# Security & Ethics – 27 Jul 2010

**Justin Williams**
**Senior Manager**
**Advisory Services**

ERNST & YOUNG
*Quality In Everything We Do*

# A Thought….

- *“Computer insecurity is inevitable. Networks will be hacked. Fraud will be committed. Money will be lost. People will die”.*
- *Bruce Schneier, master cryptographer*

# A Thought….

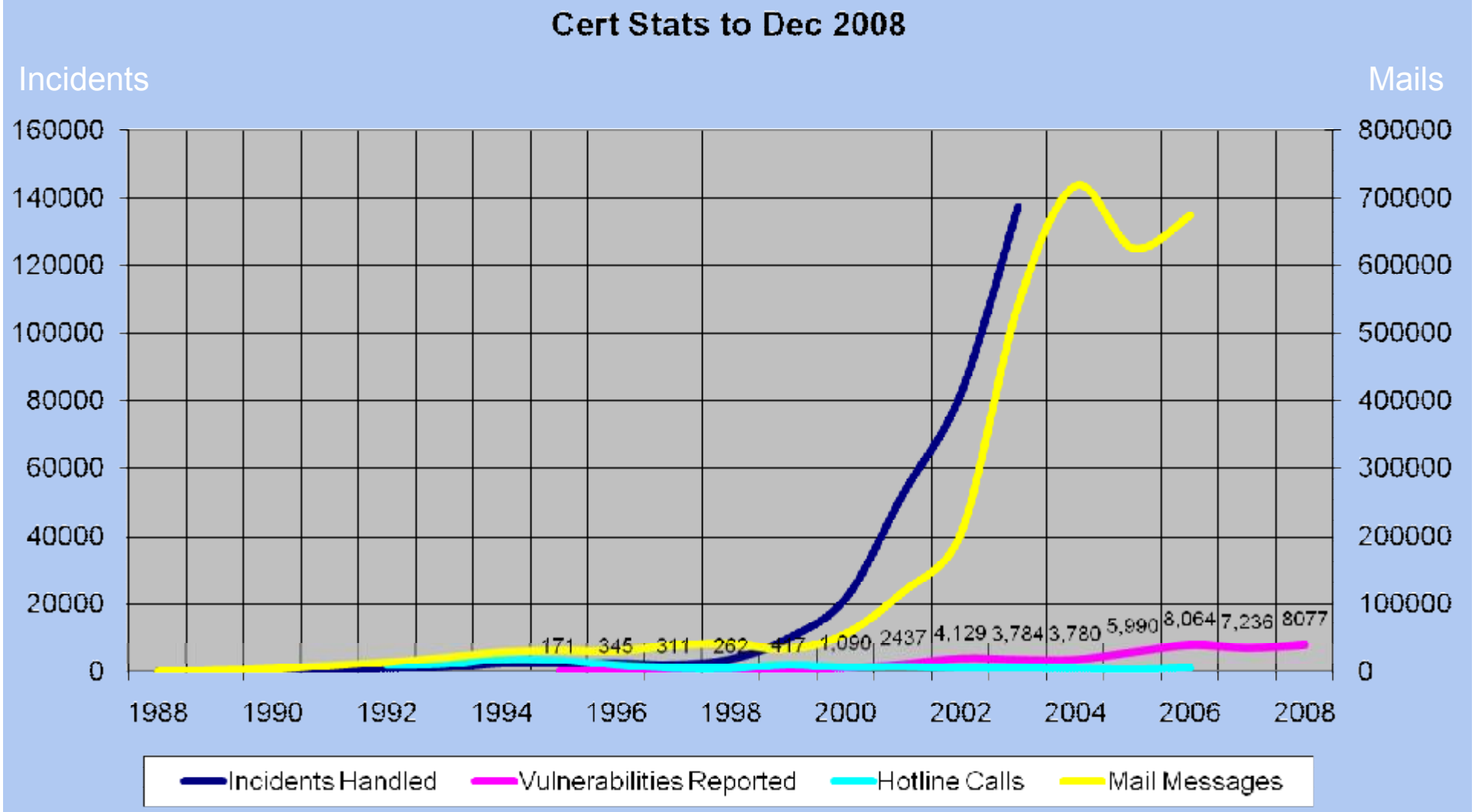
# Ethics

- IT has the potential to do good vs potential for harm
- Principles of Technology Ethics
  - Proportionality – good outweigh harm
  - Informed Consent – those affected understand and accept
  - Justice – benefits and burdens should be fairly distributed
  - Minimized risk – even if acceptable by other 3 guidelines, must be implemented to avoid risk

# Ethics

- Ethics are embodied in codes of professional conduct for IS professionals
  - Eg. Association of IT professionals (AITP), ISACA, ISC2
    - HTTP://WWW.ISACA.ORG.ZA
  - Recognises obligation to employer
    - Avoid conflicts of interest
    - Protect privacy & confidentiality etc
  - Also obligation to society
    - Ensure products of work used responsibly
    - Support, respect and abide by laws
    - Never use confidential info for personal gain

# Growth in number of security breaches



# Ernst & Young's 2009 Global Information Security Survey

The EY security survey is one of the longest-running and most recognized annual surveys of its kind. For 12 years, our survey has helped our clients focus on the right risks and priorities, identify their strengths and weaknesses, and improve their information security. This year's survey received the highest levels of participation since inception.

In this survey we take a closer look at how organisations are specifically addressing their information security needs. We also identify and summarise potential opportunities for improvement and important trends that will continue to drive information security in the coming years.

How do you protect your organization's brand and reputation in an environment of change? How do you identify and manage new risks? How do you overcome increasing challenges to deliver an effective information security program? How do you comply with new regulations and industry requirements? How do you leverage technology to not only meet business objectives but also improve security?

# 2009 Global Security Survey

## Key survey findings

### Managing risks

- Improving information security risk management is a top security priority for the next year.
- External and internal attacks are increasing.
- Reprisals from recently separated employees have become a major concern.

### Addressing challenges

- Availability of skilled information security resources is the greatest challenge to effectively delivering information security initiatives.
- Despite most organizations maintaining current spending on information security, adequate budget is still a significant challenge to delivering security initiatives.
- Security training and awareness programs are falling short of expectations.

### Complying with regulations

- Regulatory compliance continues to be an important driver for information security.
- Cost of compliance remains high, with few companies planning to spend less in the next 12 months.
- Too few organizations have taken the necessary steps to protect personal information.

### Leveraging technology

- Implementing DLP technologies is the top security priority for many organizations.
- The lack of endpoint encryption remains a key risk with few companies encrypting laptops or desktop computers.
- Virtualization and cloud computing are gaining greater adoption, but few companies are considering the information security implications.

# CSI FBI 2008 Survey : Overview

- 522 computer security practitioners in the USA
- 13th year of survey
- www.gocsi.com

**The most expensive computer security incidents were those involving financial fraud…**

…with an average reported cost of close to $500,000 (for those who experienced financial fraud). The second-most expensive, on average, was dealing with "bot" computers within the organization's network, reported to cost an average of nearly $350,000 per respondent. The overall average annual loss reported was just under $300,000.

**Virus incidents occurred most frequently…**

…occurring at almost half (49 percent) of the respondents' organizations. Insider abuse of networks was second-most frequently occurring, at 44 percent, followed by theft of laptops and other mobile devices (42 percent).

**Almost one in ten organizations reported they'd had a Domain Name System incident…**

…up 2 percent from last year, and noteworthy, given the current focus on vulnerabilities in DNS.

