AusCERT
Australian Computer Emergency Response Team

IT Security Trends

The Australian Perspective

a presentation by

Viviani Paz, Security Assurance Manager

Australian Computer Emergency Response Team
The University of Queensland
Brisbane, Queensland 4072
AUSTRALIA

Outline

- AusCERT History
- The attacker profile
- IT Security Trends

AusCERT
Australian Computer Emergency Response Team

AusCERT

- Brief history
- Organisational Structure
- Services
- Role

AusCERT
Australian Computer Emergency Response Team

In the beginning there was nothing…

Brief history

- 1988 - Morris Worm – CERT/CC
- Formed in 1993 to provide incident response assistance to Australian universities - AARNET
- Membership based funding model – late 90s
  - National and International members from Government, Corporate, Sector
- National Information Infrastructure Protection - 1999
  - Y2K & Consultative forum
- Increased focus on Global and Regional Initiatives - 2002
- Inaugural AusCERT Asia Pacific Information Technology Security Conference - 2002
- Officially recognised as Australia's National CERT - 2003
  - 2002 PM's Business-Government Task Force on Critical Infrastructure
  - National Initiatives (http://national.auscert.org.au)

Organisational Structure

- Based at The University of Queensland

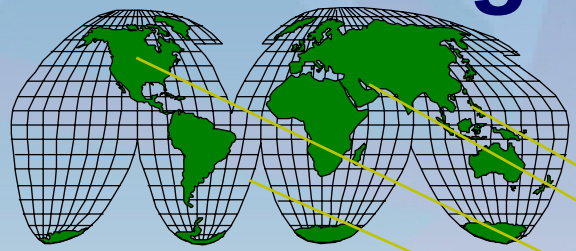
- Independent and “not for profit”
- 12+ full-time core staff and growing
- Coordination Centre
  - 24x7 on call operations centre
  - Alerts, advisories and incident response
- Budget
  - Membership subscriptions – 250 members
  - Government project based funding
  - Training
  - Conference

Services

- **Publications**
  - Member only content – news letters, business impact statements
  - Crime Survey in conjunction with Aust. Law enforcement agencies
  - Other e.g. Unix Security Checklist
  - Translated into other languages
- **Security Bulletins**
  - To organisation alias and via profile email
  - National IT Security Alert Service
- **(SMS) Early Warning Service**
- **Incident reporting (web, email, Probe)**
  - National IT Security Incident Reporting
  - AusCERT/AHTCC financial sector incident reporting
- **Member Assistance in emergency**
- **Member forum, industry group mail lists (upon request)**
- **Training and Conference (discounts for members)**

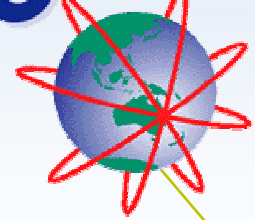
AusCERT
Australian Computer Emergency Response Team

Relationships with Other Organisations



- Research Organisations
- Other Incident Response Teams
- Law Enforcement Agencies
- Government Agencies
- Vendors and Product Manufacturers
- Consultants
- Technical Experts
- Other Network Users

AUSCERT



Role

- AusCERT is the trusted, single point of contact for
  - the dissemination of advice about computer network threats and vulnerabilities for Australian organisations
  - the coordination and handling of computer security incidents affecting Australian organisations for incidents sourced from anywhere around the globe
- National CERT for Australia

The Attacker Profile

Video: Sleepless Frights (2.05 minutes) from b-sec

The Attacker Profile

A successful attack requires: ***Motive - Means - Opportunity***

The Discriminators are:

Untargeted **(*an indiscriminate victim*)**
- **A function of the *Opportunity* aspect…**

Specifically targeted
- **A function of *any* aspect…**

Only *Opportunity* **can be controlled by the victim**
- **The attacker controls the *Motive* and the *Means***

