



Grid Security: A Business driven SWOT Analysis

September 25th, 2006



Capitalising on e-infrastructures



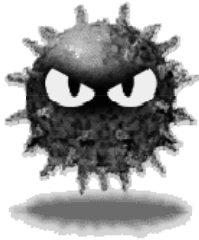
Grid Security: Today's Problems and Challenges



Question asked by the business :
How should I benefit from grid computing and share my information systems to partners and at the same time preserve sensitive data against threats : manipulation, defacement, disruption, fraud, theft, confidentiality breach?
And who should I trust?



Grid Security – Growing number of attacks



*“August 2003 reportedly has gone down as the **worst month in digital history for virus attacks.** Mi2g also notes that the Sobig virus alone accounted for **29.7 billion** of economic damages worldwide”*

*The average loss due to Denial of Service (DoS) attacks in 2003 was **\$1,427,028** , five times higher than in 2002*

Grid Security – Strengths, Weaknesses, Opportunities, Threats

*The process is called “**herding**,” and a herd of zombies is called a **botnet**. The herder then issues orders to the **zombies**, telling them to send unsolicited e-mail, steal personal information, or launch attacks. Herders also trade, rent, and sell their zombies. “The botnet is the little engine that makes the evil of the Internet work,” Chris Morrow, a senior network-security engineer at M.C.I., said. “It makes spam work. It makes identity fraud work. It makes extortion, in this case, work.”*

Grid Security – Strengths

A collaboration of Asian and European laboratories used an international Grid to analyse 300,000 possible drug components in the fight against avian flu virus H5N1. 2000 computers were used during 4 weeks in April 2006 – the equivalent of 100 years on a single computer. More than 60 000 output files with a data volume of 600 Gigabytes were created.

Virtual Grid Communities:

- *Life Sciences*
- *Physical Sciences*
- *Digital Media*
- *Manufacturing*

Grid Security – Weaknesses

- One of the challenges with end users most often citing the cultural and organizational concerns associated with resource sharing
- Liabilities, legal issues
- Management
- Potential lack of centralised controls
- Intercultural, cross-border, human factor, societal issues
- Interoperability, scalability
- Billing cycle, charging mechanism
- Data confidentiality passed over corporate grid systems
- Quality of services must always be available even if the presence of faults in the system. QoS vs cost of a compromised trustworthiness

Grid Security – Opportunities (... negative)

Botnet master jailed for five years - A California man has been jailed for almost five years for running a zombie network of compromised PCs.

J.J.A, 21, of Downey, California, used the botnets he controlled to display cash-generating adverts and as a resource he "rented" for hackers and spammers to run either denial of service attacks or junk mail campaigns.

His network of thousands of zombie computers included machines at the Weapons Division of the US Naval Air Warfare Centre in China Lake, California, as well as other US Department of Defense PCs.

Although he sold access to compromised machines through an IRC channel named "botz4sale", Ancheta's principal revenue source came from installing adware on compromised systems, a business that earned him \$60,000 and financed the purchase of a top-of-the-range BMW car along with a bank of computer servers.

For his pains, Ancheta was sentenced on Monday to 57 months imprisonment after earlier pleading guilty to conspiring to violate the Computer Fraud Abuse Act, conspiring to violate the CAN SPAM Act, causing damage to federally protected defence computers, and accessing protected computers without authorisation to commit fraud.

Grid Security – Opportunities

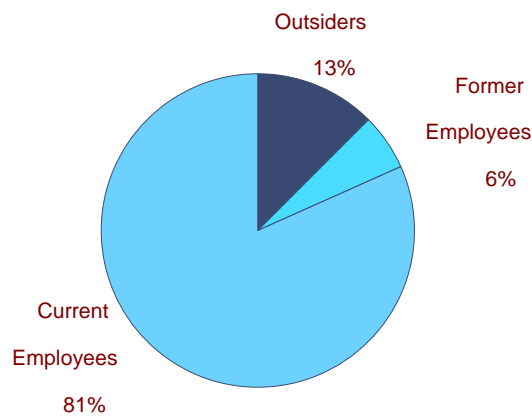
- Estimated to exceed US\$12 billion in revenue opportunity by 2007
Transforms the way users access and share information with virtual resources
- Enabler for complex research initiatives
- Allows running mission critical business applications
- *Pay-Per-Use, Use-On-demand* schemes
- Provides opportunities to reduce costs and increase revenues by making on-demand CPU power and on-demand storage services, *utility computing*
- Technology opportunities: crypto, authentication, authorisation, encryption, firewall, event management, ...
- Proof of concept

