Introduction To Computer Security

By

Hafez Barghouthi

Agenda Today

- Terminology(What)
- Security strategies
  - Prevention – detection – reaction
- Security objectives
  - Confidentiality – integrity – availability
  - Accountability – non-repudiation
  - authentication
- Fundamental dilemma of Computer Security
- Principles of Computer Security
- The layer below.
- Computer Attack Analysis (Why)

What security is about in general?

- Security is about protection of assets
  - D. Gollmann, Computer Security, Wiley
- Prevention
  - take measures that prevent your assets from being damaged (or stolen)
- Detection
  - take measures so that you can detect when, how, and by whom an asset has been damaged
- Reaction
  - take measures so that you can recover your assets

Real world example

- Prevention
  - locks at doors, window bars, secure the walls around the property, hire a guard
- Detection
  - missing items, system alarms, closed circuit TV
- Reaction
  - call the police, replace stolen items, make an insurance claim

Internet shopping example

- Prevention
  - encrypt your order and card number, enforce merchants to do some extra checks, don't send card number via Internet
- Detection
  - an unauthorized transaction appears on your credit card statement
- Reaction
  - complain, dispute, ask for a new card number, sue (if you can find of course ☺)
  - Or, pay and forget (a glass of cold water) ☺

A note on security terminology

- No single and consistent terminology in the literature!
- Be careful not to confuse while reading papers and books
- See the next slide for some terminology taken from Gollmann.

Basic security concepts

- Confidentiality: prevent unauthorised disclosure of information
- Integrity: prevent unauthorised modification of information
- Availability: prevent unauthorised withholding of information or resources
- Authenticity: "know whom you are talking to"
- Accountability (non-repudiation): prove that an entity was involved in some event

Confidentiality

- Prevent unauthorised disclosure of information (prevent unauthorized reading).
- Secrecy: protection of data belonging to an organisation.
- Historically, security and secrecy were closely related; security and confidentiality are sometimes used as synonyms.
- Do we want to hide the content of a document or its existence?
  - Traffic analysis in network security.
  - Anonymity, unlinkability

Privacy

- Privacy: protection of personal data (OECD Privacy Guidelines, EU Data Privacy Directive 95/46/EC).
- "Put the user in control of their personal data and of information about their activities."
- Taken now more seriously by companies that want to be 'trusted' by their customers.
- Also: The right to be left alone (e.g. not to be bothered by spam).

Privacy

- **OECD Privacy Guidelines,** Established by the **Organization for Economic Cooperation and Development (OECD)** in 1980, these guidelines outline principles for the protection of privacy and personal data. The principles include:
- **Collection Limitation Principle**: Limiting the collection of personal data to what is necessary for specified purposes.
- **Data Quality Principle:** Ensuring that personal data collected is accurate, relevant, and up to date.
- **Purpose Specification Principle:** Specifying the purposes for which personal data is collected and processed, and obtaining consent from individuals for such purposes.
- **Use Limitation Principle:** Restricting the use of personal data to the purposes for which it was collected, and preventing unauthorized access or disclosure.
- **Security Safeguards Principle:** Implementing appropriate security measures to protect personal data against unauthorized access, disclosure, alteration, or destruction.

Integrity

- Prevent unauthorised modification of information (prevent unauthorised writing).
- Data Integrity - The state that exists when computerized data is the same as that in the source document and has not been exposed to accidental or malicious alteration or destruction. (Integrity synonymous for external consistency.)
- Detection (and correction) of intentional and accidental modifications of transmitted data.

Integrity continued

- Clark & Wilson: No user of the system, even if authorized, may be permitted to modify data items in such a way that assets or accounting records of the company are lost or corrupted.
- In the most general sense: make sure that everything is as it is supposed to be.

  (This is highly desirable but cannot be guaranteed by mechanisms internal to the computer system.)
- Integrity is a prerequisite for many other security services; operating systems security has a lot to do with integrity.

OS Data Integrity

- OS must ensure about the integrity of data stored on the system, this involve preventing unauthorized modification, deletion, tampering with files.
- **Code integrity**, Operating systems execute a wide range of software, including applications, device drivers, and system utilities. Code integrity mechanisms help verify that this software has not been altered or compromised, ensuring that only authorized and unmodified code is executed. one of techniques that used for this purpose is **Code Signing and Verification,** All executable files and system libraries within the operating system are digitally signed by trusted source.