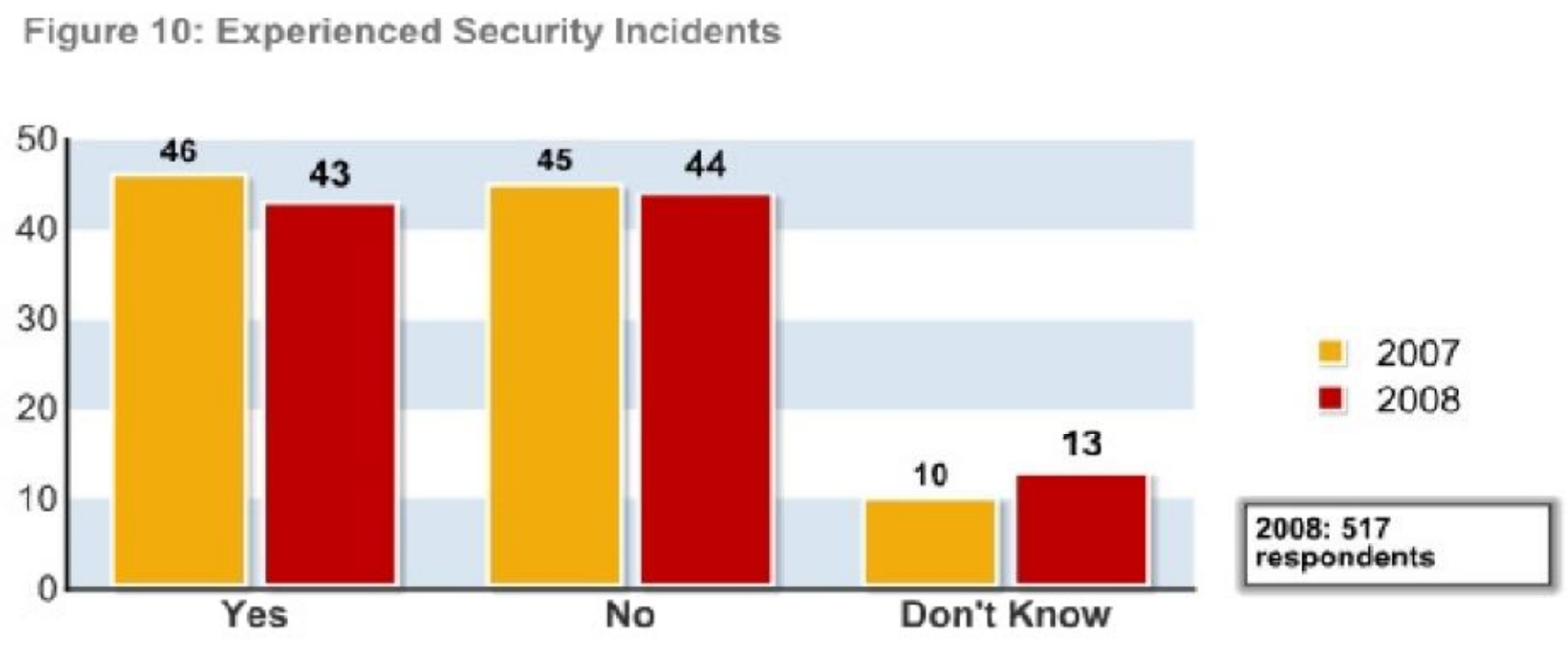
**Twenty-seven percent of those responding to a question regarding "targeted attacks"…**

…said they had detected at least one such attack, where "targeted attack" was defined as a malware attack aimed exclusively at the respondent's organization or at organizations within a small subset of the general business population.

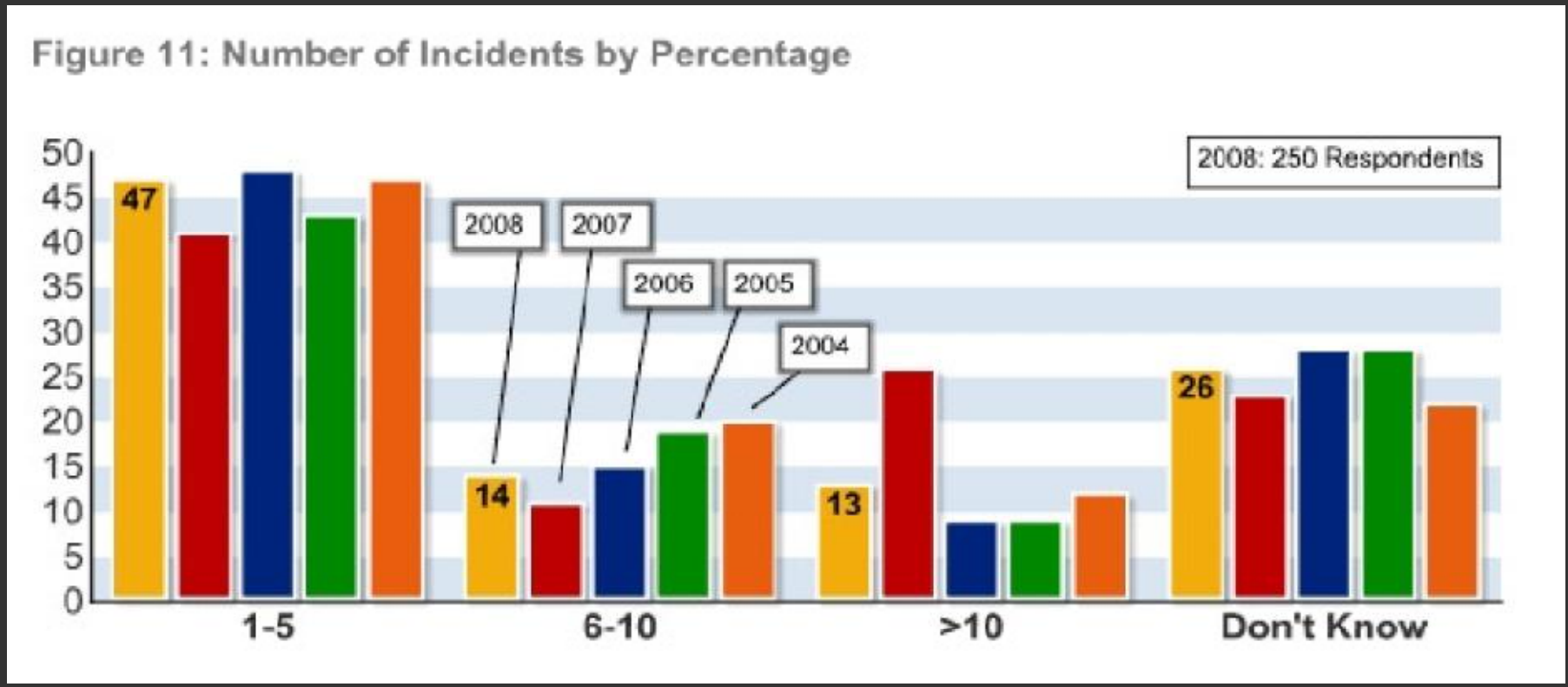
**The vast majority of respondents said their organizations either had (68 percent)…**

…or were developing (18 percent) a formal information security policy. Only 1 percent said they had no security policy.

