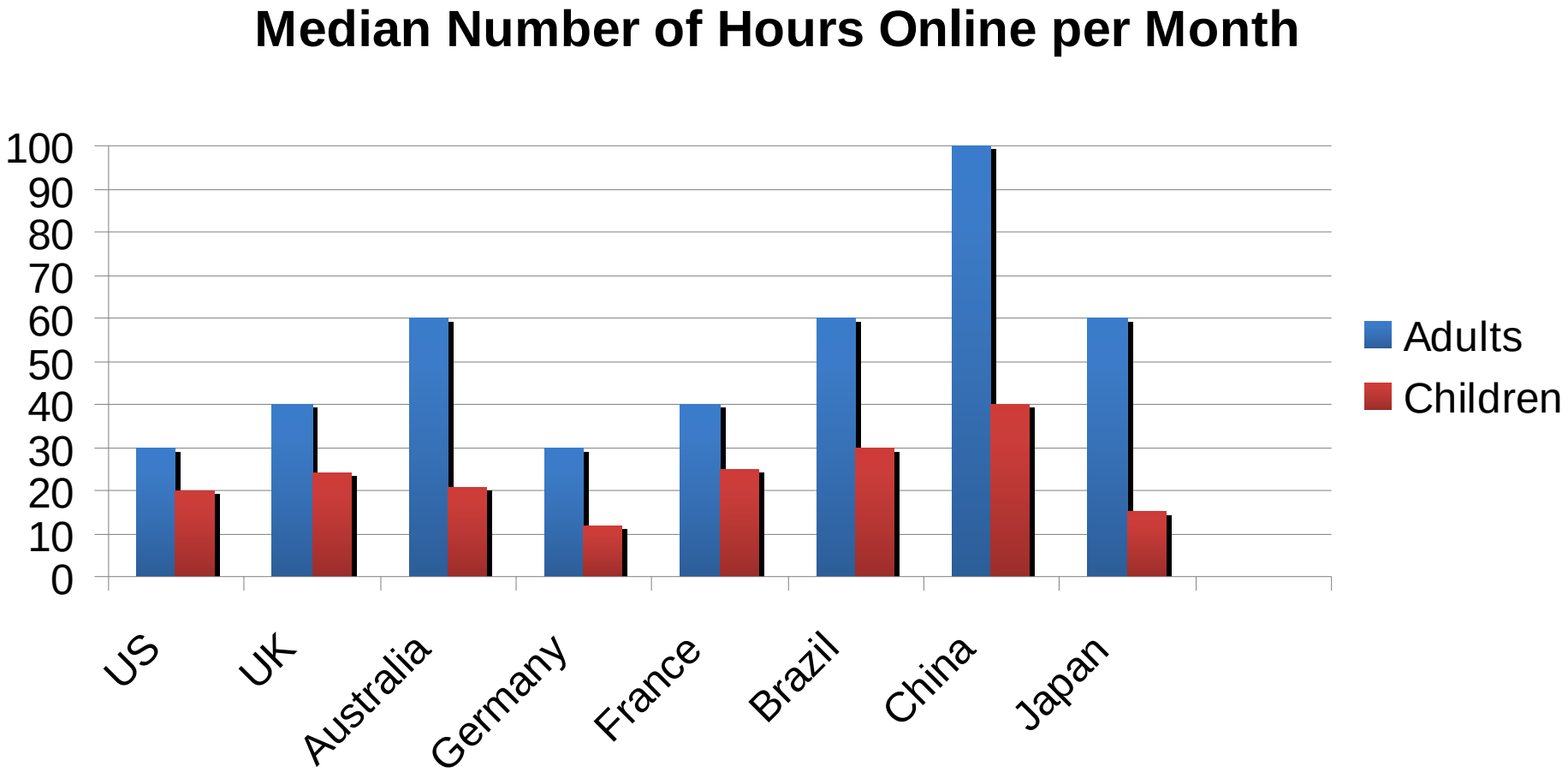
Agenda

1. The Online Security Risk
2. ENISA on Risk Assessment & Management
3. Making it work for SMEs

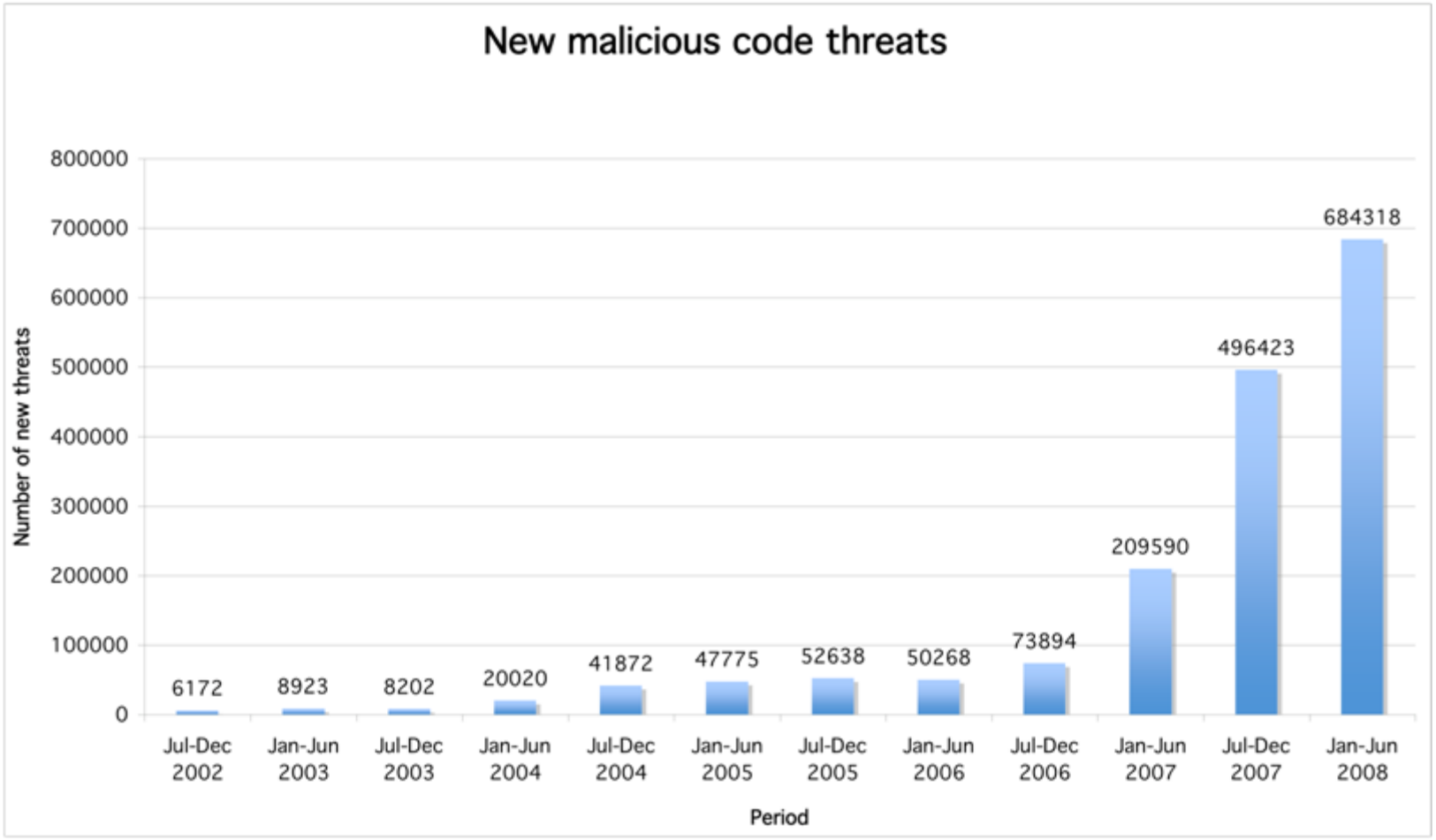
What is security risk?