OS Data Integrity

- **System Integrity:** The overall integrity of the operating system itself is crucial. Operating systems should be resistant to unauthorized changes that could compromise their stability, security, or functionality. Protecting system integrity involves measures such as **secure boot processes**, **file system protections**, and **kernel integrity checks**, based on using techniques such as Files integrity checks.

OS Data Integrity

- **User Integrity:** Operating systems must maintain the integrity of user accounts and privileges. This includes preventing unauthorized users from gaining access to sensitive resources, ensuring that users cannot escalate their privileges beyond what is necessary for their tasks, and detecting and mitigating unauthorized activities.
- **Secure Communication:** Operating systems often facilitate communication between different components, applications, and networked systems. Integrity mechanisms, such as **cryptographic protocols** and **digital signatures**, help ensure the integrity of data transmitted over networks, protecting it from unauthorized modification or tampering during transit.

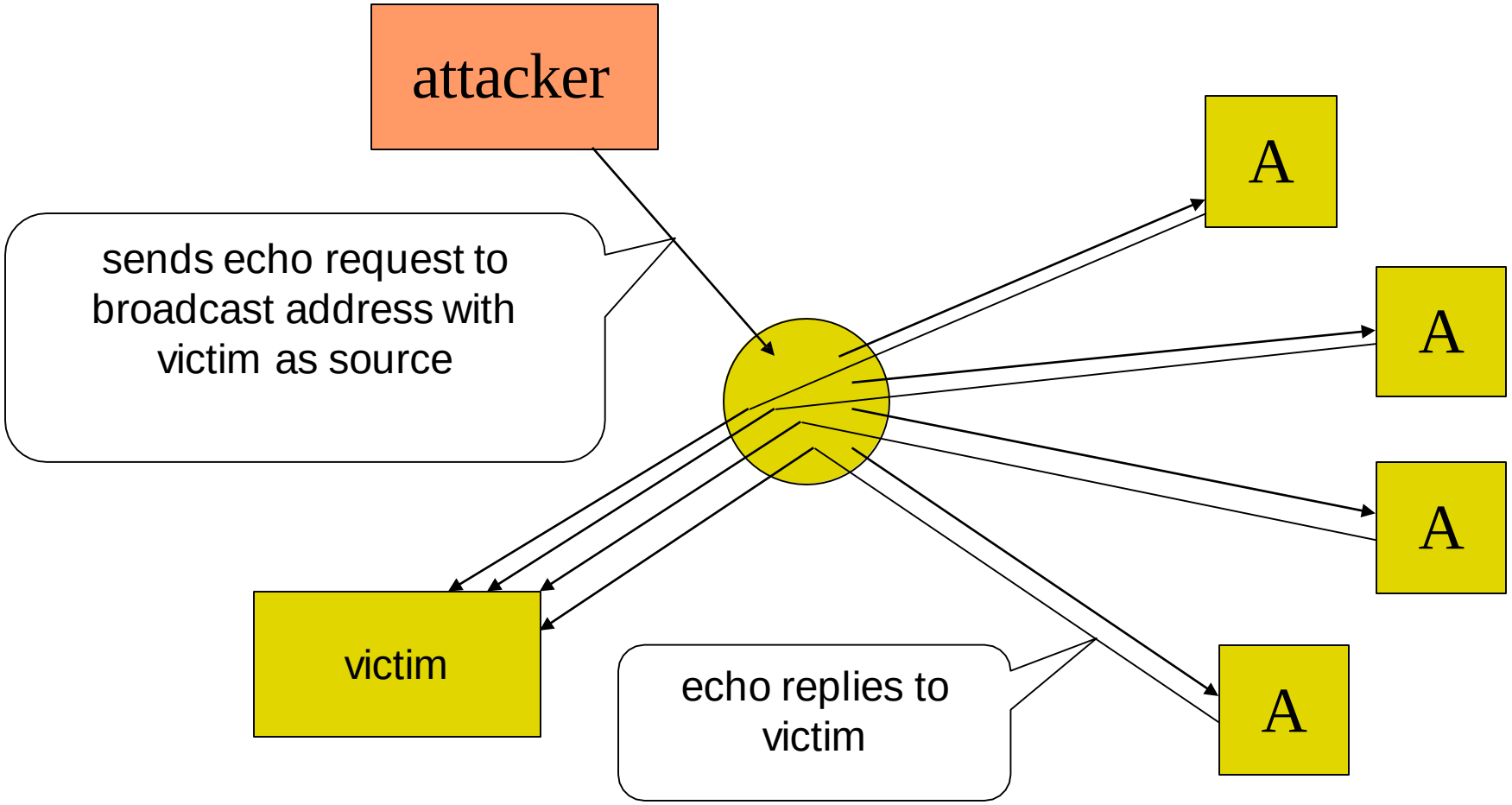
Availability

- The property of being accessible and usable upon demand by an authorised entity.
- Denial of Service (DoS): The prevention of authorised access of resources or the delaying of time-critical operations.
- Maybe the most important aspect of computer security, but few methods are around.
- Distributed denial of service (DDoS) receives a lot of attention; systems are now designed to be more resilient against these attacks.

Denial of Service Attack (smurf)

- Attacker sends Internet Control Message Protocol (ICMP) echo requests to a broadcast address, with the victim's address as the spoofed sender address.
- The echo request is distributed to all nodes in the range of t he broadcast address.