Grid Security – Threats

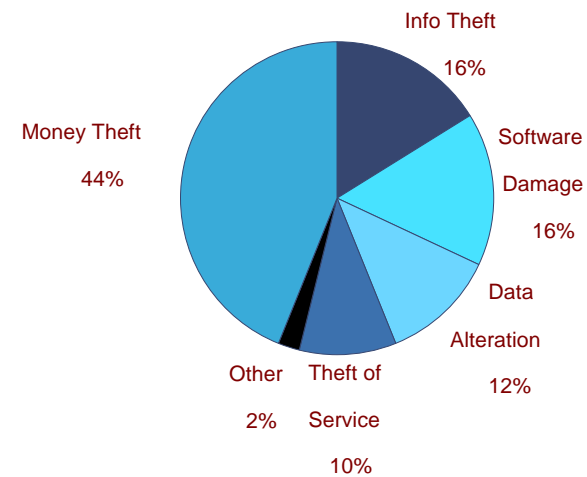
- Abuse
- Misuse
- Inappropriate management
- Loss of confidentiality / privacy
- Inappropriate data classification
- Wrong distribution of data storage capability
- Wrong deployment of data computing resources capability

Today Computer Crimes

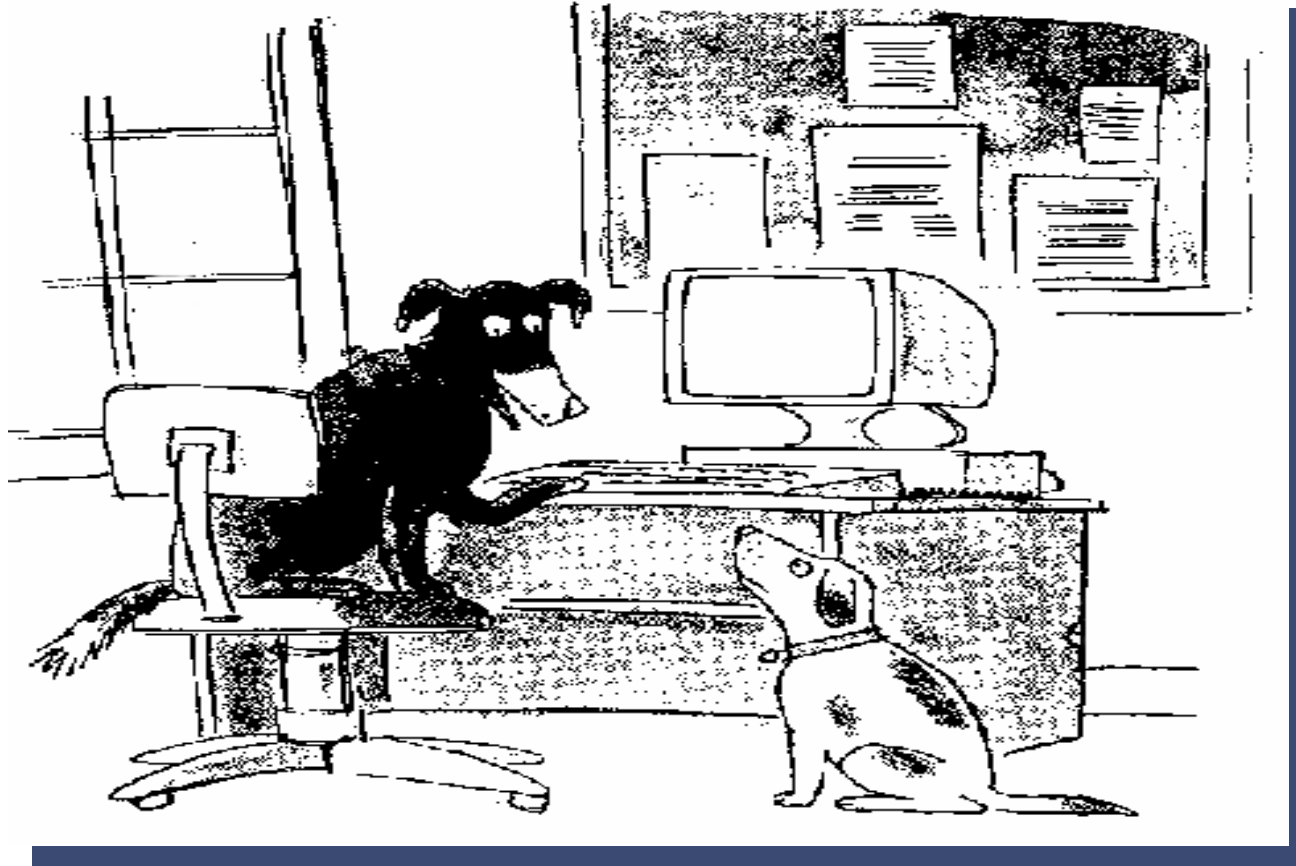
Who is the “enemy”?