- ISO 27005 definition of information security risk:
  - Potential that a given threat will exploit vulnerabilites of an asset or group of assets and thereby cause harm to the organization.
  - It is measured in terms of a combination of the likelihood of an event and its consequences.
- Risk = Threats x Vulnerabilities x Probability of Impact.

Users are the online security risk!

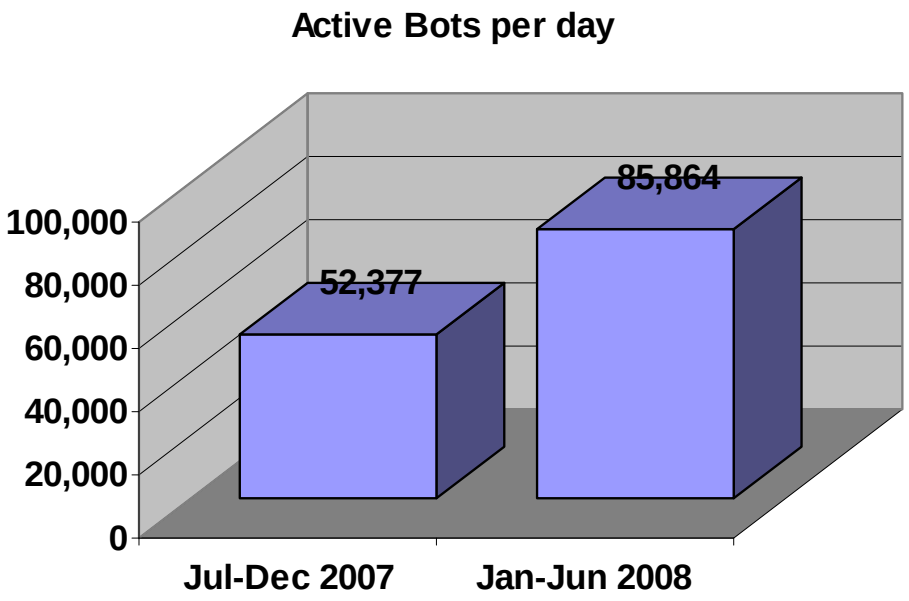


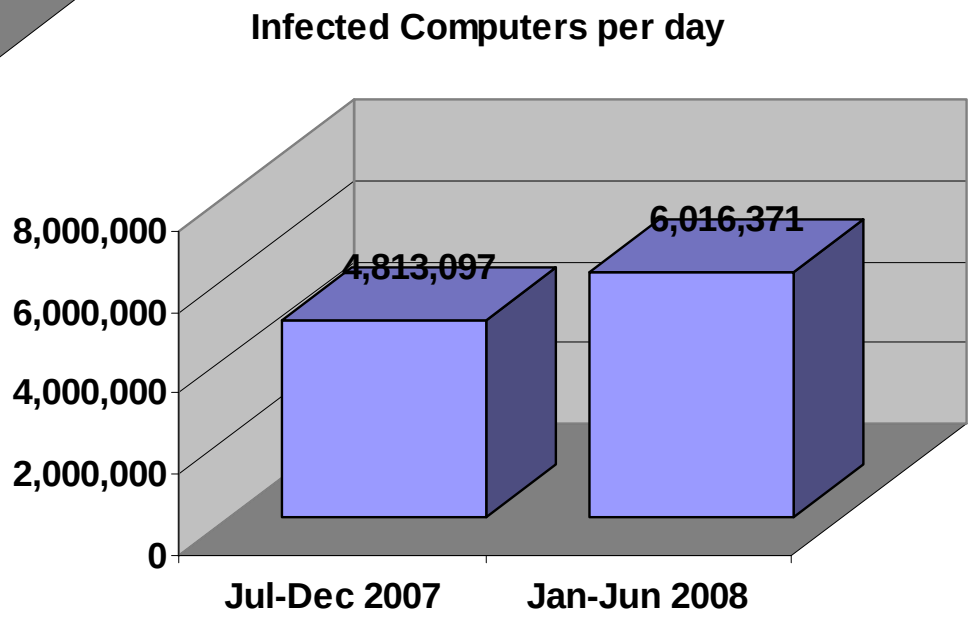
Malware threats continue to increase



Growth indicates new malware is developed by programmers employed by criminal organizations.