- Each node replies with an echo reply to the victim.
- The victim is flooded with many incoming message s.
- Note the amplification: the attacker sends one message, the victim receives many.

Denial of Service Attack (smurf)



www.wiley.com/go/gollmann

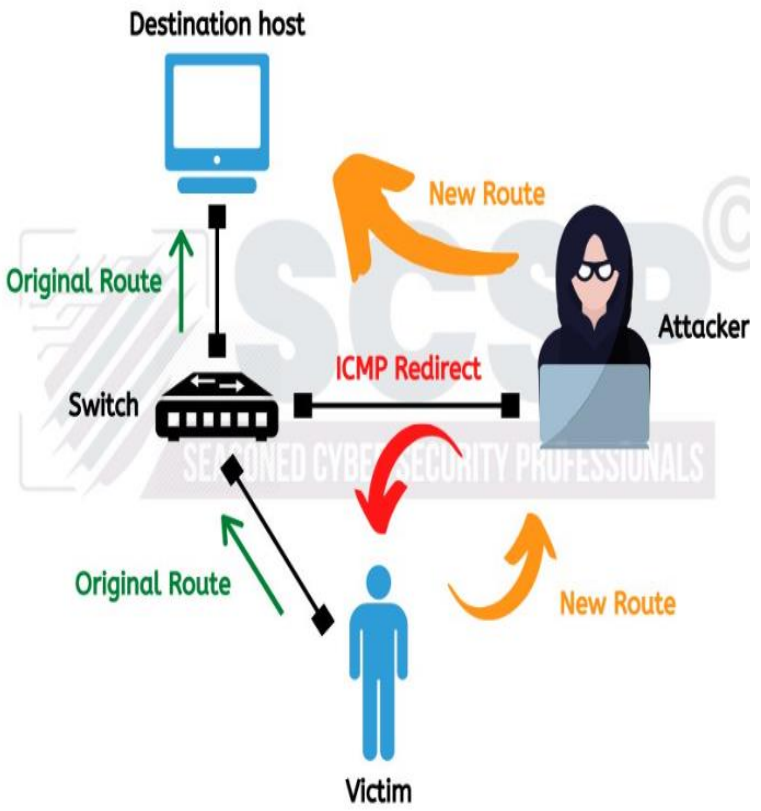
ICMP Fragmentation Attack

ICMP Fragmentation Attack: two main types of this attacks,

- first one refers submit fake fragments that cannot be defragmented. This in turn causes the fragments to be placed in temporary storage, taking up memory and in some cases exhausting all available memory resources. This can be generated using UDP flooding, whereas the botnet used to send large volume of fragments from numerous resources.
- UDP and ICMP fragmentation DDoS attacks – In this type of DDoS attack, fake UDP or ICMP packets are transmitted. These packets are designed to look like they are larger than the network's MTU, but only parts of the packets are actually sent. Since the packets are fake and can't be reassembled, the server's resources are quickly consumed, which ultimately renders it unavailable to legitimate traffic.

ICMP Redirect Attack

- An ICMP redirect message is an out-of-band message that is designed to inform a host of a more optimal route through a network, but possibly used maliciously for attacks that redirect traffic to a specific system. In this type of an attack, **the hacker, posing as a router, sends an Internet Control Message Protocol (ICMP) redirect message to a host, which indicates that all future traffic must be directed to a specific system as the more optimal route for the destination.**



Accountability

Accountability refers to the responsibility that individuals, organizations, or entities have for their actions, decisions, and behaviors, and the obligation to justify or answer for the consequences of those actions.