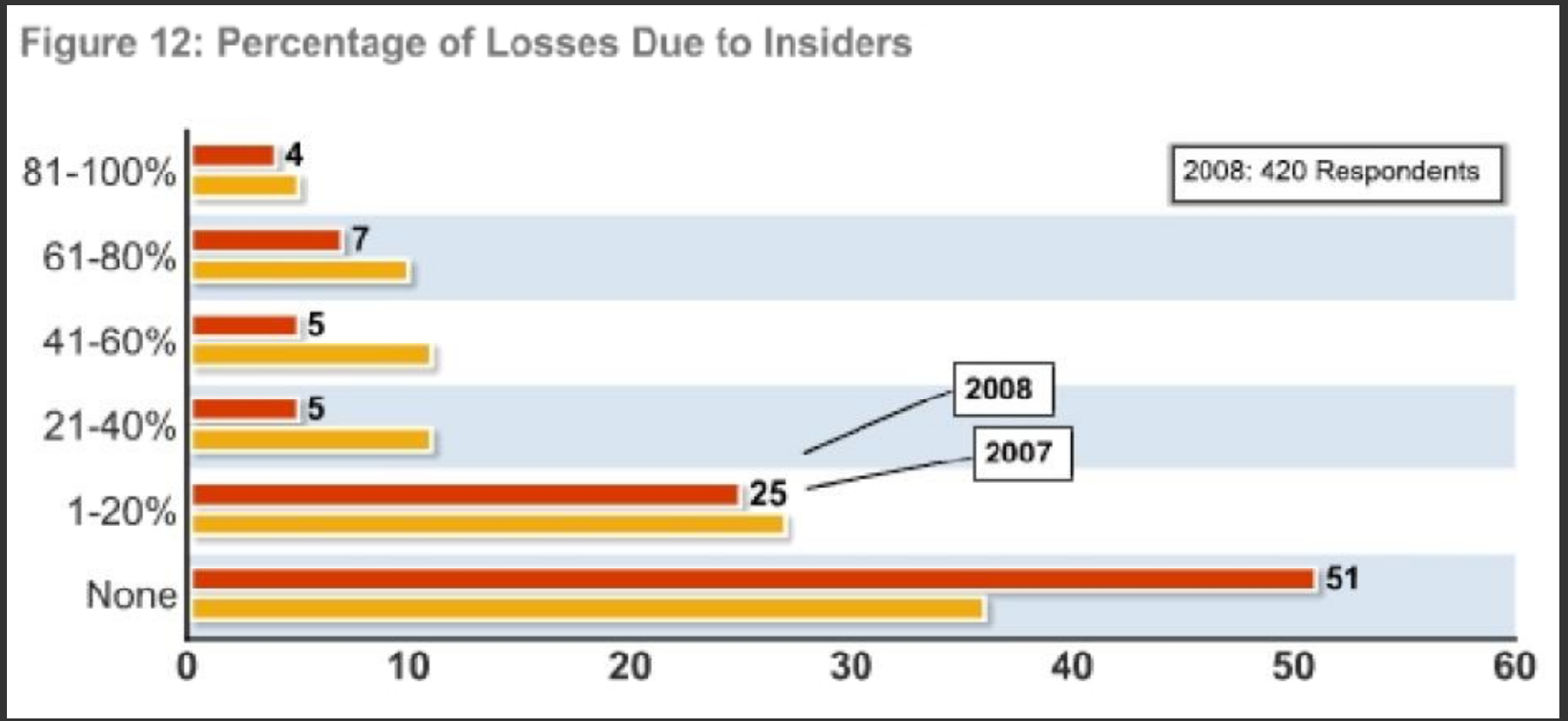
# CSI FBI 2008 Survey : Experienced Security Incidents



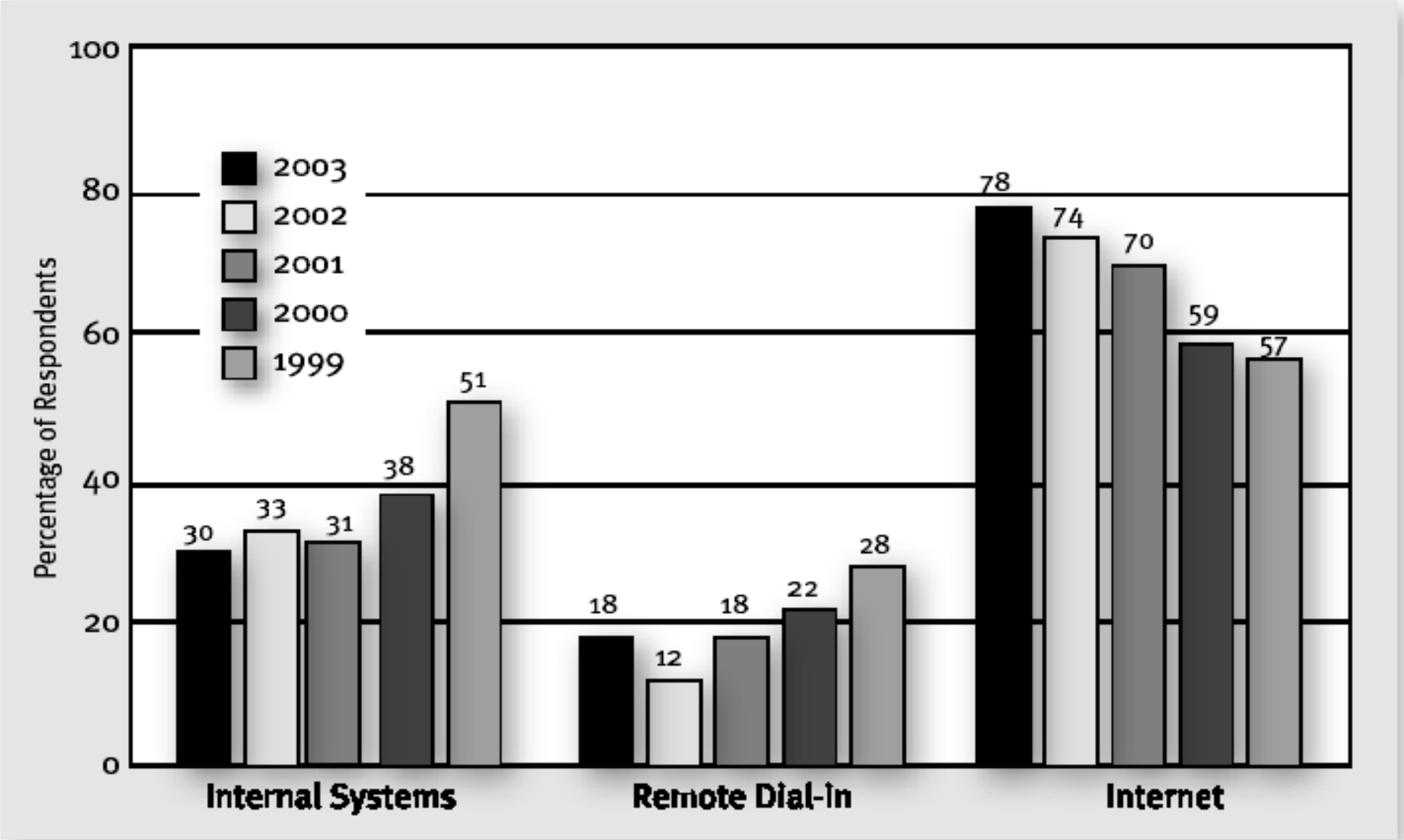
# CSI FBI 2008 Survey : Number of incidents