Assume a motivated **attacker:**
- **Do NOT assume a technical motive only!**

Attacker Motive

- **Indiscriminate attack** *(eg after a network-scan)*
- **Curiosity** *(eg "I was just testing…!")*
- **Vandalism or peer kudos** *(eg "My 'kung-fu' is the best!")*
- **Fear, greed or malice** *(eg a disgruntled ex-employee)*
- **Hacktivism** *(eg "We want full disclosure of vuls!")*
- **Industrial espionage** *(eg stealing trade-secrets)*
- **Electronic warfare** *(eg website defacements)*

Technical Goals of the Attacker

- Intelligence gathering
- Denial of Service
- Read protected information
- Modify information
- Execute arbitrary commands

  Sub-goals:

  - Privileged access (ie ‘root’ or ‘Administrator’)
  - Ensure future access

Outcomes sought

- Financial gain for attacker
- Cost to victim
- Media exposure
- Political agenda
- Any other outcome to service *fear* or *greed*

What can we do?

Security is a business problem, not a technical problem.

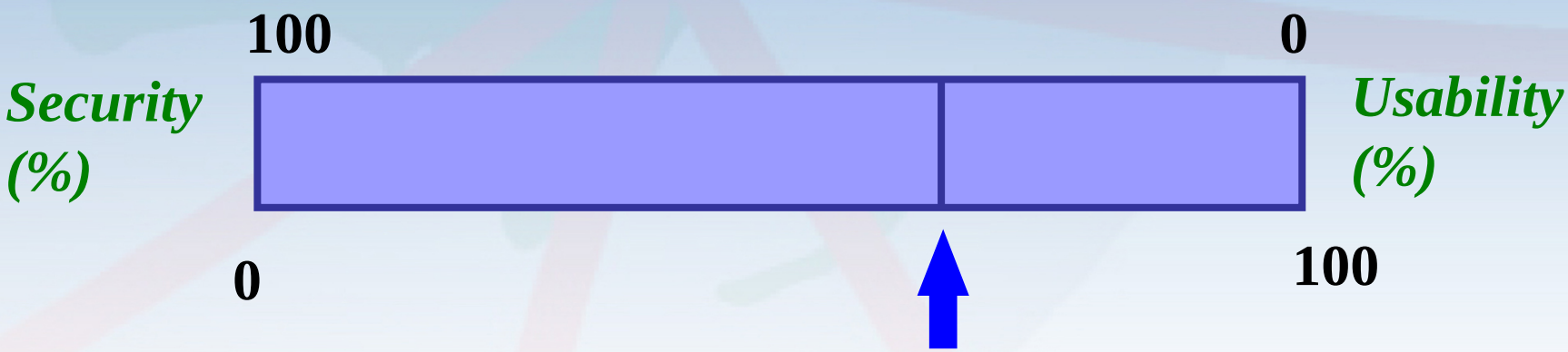
- **Not everything is solvable through technology.**
- **It requires input from multiple disciplines:**

  IT, law, risk, education.

- **Physical security**
- **Capacity planning**
- **Change control**
- **Procedures**
  - **Continuity of service**
  - **Recovery of service**
- **Purchasing criteria**
- **Service Level Agreements**
- **Administrative controls**
- **Technical defences**
- **Awareness programs**

Balance

An appropriate balance between security and competing interests is required.



Failures in security are often more about the processes (or lack off) for enabling new services or maintaining security.