- At the operating system level, audit logs record security relevant events and the user identities associated with the se events.
- If an actual link between a user and a "user identity" can be established, the user can be held accountable.
- In distributed systems, cryptographic non-repudiation mechanisms can be used to achieve the same goal.

Non-repudiation

- Nonrepudiation services provide unforgeable evidence that a specific action occurred.
- Nonrepudiation of origin protects against a sender of da ta denying that data was sent.
- Nonrepudiation of delivery protects against a receiver of data denying that data was received.
- Digital signatures using private key, consensus algorithm in blockchain.

Reliability & Safety

- Reliability and safety are related to security:
  - Similar engineering methods,
  - Similar efforts in standardization,
  - Possible requirement conflicts, implementing stringent security measures (such as encryption or access controls) to protect against cyber threats may introduce complexity or performance overhead that could impact system reliability or safety.
- Reliability addresses the consequences of accidental errors, which means that reliability refers to the ability of the system to consistently and accurately perform its intended functions while minimizing the risk of failures, errors, or vulnerabilities that could compromise security.
- Is security part of reliability or vice versa?
- Safety: Measure of the absence of catastrophic influences on the environment, in particular on human life.

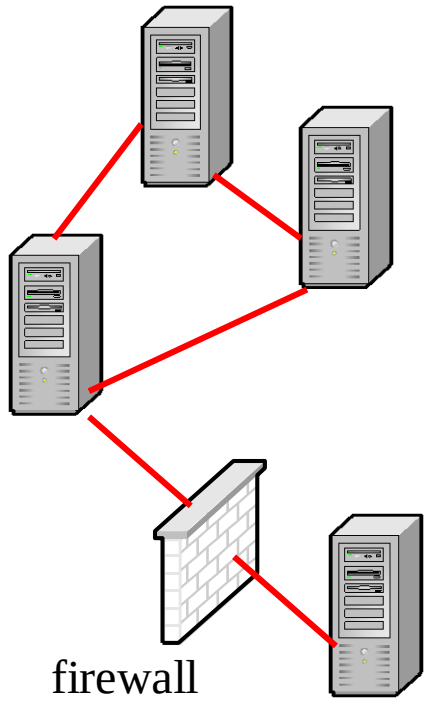
Dependability

- Proposal for a term that encompasses reliability, safety, and security
- Dependability (IFIP WG 10.4):
  - The property of a computer system such that reliance can justifiably be placed on the service it delivers. The service delivered by a system is its behavior as it is perceived by its user(s); a user is another system (physical, human) which interacts with the former.

www.wiley.com/go/gollmann

Aspects of Security

- Distributed systems: computers connected by networks
- Communications (network) security: addresses security of the communications links
- Computer security: addresses security of the end systems; today, this is the difficult part
- Application security: relies on both to provide services securely to end users
- Security management: how to deploy security technologies