# CSI FBI 2008 Survey : Loss from insiders



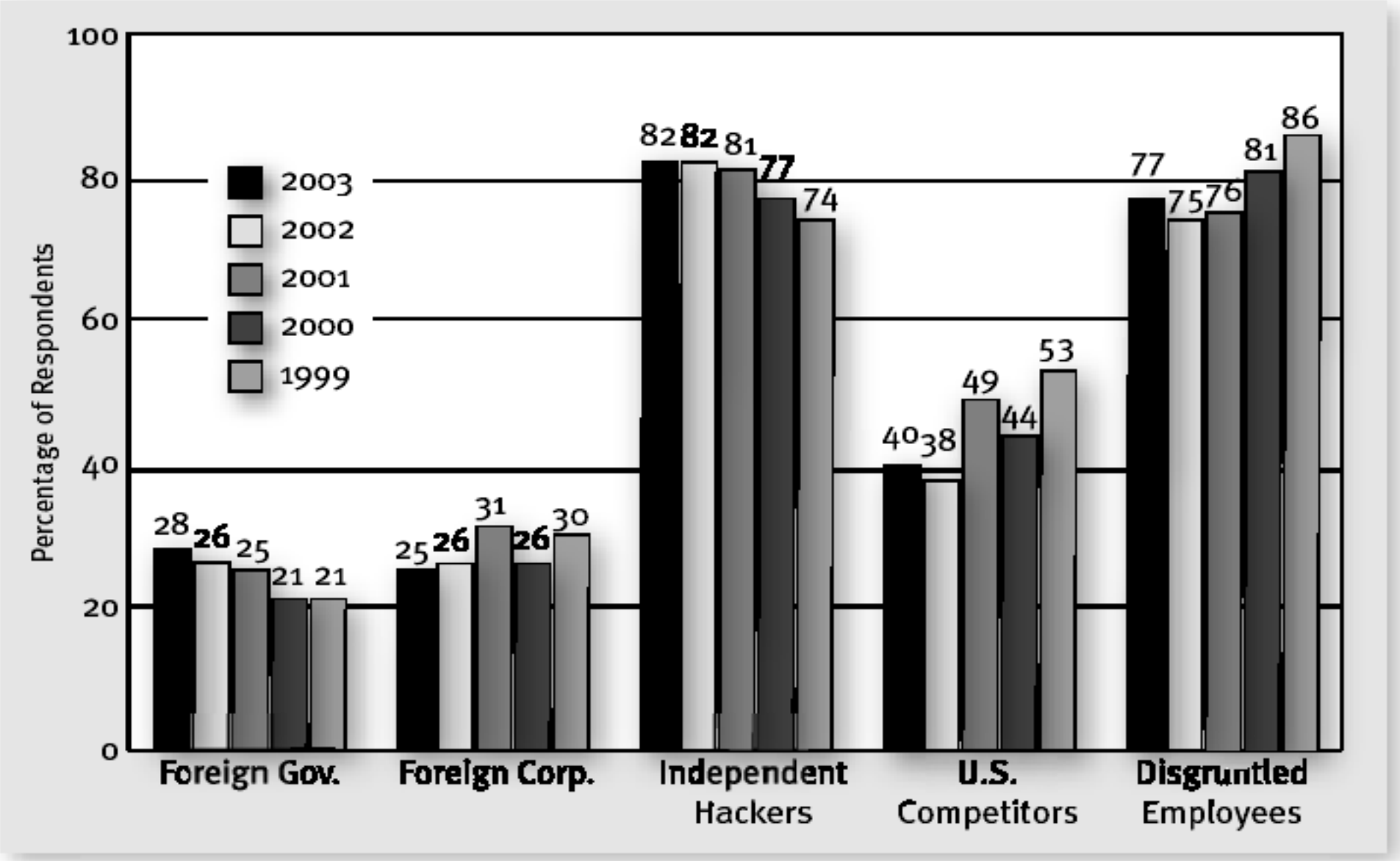
# Internet Connection is Increasingly Cited as a Frequent Point of Attack