AusCERT
Australian Computer Emergency Response Team

IT Security Trends

Global Trends

- Economies increasing dependency on public network applications
  - I.e. online banking, online stock trading, e-business, e-government, e-customs, e-etc
- Increase in Computer Network Attacks (CNA) against National Information Infrastructure (NII)
  - frequency, sophistication and scale
- Hackers / Intruders
  - increasing numbers and skills
- Attack tools
  - more sophisticated, more powerful, easier to use
- Increased Web browser/mail client based attacks
- Rapid pace of change
- Faster cycle between vulnerability and active exploit

Local Trends

Australian Computer Crime and Security Survey 2004

Australian Government
Attorney-General's Department
Department of Communications, Information Technology and the Arts

AusCERT

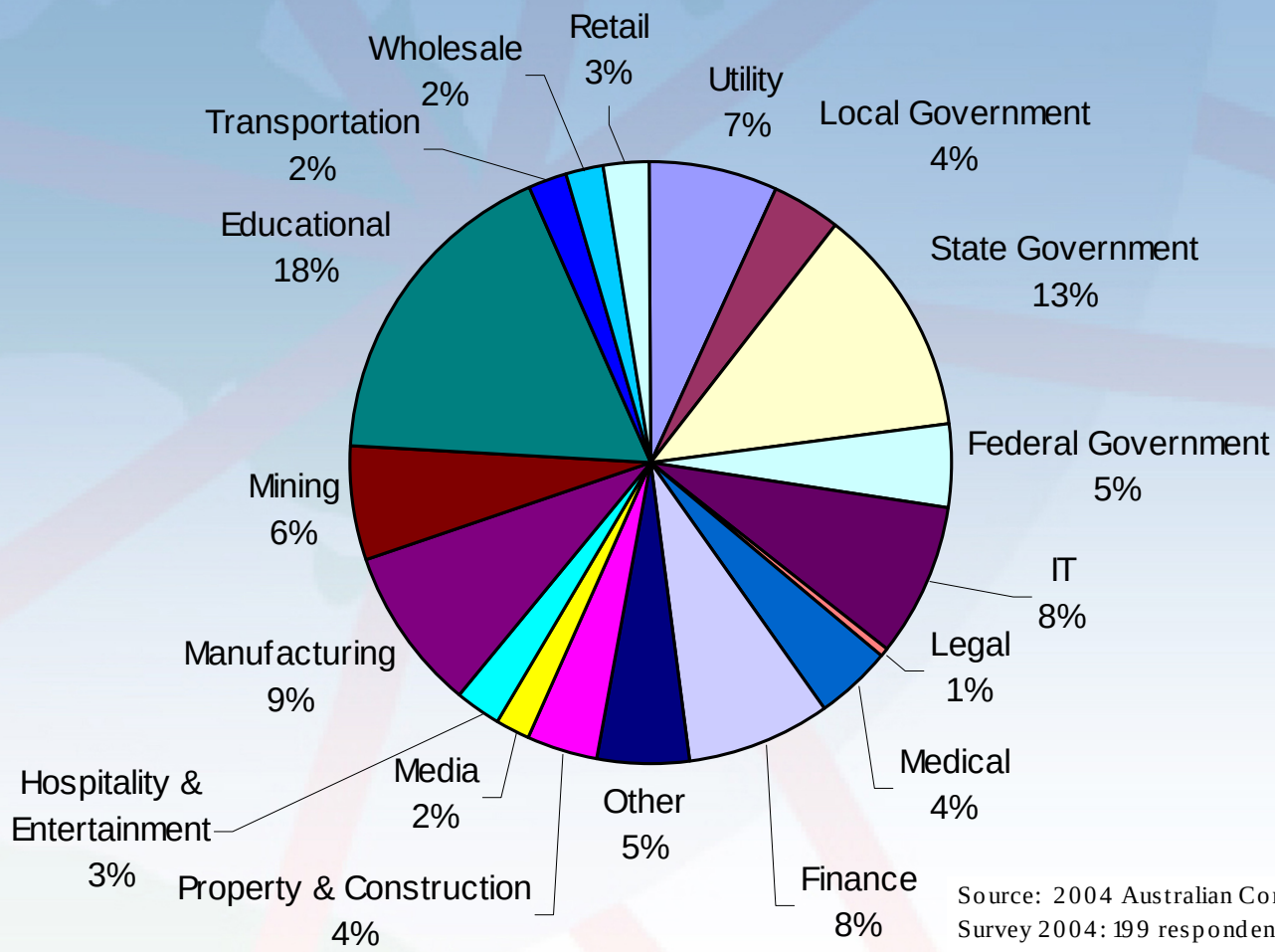
Australian Federal Police
To fight crime together and win

AusCERT
Australian Computer Emergency Response Team

Who we asked?