More Bots


Active Bots per day
100,000
80,000
60,000
40,000
20,000
0
52,377
85,864
Jul-Dec 2007
Jan-Jun 2008

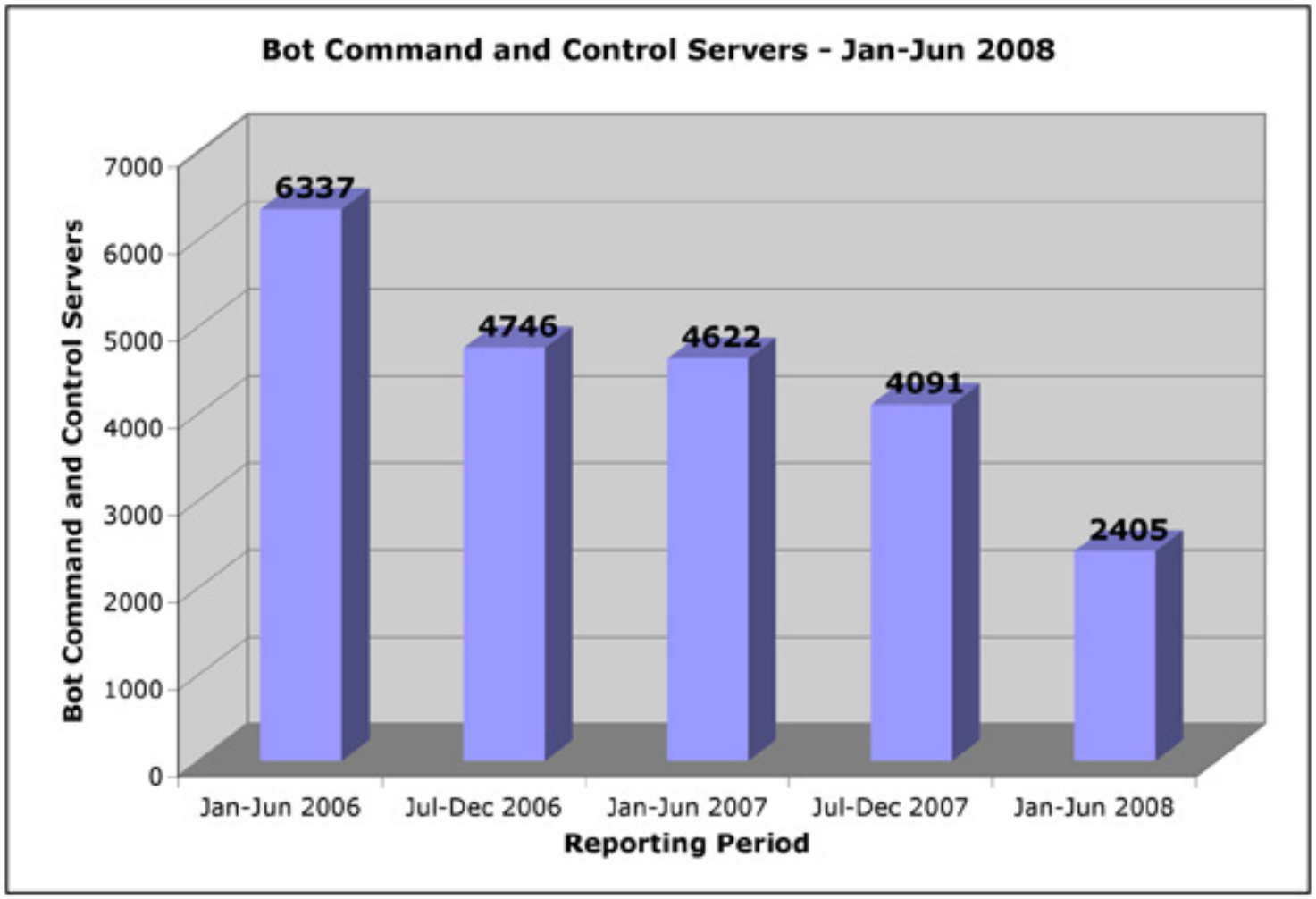

Infected Computers per day
8,000,000
6,000,000
4,000,000
2,000,000
0
4,813,097
6,016,371
Jul-Dec 2007
Jan-Jun 2008

Top 10 EU Bot Rankings

Rank	Country	Bot Numbers	% of World Bots
1	Germany	469439	10%
2	Spain	357619	7%
3	Italy	271010	6%
4	Poland	258437	5%
5	France	238223	5%
6	United Kingdom	193826	4%
7	Portugal	71903	1.5%
8	Hungary	25754	0.5%
9	Netherlands	24731	0.5%
10	Sweden	20143	0.4%
TOTAL			40%