CSI/FBI 2003 Computer Crime and Security Survey

Source: Computer Security Institute

# Likely Sources of Attack

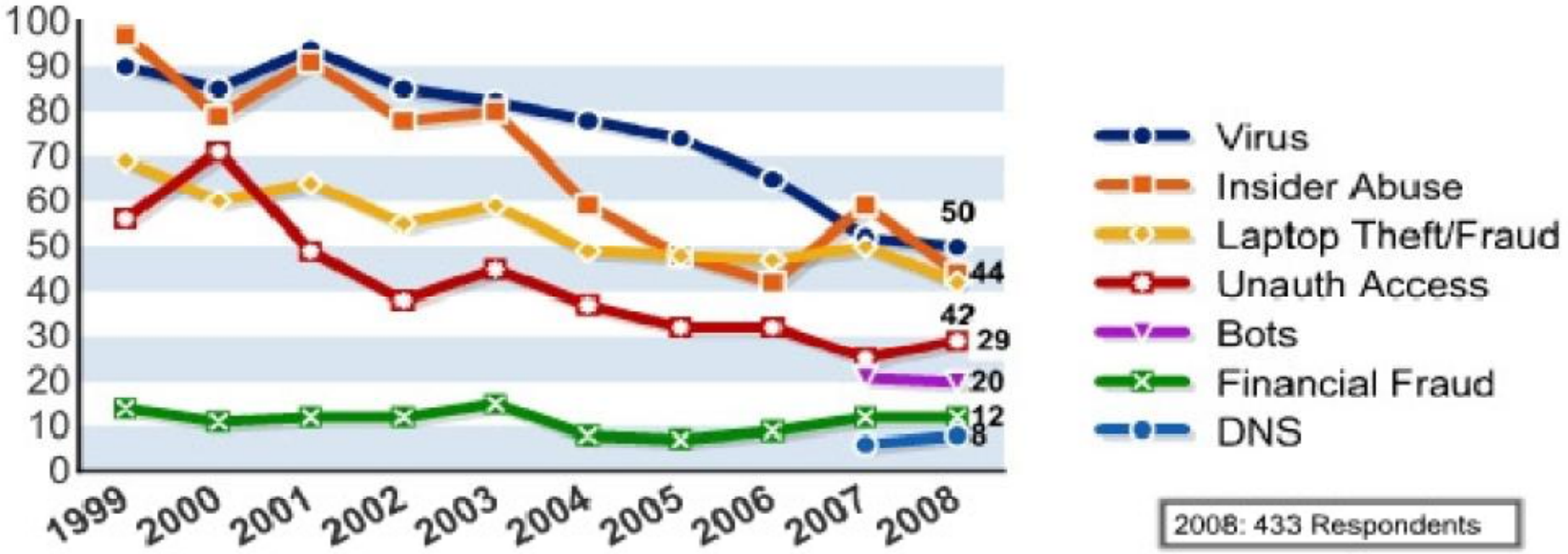



CSI/FBI 2003 Computer Crime and Security Survey

Source: Computer Security Institute

# CSI FBI 2008 Survey : Types of incidents

Figure 13: Percentages of Key Types of Incident

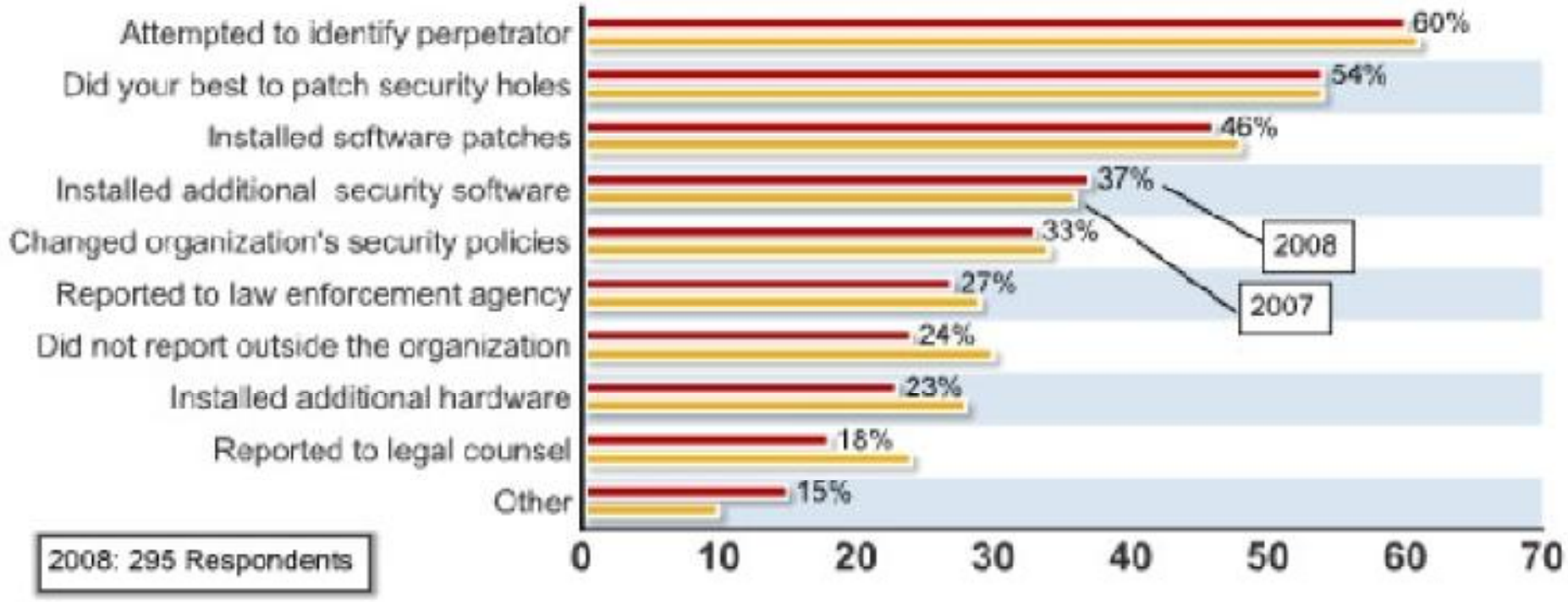


# CSI FBI 2008 Survey : Types of incidents

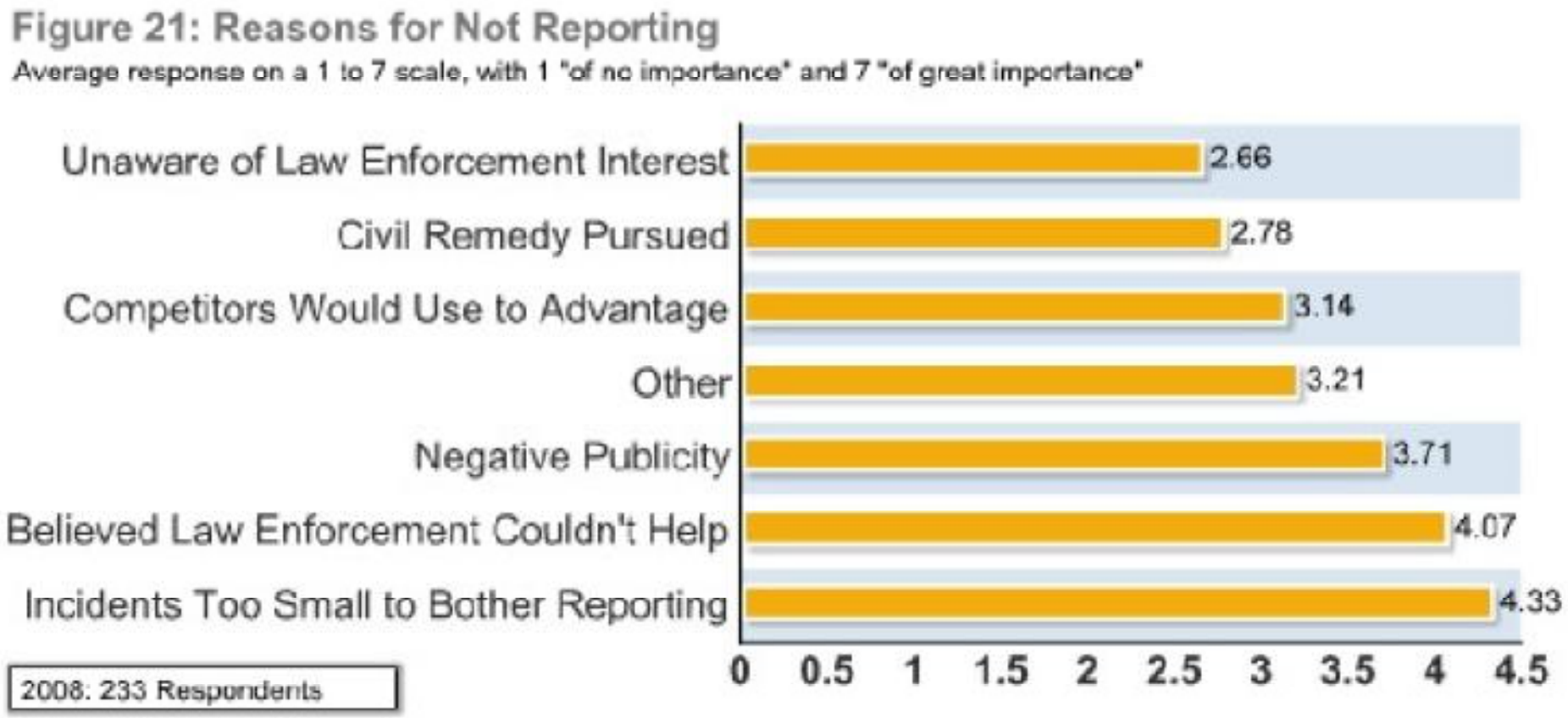
| Table 1 | 2004 | 2005 | 2006 | 2007 | 2008 |
|---|---|---|---|---|---|
| Denial of service | 39% | 32% | 25% | 25% | 21% |
| Laptop theft | 49% | 48% | 47% | 50% | 42% |
| Telecom fraud | 10% | 10% | 8% | 5% | 5% |
| Unauthorized access | 37% | 32% | 32% | 25% | 29% |
| Virus | 78% | 74% | 65% | 52% | 50% |
| Financial fraud | 8% | 7% | 9% | 12% | 12% |
| Insider abuse | 59% | 48% | 42% | 59% | 44% |
| System penetration | 17% | 14% | 15% | 13% | 13% |
| Sabotage | 5% | 2% | 3% | 4% | 2% |
| Theft/loss of proprietary info | 10% | 9% | 9% | 8% | 9% |
| from mobile devices | | | | | 4% |
| from all other sources | | | | | 5% |
| Abuse of wireless network | 15% | 16% | 14% | 17% | 14% |
| Web site defacement | 7% | 5% | 6% | 10% | 6% |
| Misuse of Web application | 10% | 5% | 6% | 9% | 11% |
| Bots | | | | 21% | 20% |
| DNS attacks | | | | 6% | 8% |
| Instant messaging abuse | | | | 25% | 21% |
| Password sniffing | | | | 10% | 9% |
| Theft/loss of customer data | | | | 17% | 17% |
| from mobile devices | | | | | 8% |
| from all other sources | | | | | 8% |

# CSI FBI 2008 Survey : Actions taken after incident

Figure 20: Actions Taken After an Incident



# CSI FBI 2008 Survey : Why not report



# Cost of computer security breaches

- 80% of organisations acknowledged financial loss as a result of a computer breach.
- 44% were willing and/or able to quantify their financial loss
- Most serious financial loss as a result of theft of proprietary information and financial fraud
  - Theft of proprietary information and financial fraud account for 2/3 of financial losses
  - Yet, only 20% report incidents of theft of proprietary info and only 12% report incidents of financial fraud