AusCERT
Australian Computer Emergency Response Team

Respondents by industry sector



Source: 2004 Australian Computer Crime and Security Survey 2004: 199 respondents/83%

Key Findings

- **Despite improvements in the levels of respondents using and applying various security counter-measures (technical and procedural):**
  - **more harmful electronic attacks have been reported**
  - **greater cost impacts have been reported**
  - **fewer organisations are confident that they are managing their information security well**
- **Clearly measures taken to manage information security appear to be insufficient to protect against common security threats.**
  - **A function of the rapidly changing threat and vulnerability environment in which organisations must operate**

Key Findings

Worm, virus and trojan infections

- Affects all industries and e-commerce customers
- Unless the trend changes, it has the potential to undermine public confidence in e-commerce and other forms of on-line security

Computer security management

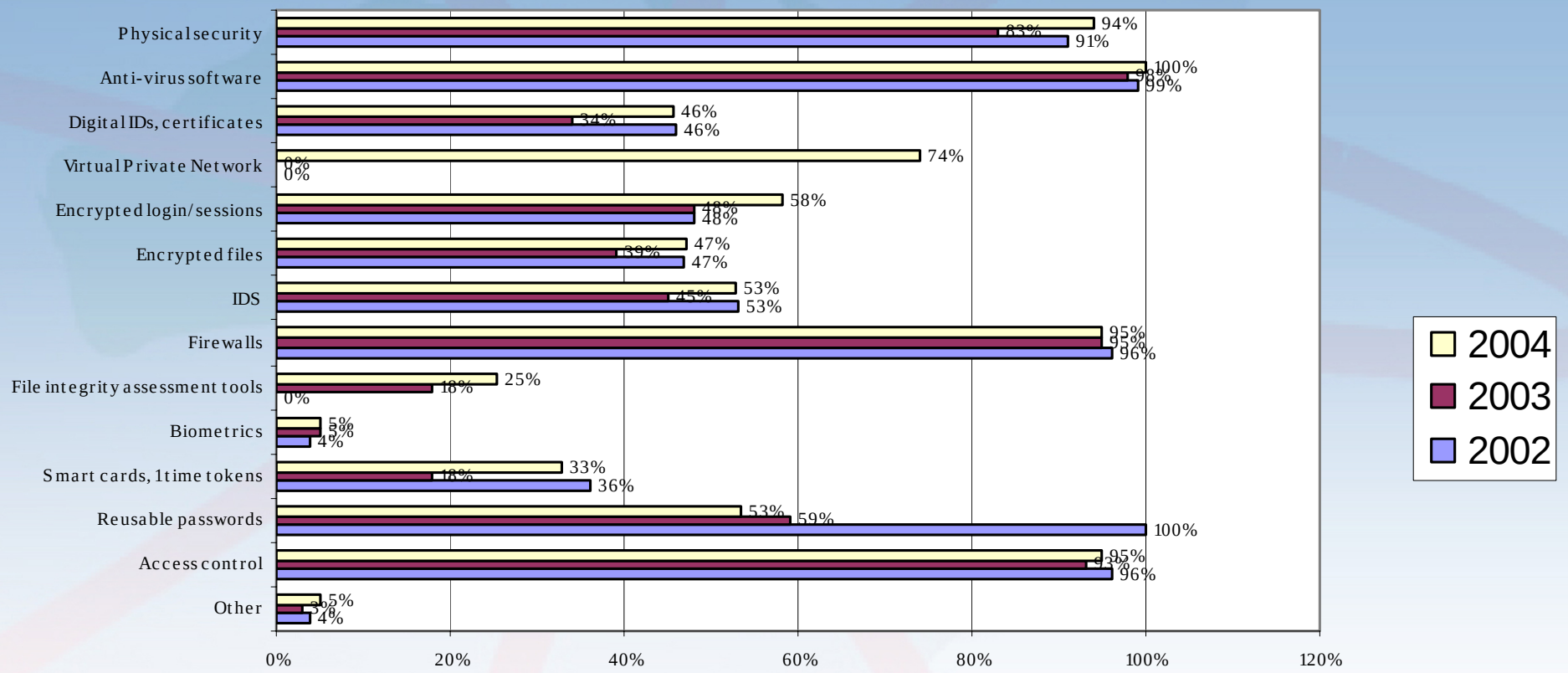
- 70% increased spending during last 12 months due to concerns about adequacy of organisation's computer security