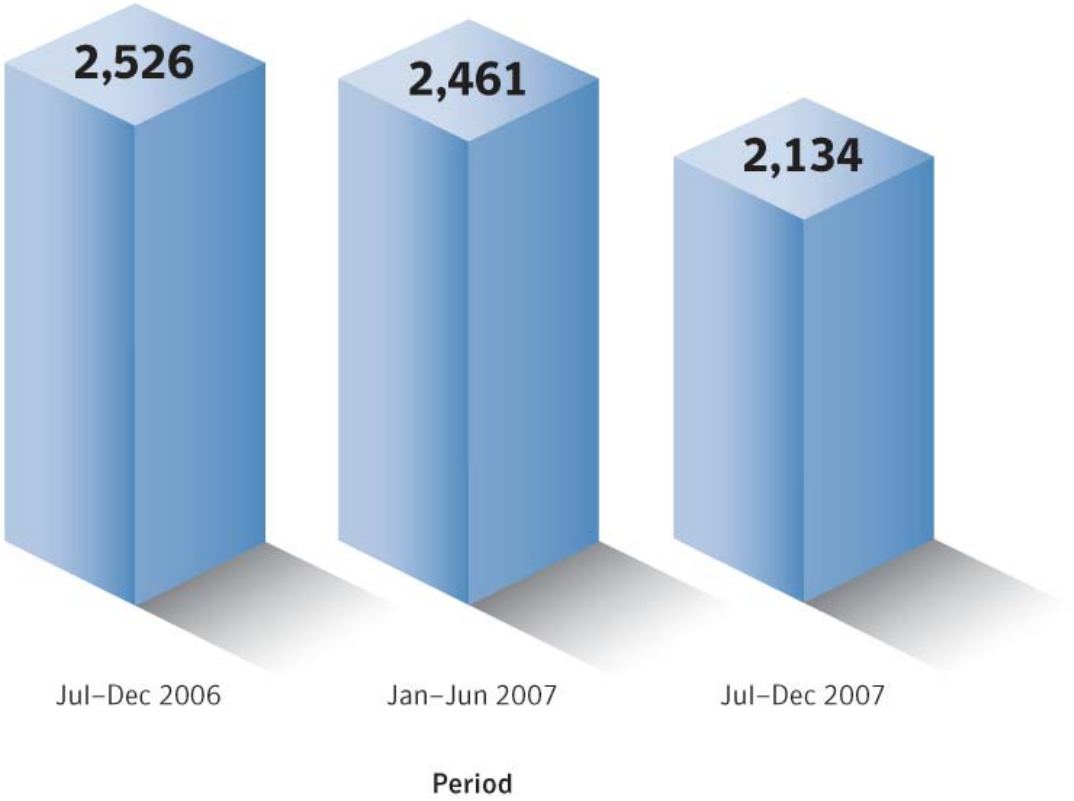
Symantec Data: September 2008

… Fewer Controllers

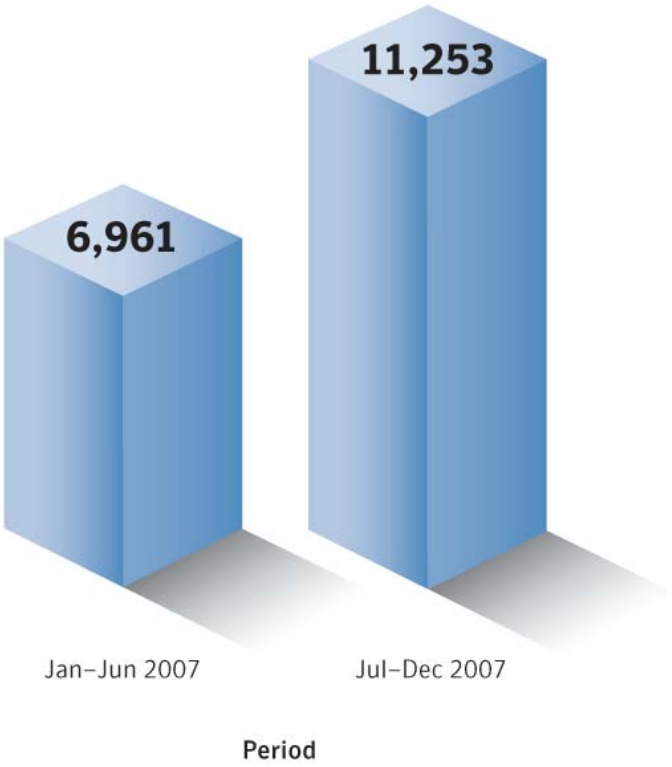


Cyber-Criminals are becoming more organized!