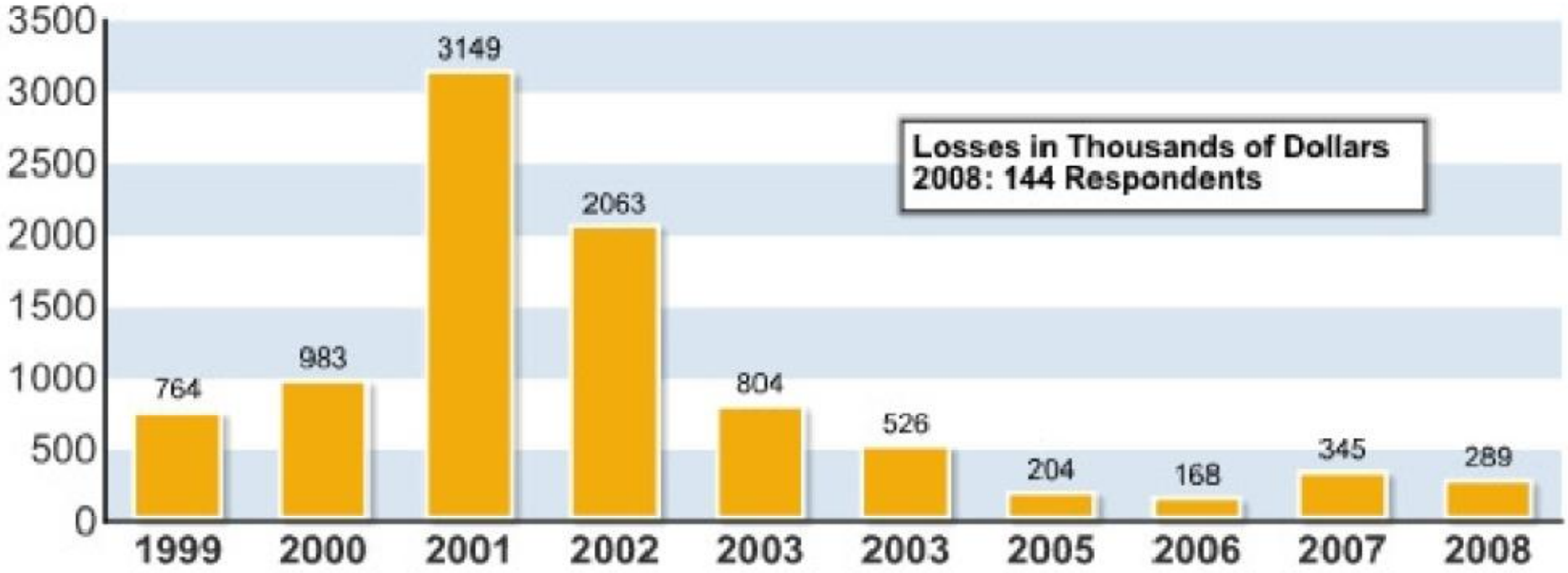
# Cost of computer security breaches …

- Trend moved downwards (per CSI/FBI)
  - $289k average incident loss, still down from early 2000's
  - Highest Average loss $3,149k in 2001

- Other
  - In South Africa, the average loss per incident is over R575 000 (from KPMG's 2002 security survey)
  - RIAA won $1million settlement from IIS - employees ran INTERNAL server for MP3's
  - Biggest concern is reputation damage (Ernst & Young 2008 survey)

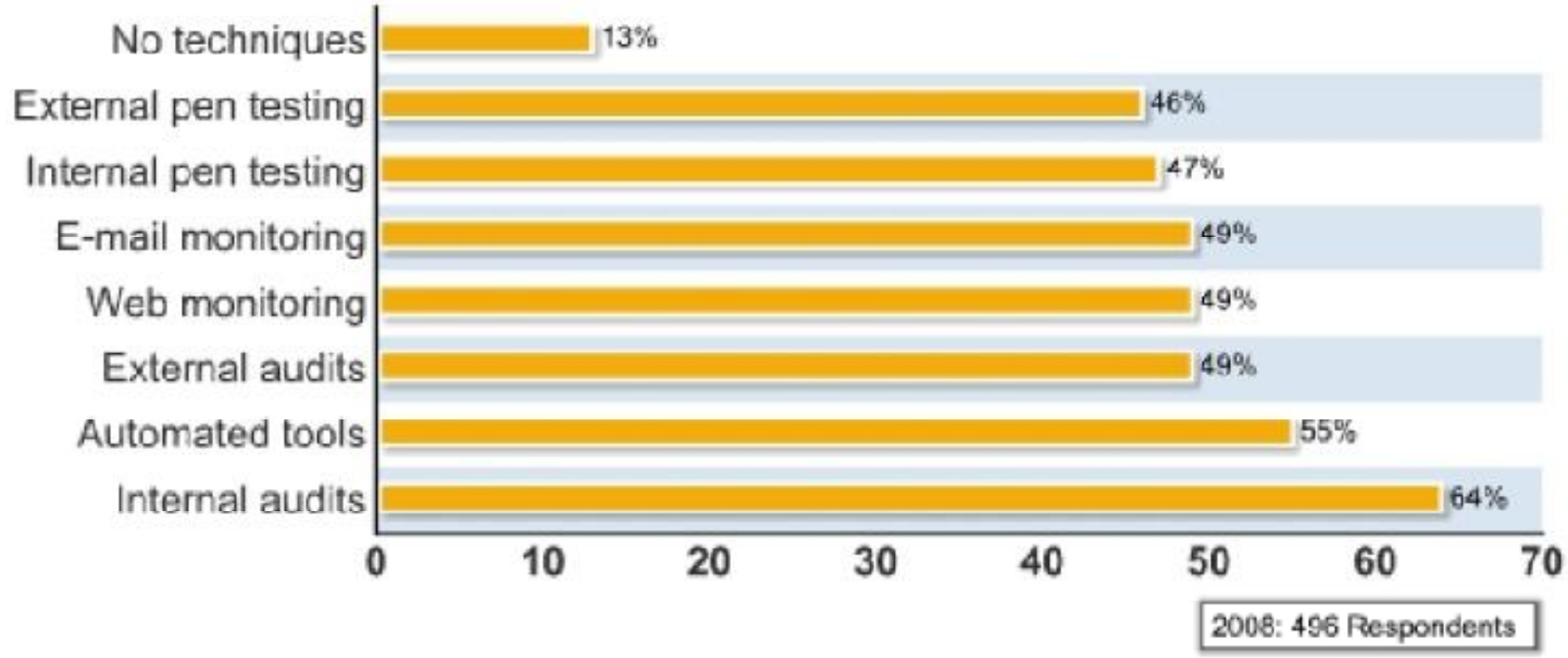
# CSI FBI 2008 Survey : Loss per incident

Figure 14: Average Losses Per Respondent



# CSI FBI 2008 Survey : Evaluating Security

Figure 17: Techniques Used To Evaluate Security Techology




"The virus was contained in an e-mail warning about the virus . . ."

# 2 Case Studies

## EFT System
## End User Computing

ERNST & YOUNG
Quality In Everything We Do

# Why test ?

*Hundreds of millions of rands of payments being made every year*

## Case Study : Electronic Funds Transfer

- **Scenario :**

  A multinational company approachedus to assess the security of their EFT infrastructure from the perspective of a malicious employee on the local network.