AusCERT
Australian Computer Emergency Response Team

Readiness to Protect IT Systems

AusCERT
Australian Computer Emergency Response Team

Security technologies used

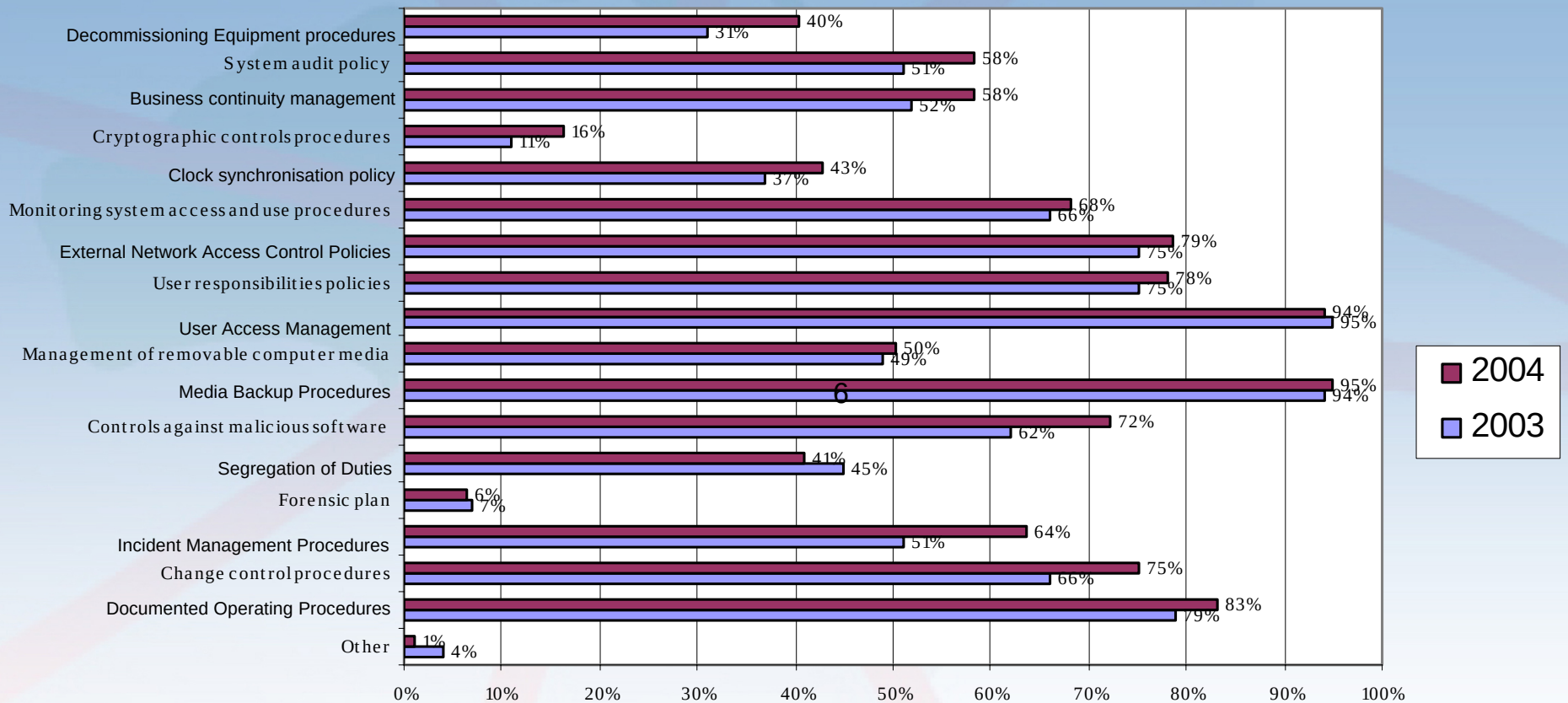


Source: 2004 Australian Computer Crime and Security Survey 2004: 182 respondents/76%, 2003: 214 respondents/100%,

Note: In 2002, respondents were not asked if they used file integrity assessment tools