Websites are the focal point

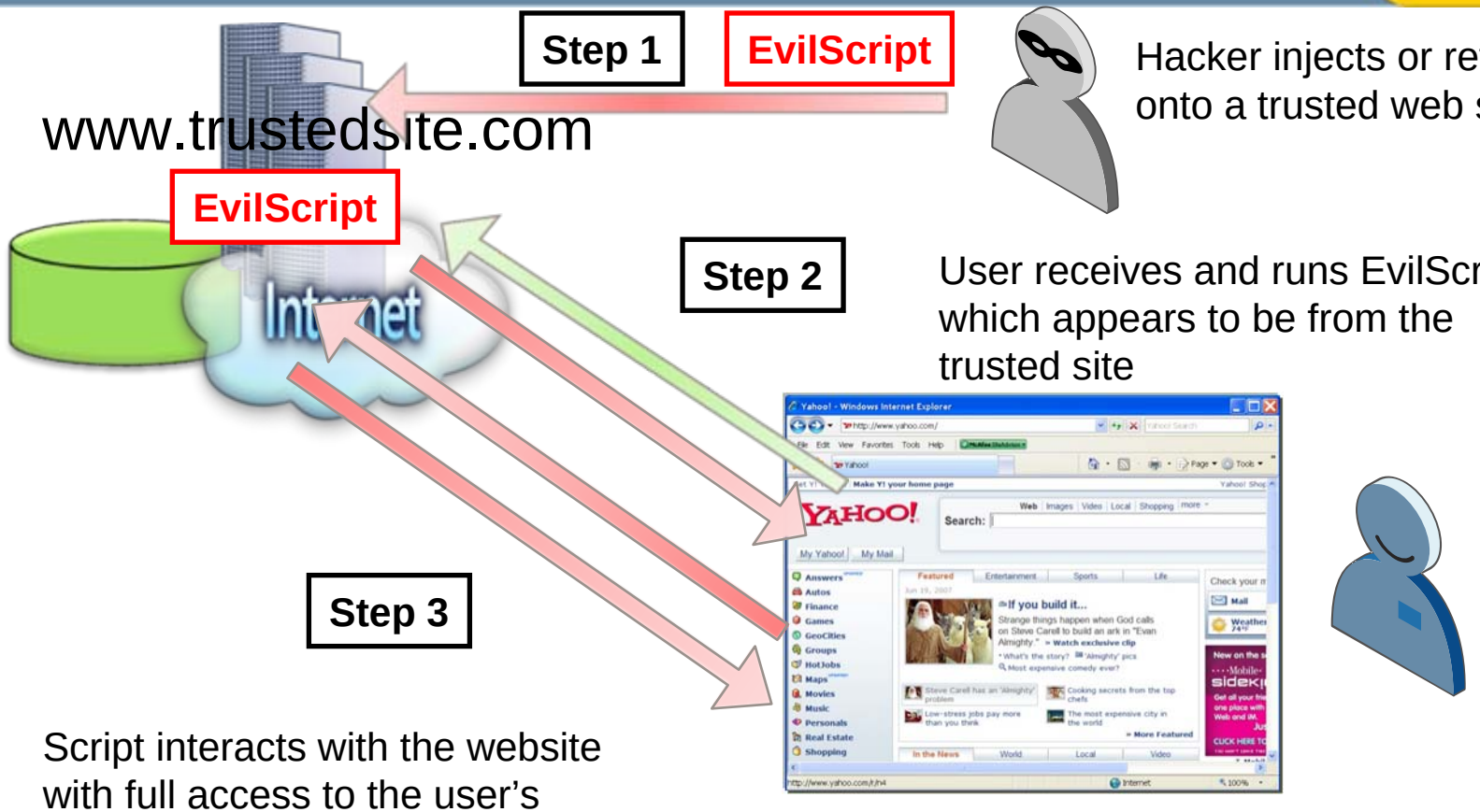


Traditional Vulnerabilities



Cross-Site Scripting

How cross-site scripting works



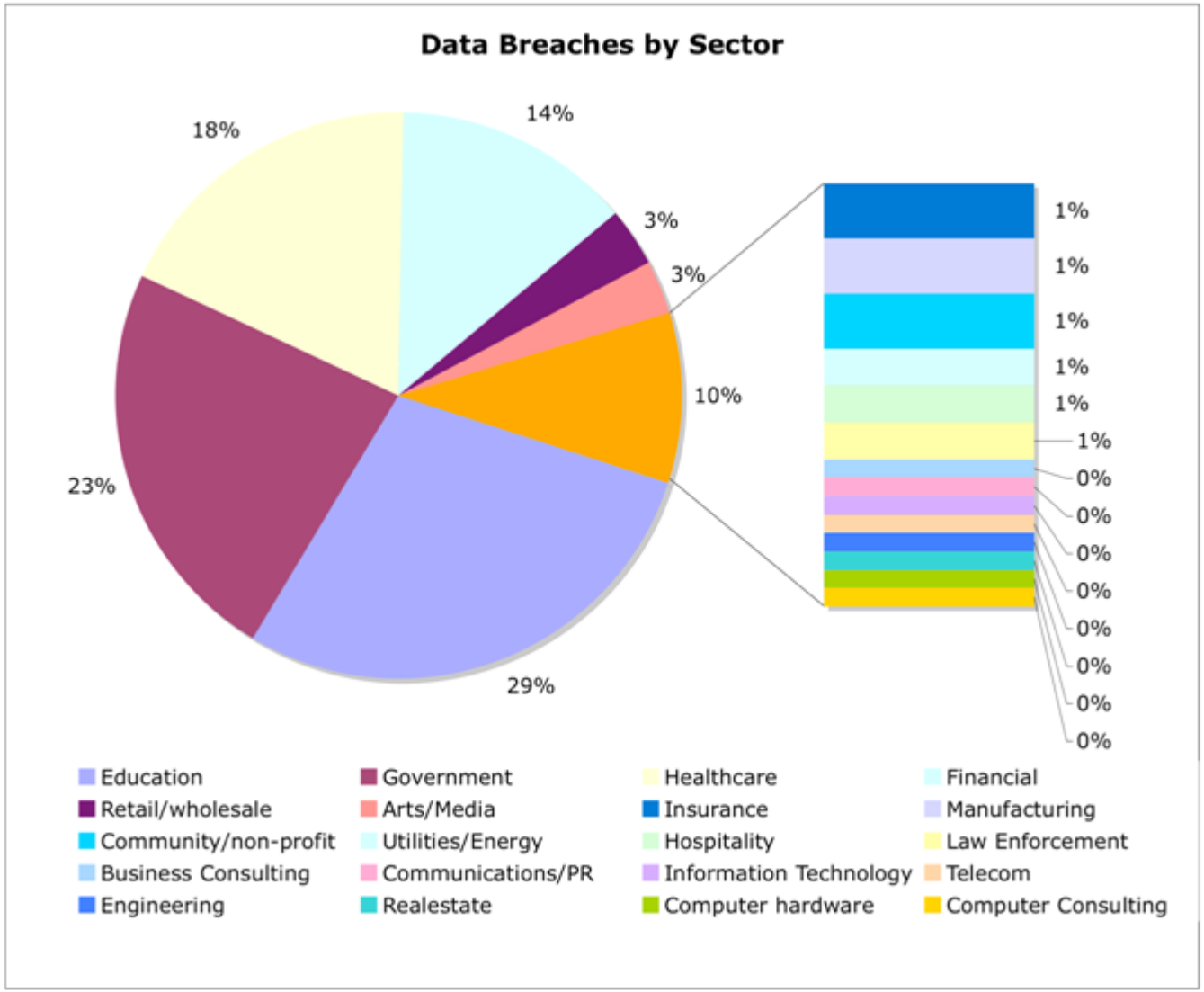
Hacker injects or reflects a script onto a trusted web site