- **Objective :**

  Gain access to and process transactions on the EFT system.

## Case Study : Electronic Funds Transfer

- **Champion :**

  The work was commissioned by senior management without the knowledge of IT

- **Purpose :**

  To gain understanding of the true current state and validate whether the position put forward by IT was a true reflection of reality

## Case Study : Electronic Funds Transfer

- **Outcome :**
  - Gained full access to the mainframe based EFT application with supervisor and signatory privileges
  - This would have allowed us to fraudulently process transactions, alter account details and severely disrupt the company's accounting system
  - Organisation failed test

## Case Study : Electronic Funds Transfer

- **How It Was Done :**
  - Used company phone list to identify financial staff.
  - Obtained access to key workstations, allowing us to install key loggers, download sensitive data, obtained client software used to connect to EFT system.
  - Obtained access to the Windows NT domain allowing us to crack 98.8% of domain passwords.

## Case Study : Electronic Funds Transfer

- **How It Was Done Continued :**
  - Accessed E-mail infrastructure with NT domain passwords. This allowed us to intercept sent email describing EFT signatories, limits etc.
  - Network eavesdropping allowed us to intercept all network traffic between the EFT system and workstations, including usernames & passwords.

## Case Study : Electronic Funds Transfer

- **Results:**
  - Accessed the EFT system.
  - With the information obtained above it was trivial to log onto the EFT system as a privileged user and process transactions.
  - We were not detected.
  - The route we followed to achieve our objectives indicates the importance of a comprehensive security architecture.

# Why test?

*Determine the likelihood of and impact of the compromise of **users** through use of non-technical means*

## Case Study : End User Computing

- **Scenario :**

  A prominent financial services group approached us to perform a social engineering exercise to test the level of security awareness of their employees.

- **Objective :**

  To obtain unauthorized access to employees workstations/network access. Specifically senior management was targeted.

## Case Study : End User Computing

- **Champion :**

  The work was commissioned by senior management of a business division, with the knowledge of IT executives.

- **Purpose :**

  To gain an understanding of the general level of security awareness within the organisation.

## Case Study : End User Computing

- **Outcome :**
  - We were able to collect usernames and passwords from 9/10 employees targeted
  - Gained access to network and workstations of these key personnel (Secretary of director, Senior managers)
  - Organisation failed the test

# Case Study : End User Computing

- **How It Was Done :**
  - Used company phone list to identify senior management staff and select targets
  - Used the switchboard to “spoof” and hide the origin of our calls. All our calls appeared to be from internal.

## Case Study : End User Computing

- **How It Was Done Continued :**
  - Pretended a dangerous virus was present and all data could be lost
  - Informed user that automatic update had failed and updated must be done manually
  - Employees “panicked” and simply gave us their usernames and passwords.

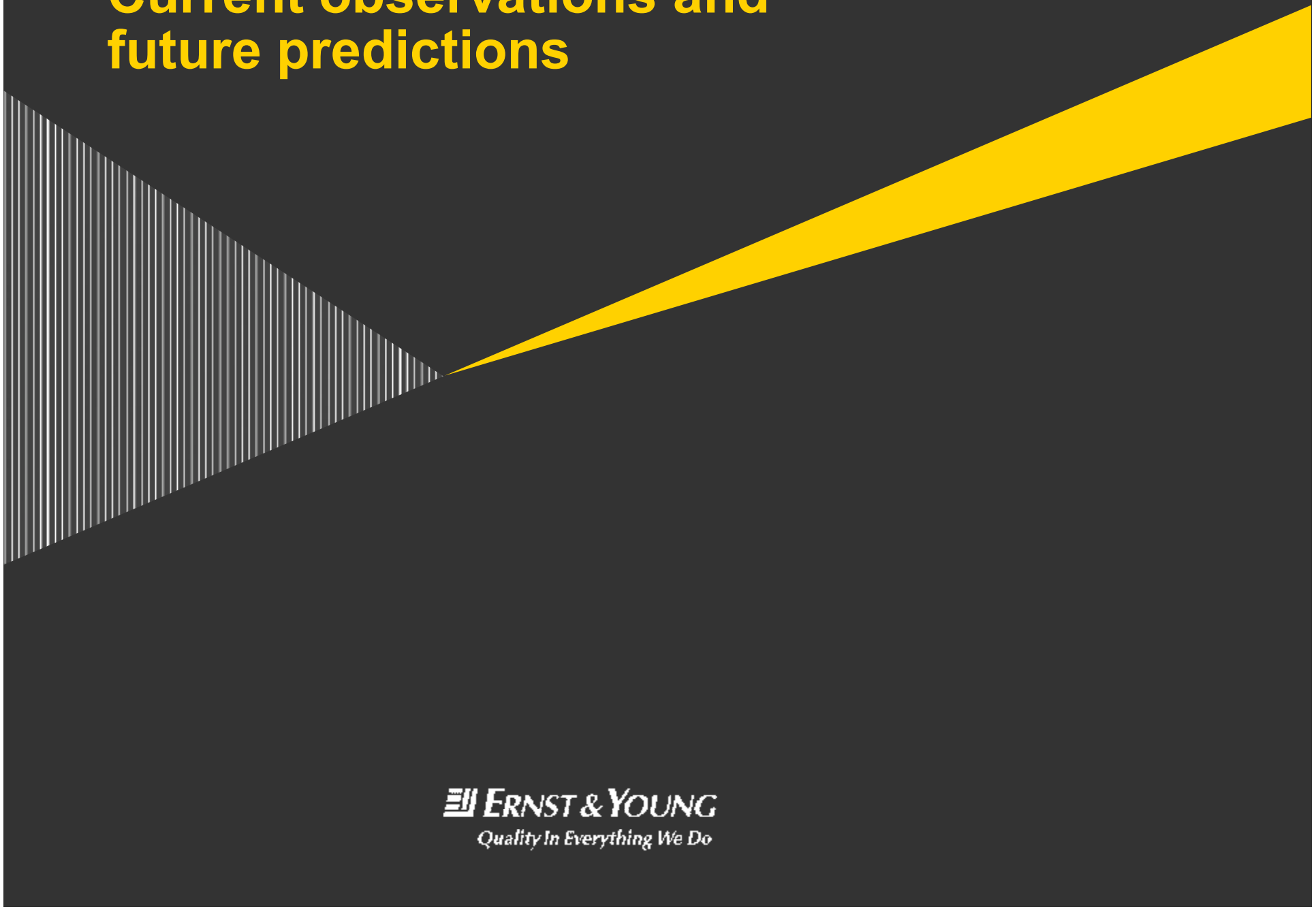
## Case Study : End User Computing

- **Results:**
  - 9 employees' workstations and network access was compromised.
  - 1 employee was alert and did not compromise the organisation
  - Employees did not adhere to company policy.
  - The information obtained through social engineering could be used to further infiltrate the organisation.