and in 2002 and 2003, respondents were not asked if they used

AusCERT
Australian Computer Emergency Response Team

Computer security policies and procedures used



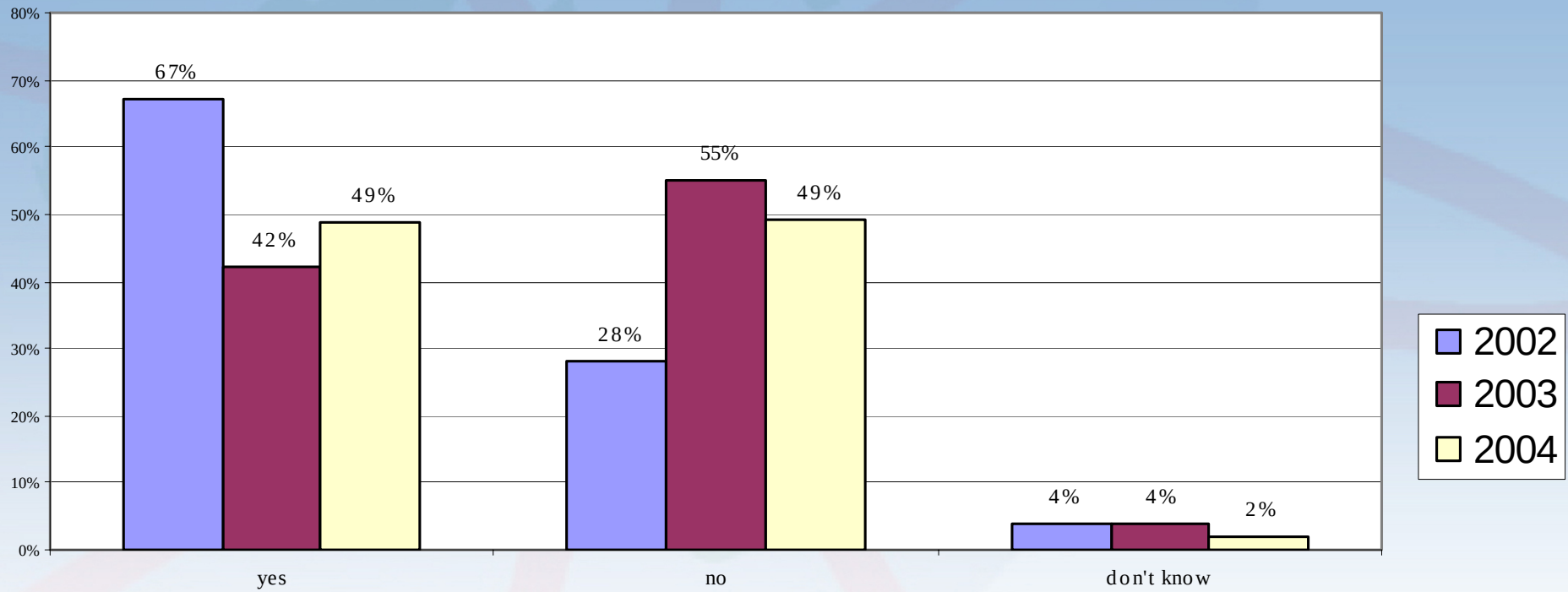
Source: 2004 Australian Computer Crime and Security Survey
2004: 173 respondents/72%, 2003: 213 respondents/99%

Note: This question was not asked in the 2002 Australian Computer Crime and Security Survey.