User receives and runs EvilScript, which appears to be from the trusted site

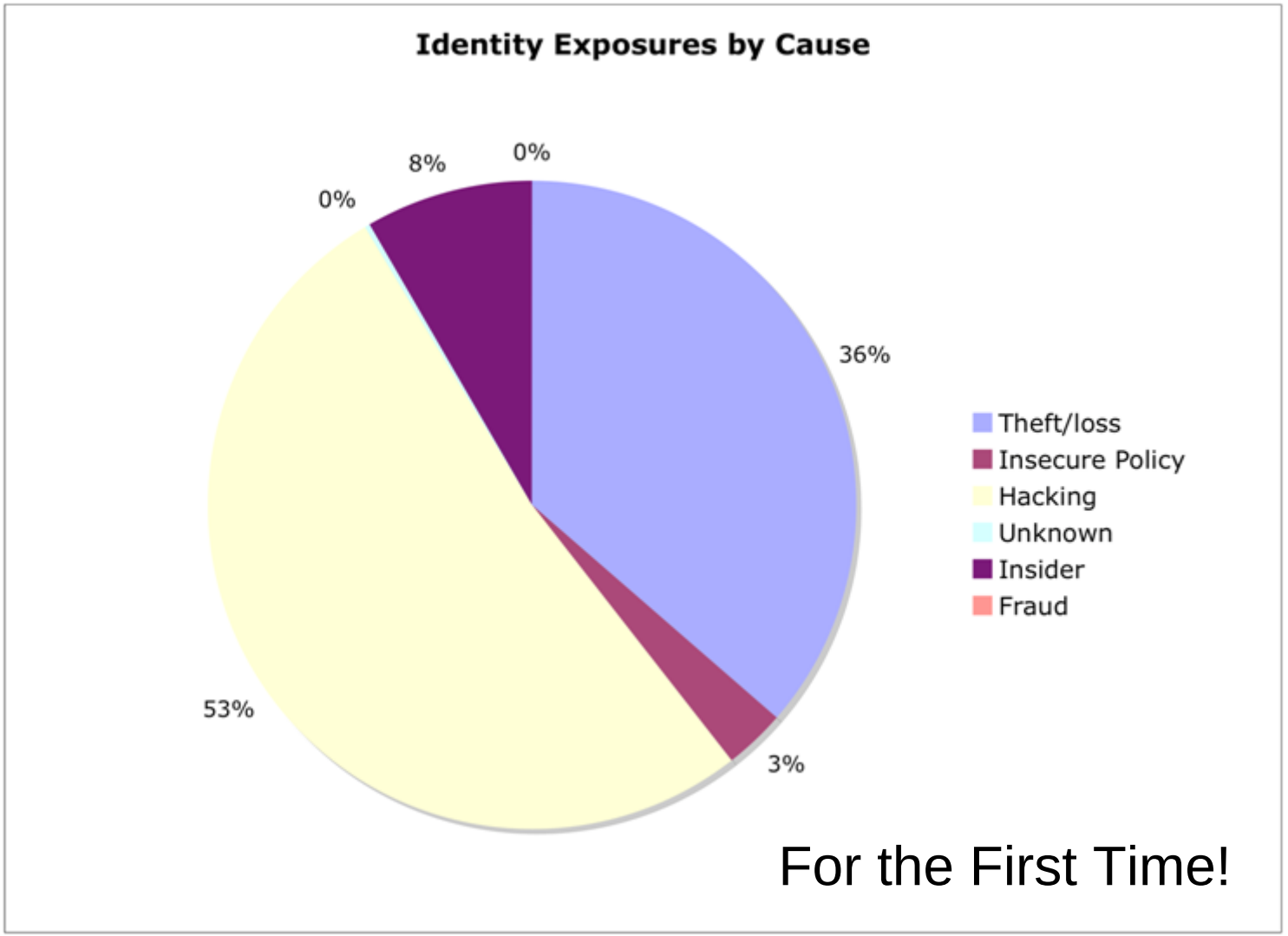
Script interacts with the website with full access to the user's cookies, authentication, etc

Blocking any of these steps stops the attack

Data Breaches Jan-Jun 2008



Hacking Causes Most Exposure



For the First Time!

Agenda

2 ENISA on Risk Assessment & Management

ENISA and Information Security Risk

- European Network and Information Security Agency:
  - Centre of excellence
  - Best practice exchange
  - Government/industry cooperation
- Management Board (from EU Governments)
- Permanent Stakeholders Group (expert group)
- Working Group on Risk Assessment and Management http://www.enisa.europa.eu/rmra/h_home.html

ENISA Risk Assessment/ Management

Address http://www.enisa.europa.eu/rmra/h_home.html Go

European Network and Information Security Agency

Home | Current Risks | Emerging Risks | RM & Regulation | Integrated RMRA

Sitemap | Legal Notice

Search

this section site

- Home
- Announcements
- Working Group
- Events
- Contact us

Home

Risk Management / Risk Assessment

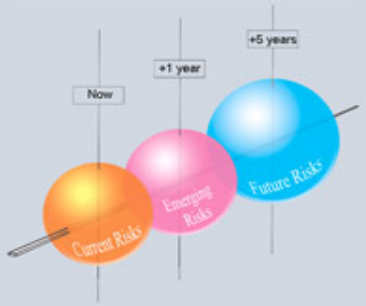
The present site is the central hub of information about Risk Management / Risk Assessment developed and maintained by ENISA.

This site encompasses a variety of information pertinent to Risk Management and Risk Assessment but it also gives information about activities and events in that area.

Target group of this content are all kinds of users (e.g. experts and non experts) who are interested to learn more about Risk Management, to get informed about current development and trends in that area or to apply existing Risk Management practices to their organization.

Numerous issues in the area of Risk Management addressed through the ENISA work Programmes will be gradually integrated into this site, such as:

- Inventories of methods tools and good practices
- Achieved results in the area of Emerging Risks
- Information material for Small and Medium Enterprises (SMEs)
- Comparability and interoperability issues of methods, tools and good practices
- Integration issues of Risk Management with other operational processes