And what are their crimes?

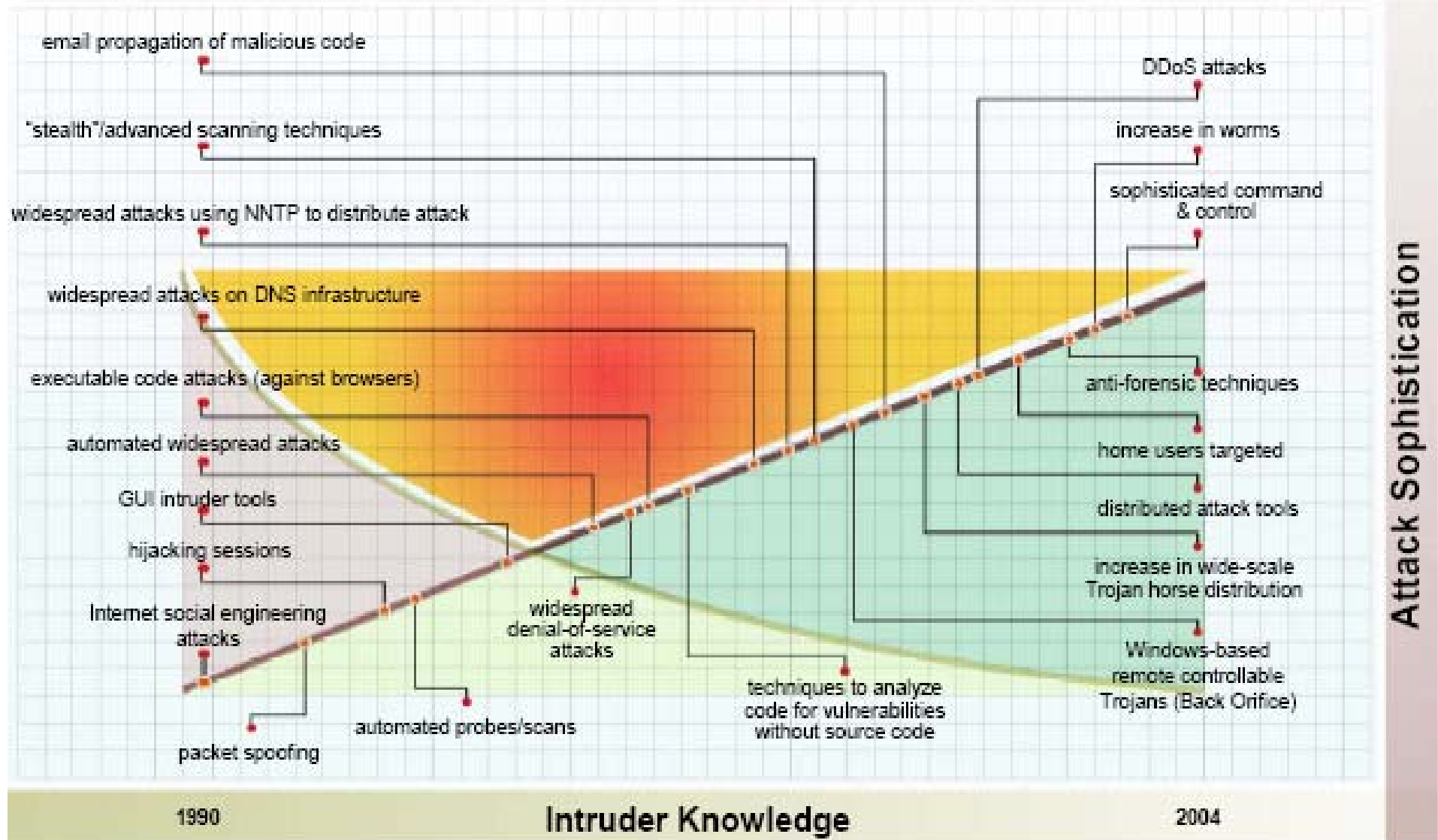


Grid Security – Threats