Trends

AusCERT
Australian Computer Emergency Response Team

Did your organisation experience one or more electronic attacks in the last 12 months?



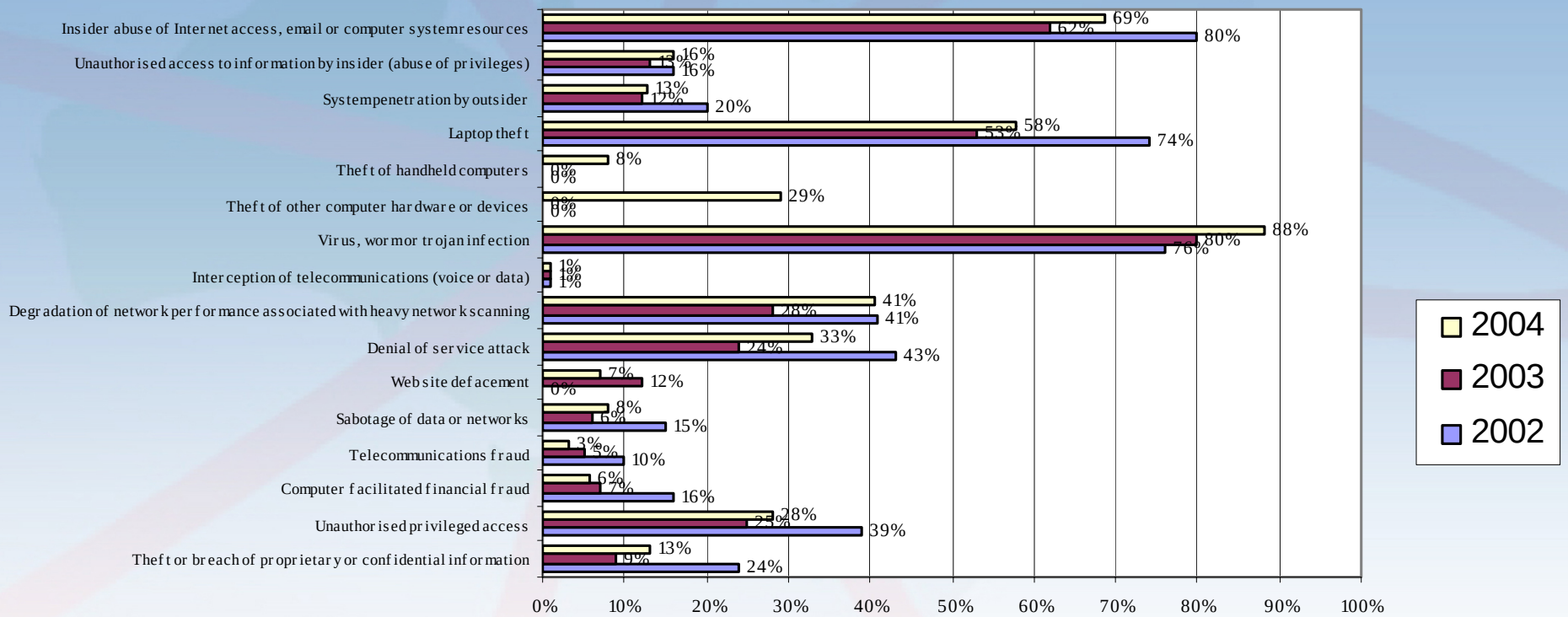
Source: 2004 Australian Computer Crime and Security Survey 2004: 238 respondents/99%, 2003: 212 respondents/99%, 2002: 92 respondents/97%

Note: In 2004, an electronic attack was defined as an attack which harmed the confidentiality, integrity or availability of network data or systems. In 2003, the term "computer security incidents" was used instead of "electronic attacks" and was defined as an attack against a computer or network which harmed the confidentiality, integrity or availability of network data or systems. In 2002, a computer security incident was defined as an attack against a computer or network, either real or perceived.