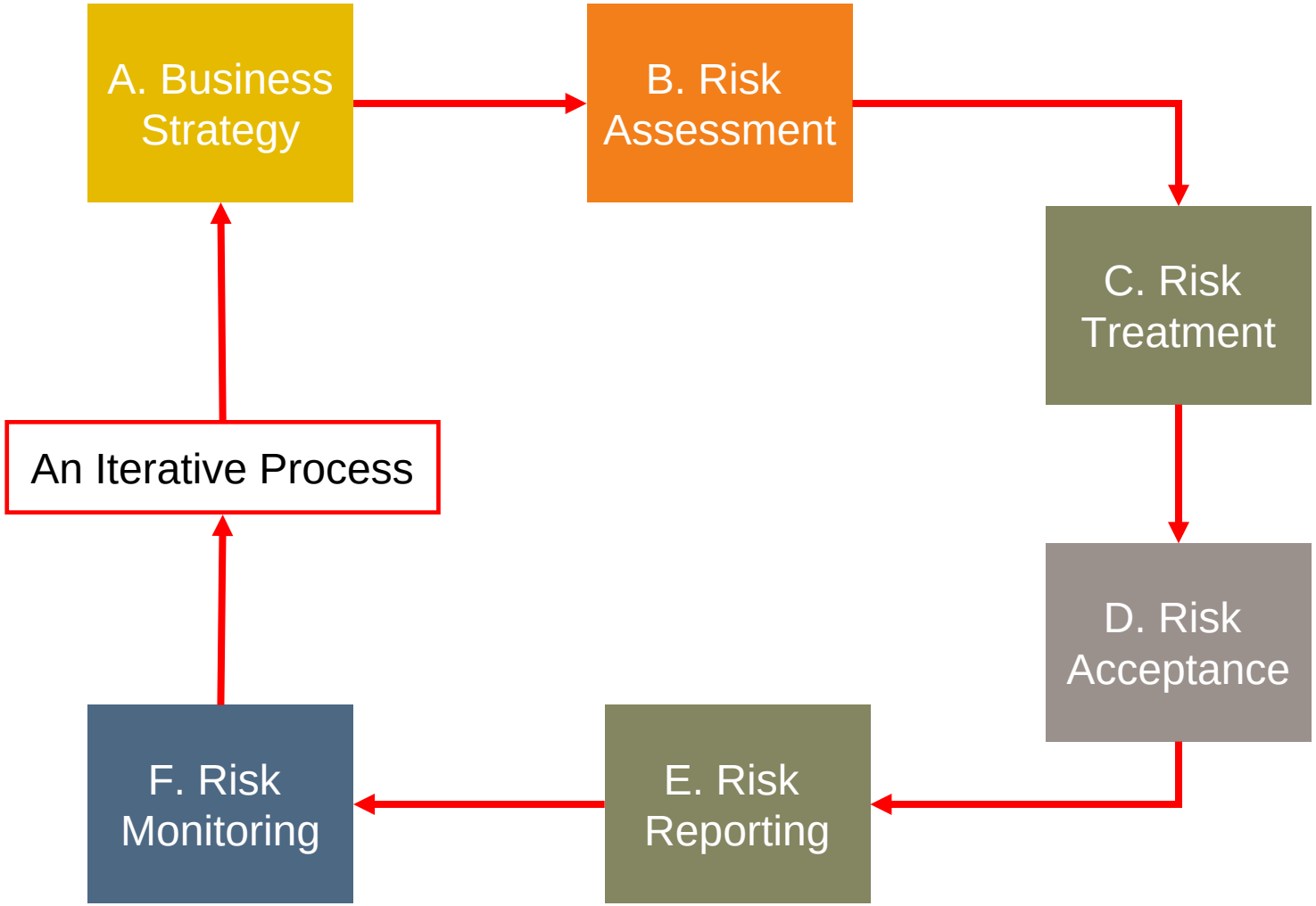
All this information will be published both by means of interlinked content and downloadable reports.

Besides this kind of information, ENISA will inform interested users about relevant events in this field, about the activities of the ENISA ad hoc Working Group on Risk Management / Risk Assessment, about relevant national and international sources of information, etc.

In the middle term, ENISA intents to develop this site to a significant collection of knowledge in the area of Risk Management / Risk Assessment for all interested European stakeholders.

01 August 2008: The tools Resolver*Risk and Resolver*Ballot have been added on the inventory of RM/RA tools. **04 June 2008:** The met

Basic Risk Management



Agenda

3 Making it work for SMEs

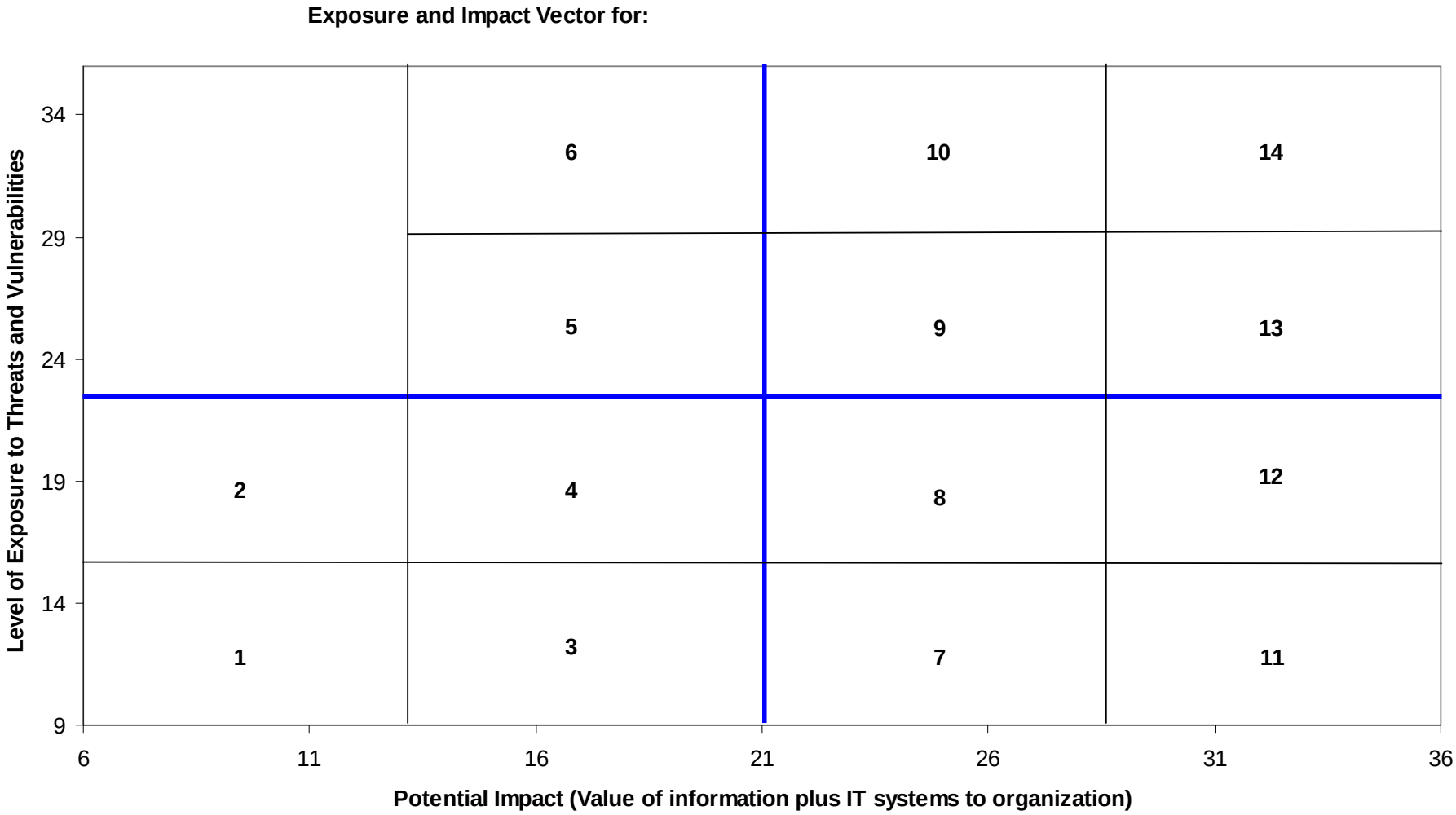
Assessing Exposure to Threats and Vulnerabilities