www.wiley.com/go/gollmann

The Fundamental Dilemma of Computer Security

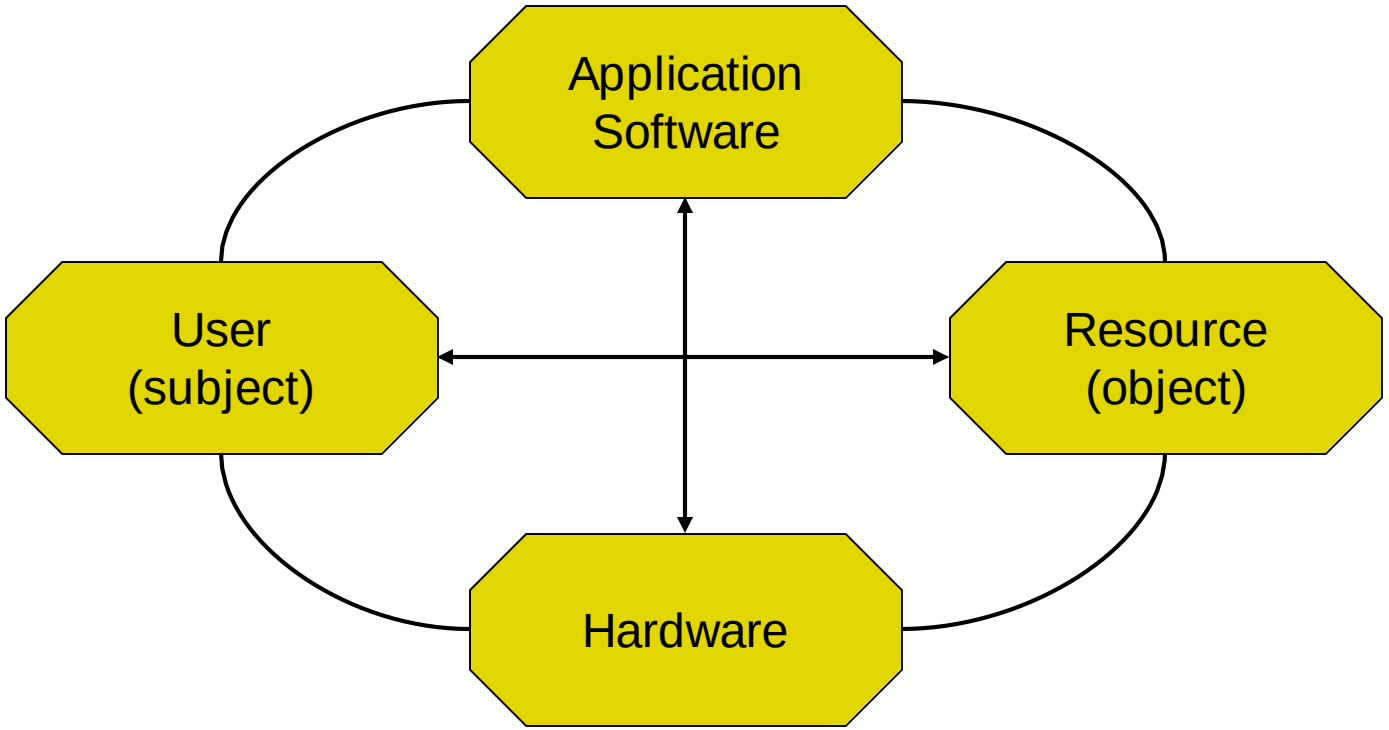
Security unaware users have specific security requirements but no security expertise.

- The Fundamental Dilemma of Computer Security refers to the inherent challenge of balancing security measures with usability and convenience.
- If you provide your customers with a standard solution it might not meet their requirements.
- If you want to tailor your solution to your customers' needs, they may be unable to tell you what they require.

www.wiley.com/go/gollmann

Principles of Computer Security

The Dimensions of Computer Security



www.wiley.com/go/gollmann

1st Fundamental Design Decision

Where to focus security controls?

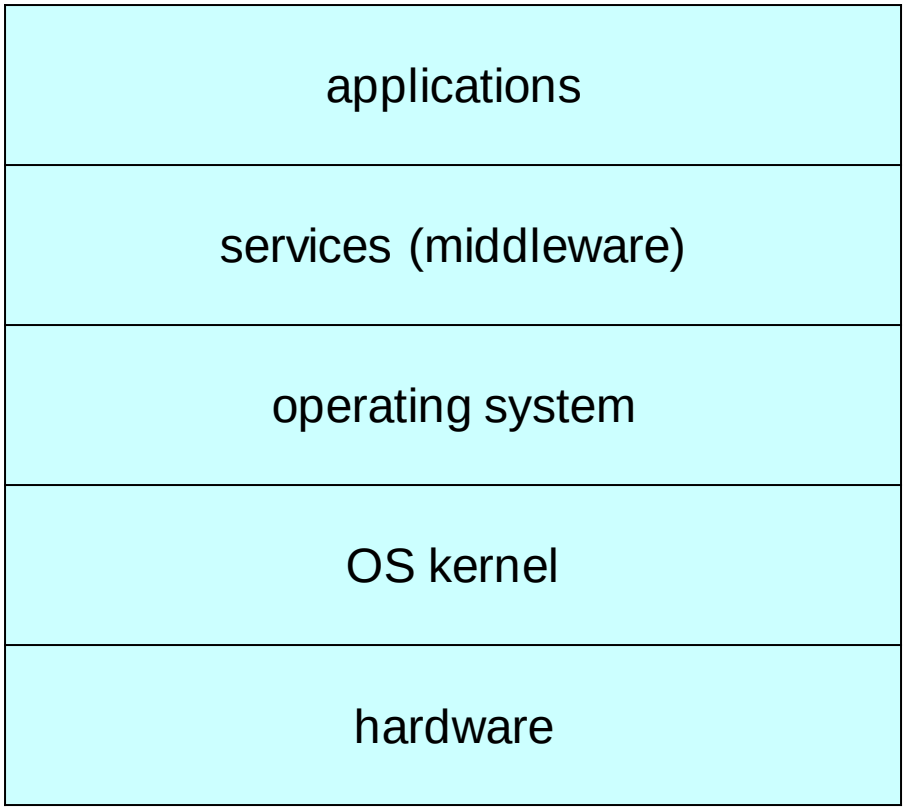
The focus may be on data – operations – users; e.g. integrity requirements may refer to rules on