Nature and Impact

AusCERT
Australian Computer Emergency Response Team

Which of the following types of electronic attack, computer crime, computer access misuse, or abuse did your organisation detect in the last 12 months?



Source: 2004 Australian Computer Crime and Security Survey
2004: 227 respondents/95%, 2003: 196 respondents/91%

Note: In 2002 and 2003, respondents were asked if they had experienced "telecommunications eavesdropping" or "wiretapping" instead of "interception of telecommunications (voice or data)". Also in 2002 and 2003, "theft of handheld computers" and "theft of other computer hardware or devices" were not included under this question. In 2002, web site defacement was not a category under this question.

The Cost of Computer Crime

How losses were incurred	*Total Annual Loss*		
	2002	**2003**	**2004**
Virus, worm, Trojan infection	891,100	2,223,900	7,097,100
Computer facilitated financial fraud	807,000	3,525,000	2,457,000
Degradation of network performance associated with network scanning	161,500	528,200	1,709,000
Laptop theft	1,263,900	2,258,183	1,484,244
Theft/breach of proprietary or confidential information	290,000	258,000	1,340,000

Financial impact trends

- 57% of all respondents quantified losses for 1 or more types of electronic attack, computer crime or computer access misuse
- In 2004, average annual losses increased by 20%:
  - From $93,657 in 2003 to $116,212 in 2004
- 2nd largest source of financial loss was due to computer facilitated financial fraud
  - Totaled $2,457,000 or 15% of total losses reported

AusCERT
Australian Computer Emergency Response Team

Computer Security Management

Computer security management

The most common vulnerabilities that contributed to harmful electronic attacks were:

- Exploitation of unpatched or unprotected software vulnerabilities – 60%
  - Compared to 29% in 2003
  - A major reason for the large numbers of worm infections reported
- Inadequate staff training and education in security practices and procedures – 49%
  - Compared to 42% in 2003
- Poor security culture in organisation – 46%
  - Compared to 49% in 2003

Challenges

- **Most challenging or problematic areas of computer security management:**
  - **Changing users' attitudes and behavior regarding computer security practices – 65%**
  - **Keeping up to date with computer threats and vulnerabilities – 61%**
    - **both factors are likely contributors to the prevalence of virus, worm and trojan infections reported by respondents**

Conclusion

- More organisations have improved their readiness to protect their information systems
- But there remains a high percentage who are dissatisfied with the capacity of their organisation to effectively protect their information systems
- Major reasons for this are:
  - Worsening number of electronic attacks, particularly virus, worm and trojan infections and their consequent damage to the organisation
  - the nature of the external threat environment which organisations must operate and the inherent vulnerability of system software being used on their networks
- Organisations believe their ability to consistently and effectively apply appropriate security measures is not keeping pace with factors beyond their control – primarily the external threat environment and software vulnerabilities

www.auscert.org.au/crimesurvey

AusCERT
Australian Computer Emergency Response Team

AusCERT Contact Information

24 Hour Hotline: (07) 3365 4417 (After Hours for Emergencies)

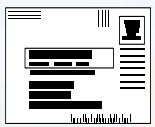
International: +61 7 3365 4417 (GMT+1000)

Facsimile: (07) 3365 7031

International: +61 7 3365 7031

Electronic Mail: auscert@auscert.org.au

World Wide Web: http://www.auscert.org.au/



Postal: AusCERT
The University of Queensland
Brisbane Qld. 4072
Australia