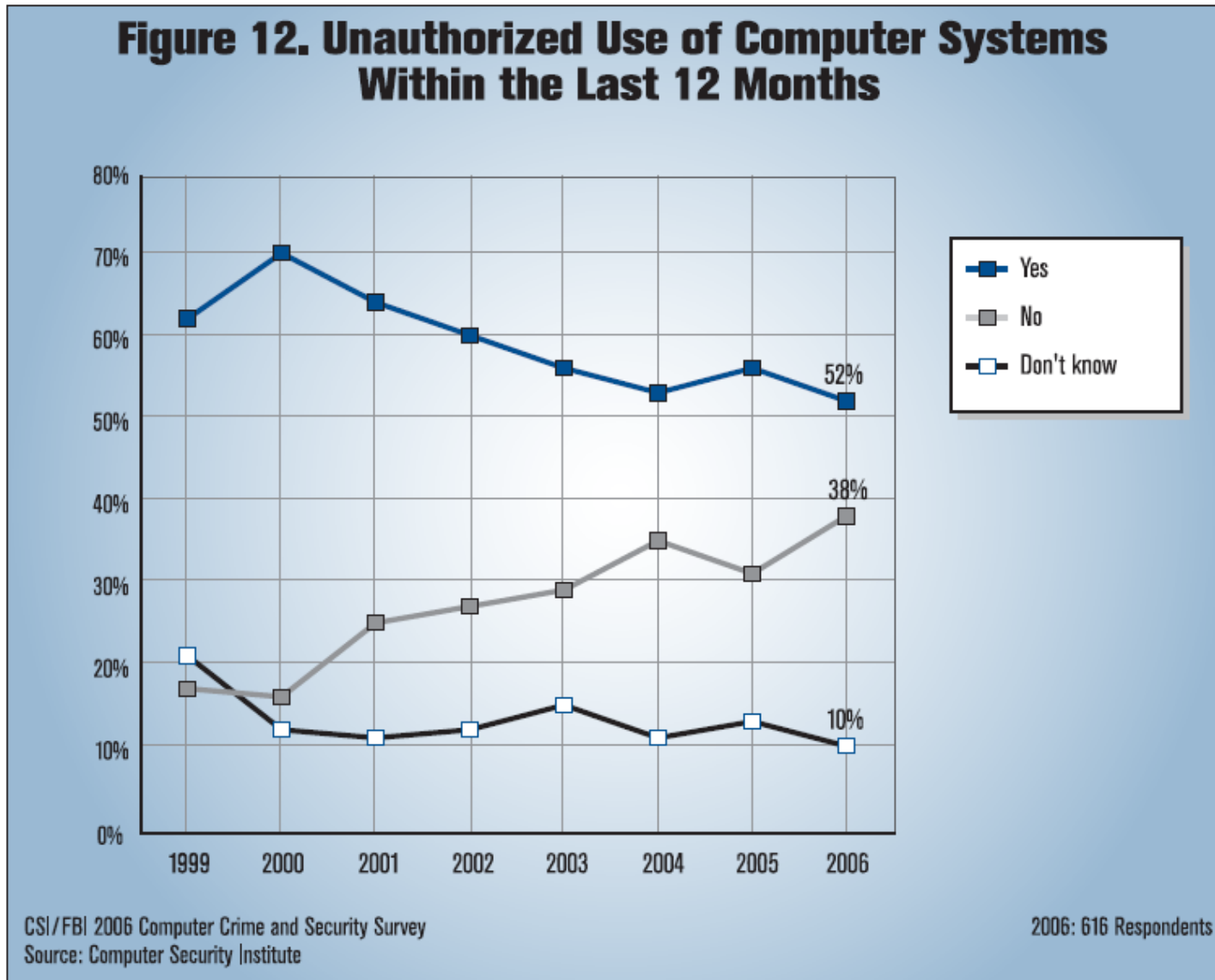


« On the Internet, nobody knows you're a dog »