- Format and content of data items (internal consistency): account balance is an integer.
- Operations that may be performed on a data item: credit, debit, transfer, …
- Users who are allowed to access a data item (authorised access): account holder and bank clerk have access to account.

www.wiley.com/go/gollmann

2nd Fundamental Design Decision

Where to place security controls?



www.wiley.com/go/gollmann

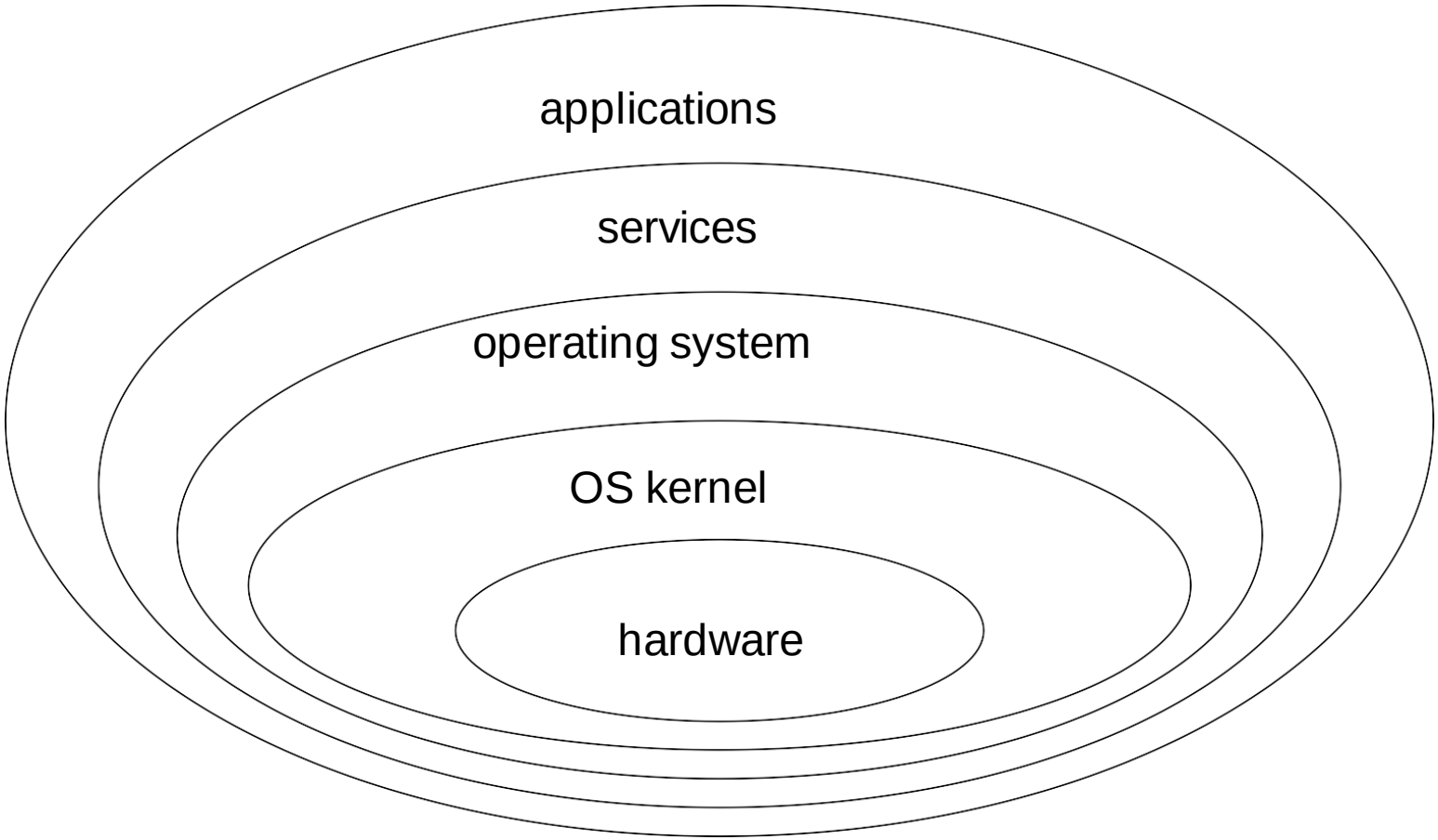
The Man-Machine Scale

- Visualize security mechanisms as concentric protection rings, with hardware mechanisms in the centre and application mechanisms at the outside.
- Mechanisms towards the centre tend to be more generic while mechanisms at the outside are more likely to address individual user requirements.
- The man-machine scale for security mechanisms combines our first two design decisions.

Défense in Depth

- Which can define as is a strategic approach to cybersecurity that emphasizes multiple layers of defense throughout an information system. The concept draws its inspiration from the layers of an onion, where each layer represents a different security measure, and even if one layer is breached, there are still more layers to protect the system.
- The basic idea behind the Onion Model is to provide redundancy and resilience in security measures. Instead of relying solely on one security mechanism (like a firewall or antivirus software), multiple layers are implemented to protect against a variety of threats.

Onion Model of Protection(Défense in Depth)



www.wiley.com/go/gollmann

Layers

- **Hardware layer,** whereas Security measures at this layer may include physical security controls such as locks, access control systems, and surveillance cameras.
- **Operating System Kernal Layer,** since the kernel refers to the core of OS which responsible for manage system resources and provide essential services to higher-level software. Security measures at this layer may include physical security controls such as locks, access control systems, secure inter-process communications, memory protection such as buffer overflow attack .
- **Operating System Layer,** Security measures at this layer include applying security patches and updates, configuring security settings (e.g., user permissions, firewall rules), and using security features provided by the operating system (e.g., built-in firewalls, encryption).

Layers

- **Services Layer,** which consists of various services such as web services, database server, email servers, and other network services. Securing these services involves hardening their configuration , limiting network exposure, and regularity patching vulnerabilities, and implementing security controls such as intrusion detection/prevention systems (IDS/IPS), access control lists (ACLs), and application firewalls.