# Case Study : End User Computing

- **Other social engineering methods:**
  - Handing out memory sticks
  - Facebook / Linkedin / Twitter

# Current observations and future predictions



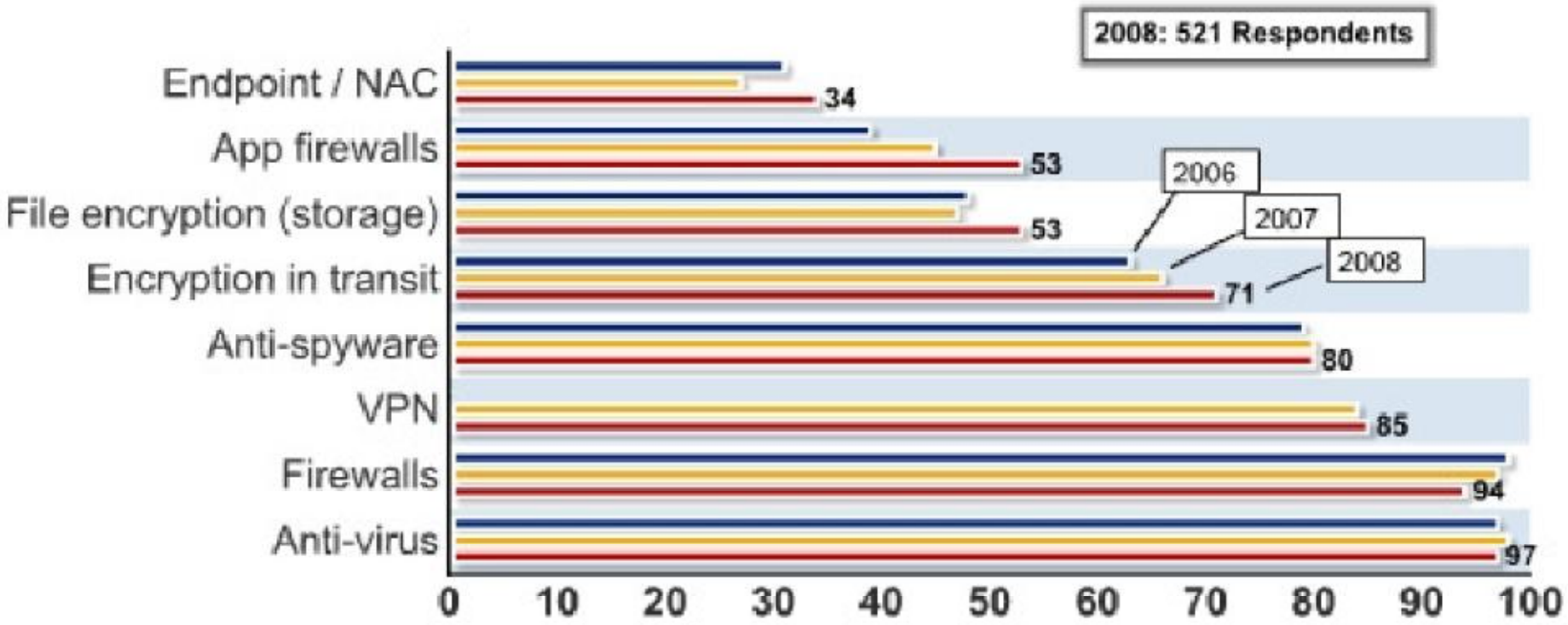
ERNST & YOUNG
Quality In Everything We Do

# Observations

- Attitude towards security is improving significantly
  - Appointment of security officers
  - Moving beyond policy, procedure and standards
    - More than just operating systems
    - Scorecards & dashboards
    - Self assessment
    - Ongoing compliance testing
  - Protecting reputation and brand become a significant driver
- Privacy has been identified as requiring action
  - Protection of personal information act/bill

# CSI FBI 2008 Survey : Technology used

Figure 16: Security Technologies Used



# CSI FBI 2008 Survey : Technology used

| Table 2: Technologies Used | 2008 |
|---|---|
| Anti-virus software | 97 % |
| Anti spyware software | 80 % |
| Application-level firewalls | 53 % |
| Biometrics | 23 % |
| Data loss prevention / content monitoring | 38 % |
| Encryption of data in transit | 71 % |
| Encryption of data at rest (in storage) | 53 % |
| Endpoint security client software / NAC | 34 % |
| Firewalls | 94 % |
| Forensics tools | 41 % |
| Intrusion detection systems | 69 % |
| Intrusion prevention systems | 54 % |
| Log management software | 51 % |
| Public Key Infrastructure systems | 36 % |
| Server-based access control lists | 50 % |
| Smart cards and other one-time tokens | 36 % |
| Specialized wireless security systems | 27 % |
| Static account / login passwords | 46 % |
| Virtualization-specific tools | 29 % |
| Virtual Private Network (VPN) | 85 % |
| Vulnerability / patch management tools | 65 % |
| Web / URL filtering | 61 % |
| Other | 3 % |

# Biggest Issues for South African Companies

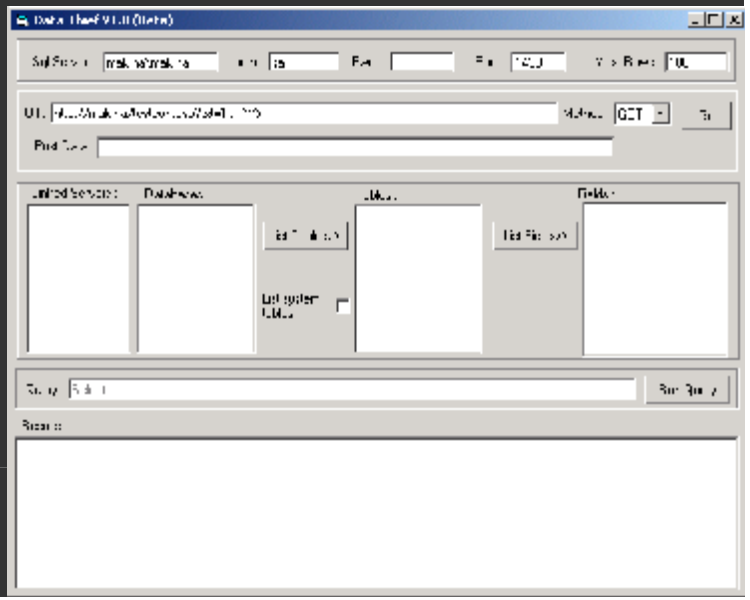
- Strategic
  - Privacy
  - Protection of reputation and brand
  - King 3 compliance
- Technical
  - Patch management
  - Secure Solution Selection and implementation
  - Complexity of environment (and trust)
  - User environment (Workstations) not secured
  - Data moving to the cloud
  - Skills, cost of skills and cost of technology solutions
- Procedural
  - Ongoing compliance
  - Poor administrative practices
  - User Education

# Next big things

- Smart code
  - Trojans / worms bypass current security measures
  - Embedding the code in the web browser
    - Commits actions on behalf of user (withdraw funds)
    - Changes what is displayed (fraudulent transactions eliminated)
  - Exploits end user applications : Windows Media Player, Winamp, Mirc or any others
  - Machines “protected” by corporate firewalls are accessible to hackers on the outside
- Cloud computing
  - Ownership and data security
  - Business continuity
  - Ability to switch service providers

# Next big things

- Hacking “other” Network devices
  - Printers
  - Routers, switches, gateways
  - PABX Systems
  - Voice over IP
  - Mobile devices (Blackberry etc)
- Higher application layers
  - Databases
    - Automated tools already available to attack databases and web based applications (Eg. DataThief)
  - Application specific attacks
    eg. Recent SCADA attacks



# Participating further

- ISACA KZN Chapter
  - WWW.ISACA.ORG.ZA
- ISG Africa / Whitehat
  - Regular meetings at UKZN : WWW.ISGAFRICA.ORG
- Institute of Internal Auditors – IT SIG
  - WWW.IIA.ORG.ZA
- Podcasts
  - WWW.DISCUSSIT.CO.ZA
- Follow me on twitter : jjza

# Questions ??

Contact :

- Email : justin.williams@za.ey.com
- Alternate : justin@j-j.co.za
- Mobile : 082 772 9881
- Website : http://j-j.co.za
- 

jjza
http://twitter.com/jjza
- 

Justin Williams, Durban, SA