- Business exposure:
  - Size and complexity of the business
  - Attitude to change.
- Exposure to problems:
  - Likelihood of technical problems
  - Likelihood of problems caused by people
  - Likelihood that people have the knowledge & means to cause problems.
- Use of IT:
  - Complexity of IT systems
  - Importance of Internet to the business
  - Partner access to your network
  - Home and remote access to your network.

Assessing Potential Impact

- Importance of legal and regulatory requirements to your business.
- Value of information to your business:
  - Loss of availability
  - Loss of integrity
  - Loss of confidentiality.
- Value of IT systems to your business:
  - Importance in enabling you to achieve objectives
  - Importance of your systems to your business partners.

Plotting Level of Exposure and Impact



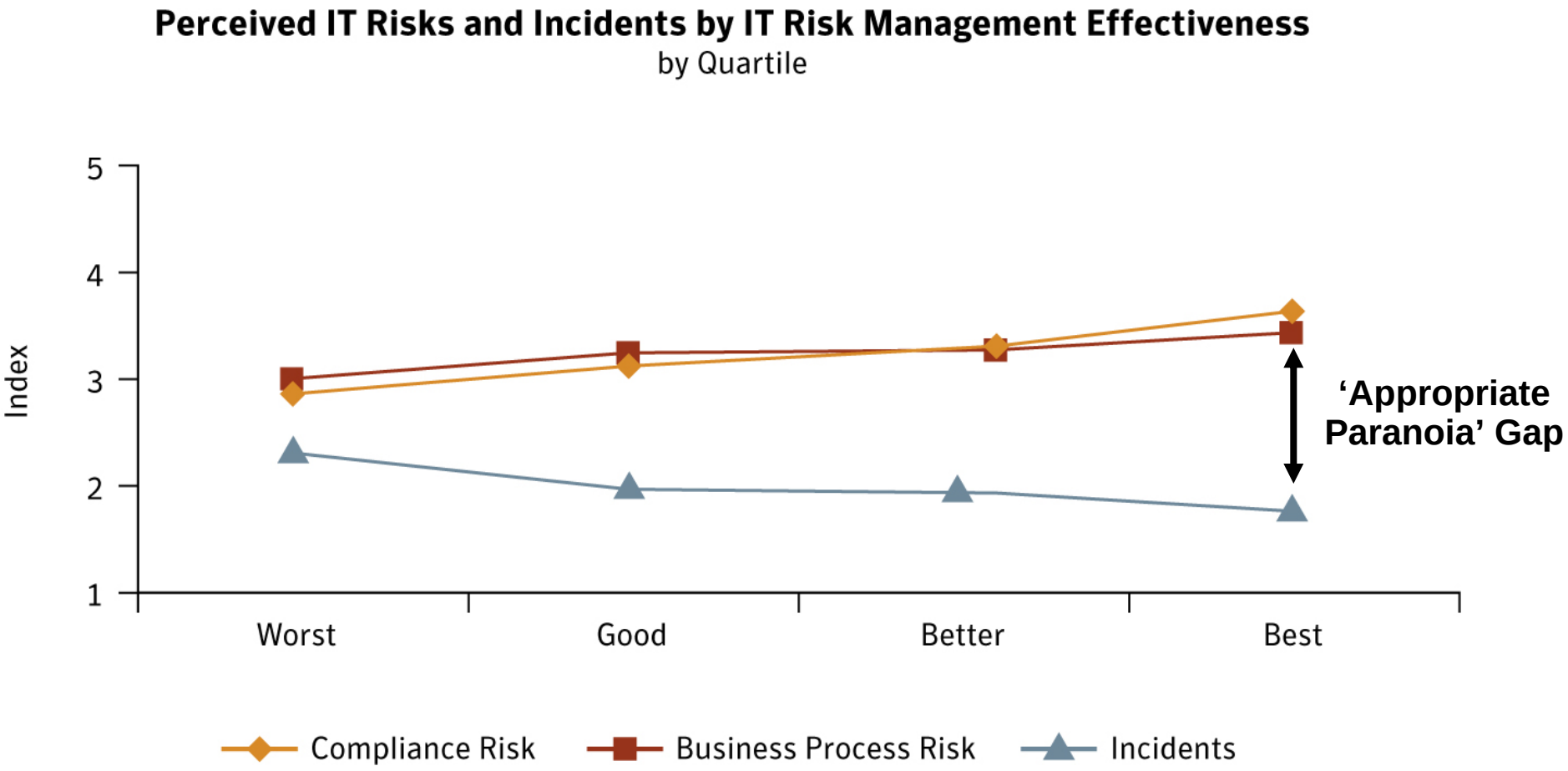
Example Approach (Level 2)

- General Information:
  - Basic understanding of risks and some investment in resources.
- Degree of Action:
  - Basic concern with a few processes, focusing on risk treatment.
- Requirements:
  - Understanding information assets.
  - Understanding stakeholders and organization.
  - Understanding risk acceptability and strategy for managing this.
  - Identifying business strategies relevant to risk management.
  - Understanding basic threats and impacts and having a simple plan to deal with these.

Example Recommendations (Level 2)

- Use basic guides to good practice and keep simple checklists.
- Coordinate and cost the actions to be taken.
- Prioritize actions to be taken.
- Assign responsibility for carrying out actions.
- Produce basic reports about the actions carried out.

Understanding leads to action



Source: Symantec IT Risk Management Report. Jan. 2008

Any questions…?

jeremy_ward@symantec.com