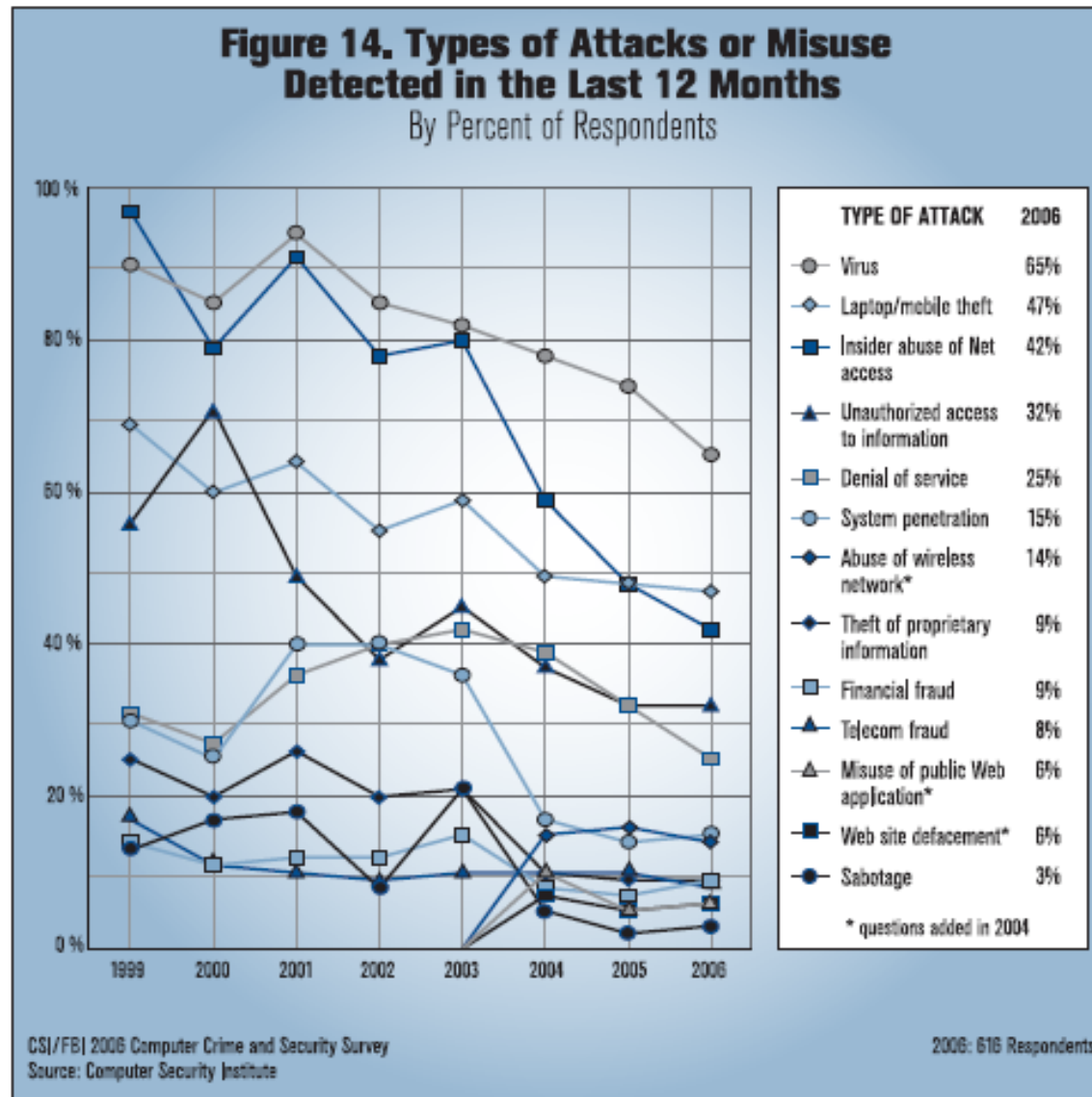
Grid Security – Threats



Grid Security – Threats: Unauthorized use of computer systems



Grid Security – Threats: Types of Attacks or Misuse



Grid Security: Suggested Action plan

- **Proof of concept and Return on investment**
- **Services needed**
- **Assets identification, criticality classification, data classification**
- **Reporting mechanism**
- **Liabilities and legal aspects**
- **Understanding its own business and industry sector in depth and as a whole**
- **Assessing the impact of decisions on all parties over the short and long term**
- **Applying learning from other industries**
- **Connecting with others who have more or different experience**
- **Considering the ethical dimensions of the actions**

Thank you.

Paul Wang
Tel: +41 58 792 96 01
Paul.Wang@ch.pwc.com

© 2005 PricewaterhouseCoopers AG/SA. All rights reserved. PricewaterhouseCoopers AG/SA refers to the Swiss firm of PricewaterhouseCoopers AG/SA and the other member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity.

PRICEWATERHOUSECOOPERS 