- **Application Layer,** whereas Securing applications involves ensuring they are developed using secure coding practices, regularly updating them with security patches, and implementing additional security measures such as input validation, authentication, and authorization mechanisms.

The Man-Machine Scale

specific
complex
focus on users

generic
simple
focus on data

man
oriented

machine
oriented

www.wiley.com/go/gollmann

Data VS Information

Controlling access to information may be elusive and need to be replaced by controlling access to data.
If information and corresponding data are closely linked the two approaches give very similar results, but this is not always the case.

Inference in statistical databases: combine statistical queries to get information on individual entries.

Data VS Information

- Controlling Access to information, which involves **managing permissions and privileges based on the content and context of the information itself.**
- This approach focuses on **restricting access to specific pieces of information, regardless of the underlying data structure or storage mechanism.**
- Controlling Access to data, which involves **managing permissions and privileges based on the underlying data elements or records.**
- This approach focuses on granular control over individual data elements, attributes, or fields, rather than entire information objects.

3rd Fundamental Design Decision

Complexity or Assurance?

- Often, the location of a security mechanism on the man-machine scale is related to its complexity.
- Generic mechanisms are simple, applications clamour for feature-rich security functions.
- Do you prefer simplicity – and higher assurance – to a feature-rich security environment?

www.wiley.com/go/gollmann

4th Fundamental Design Decision
Centralized or decentralized control?

- Within the domain of a security policy, the same controls should be enforced.
- If a single entity is in charge of security, then it is easy to achieve uniformity but this central entity may become a performance bottleneck.

5th Fundamental Design Decision

Blocking Access to the Layer Below

- Attackers try to bypass protection mechanisms.
- There is an immediate and important corollary to the second design decision:
- How do you stop an attacker from getting access to a layer below your protection mechanism?

www.wiley.com/go/gollmann

Computer Attack Analysis

- Basic overview of:
  - Attack patterns
  - Countermeasures applied
  - Costs involved
- All figures from "CSI Computer Crime & Security Survey 2008" (www.gocsi.com)

Figure 6: Awareness Training as a Percentage of Security Budget

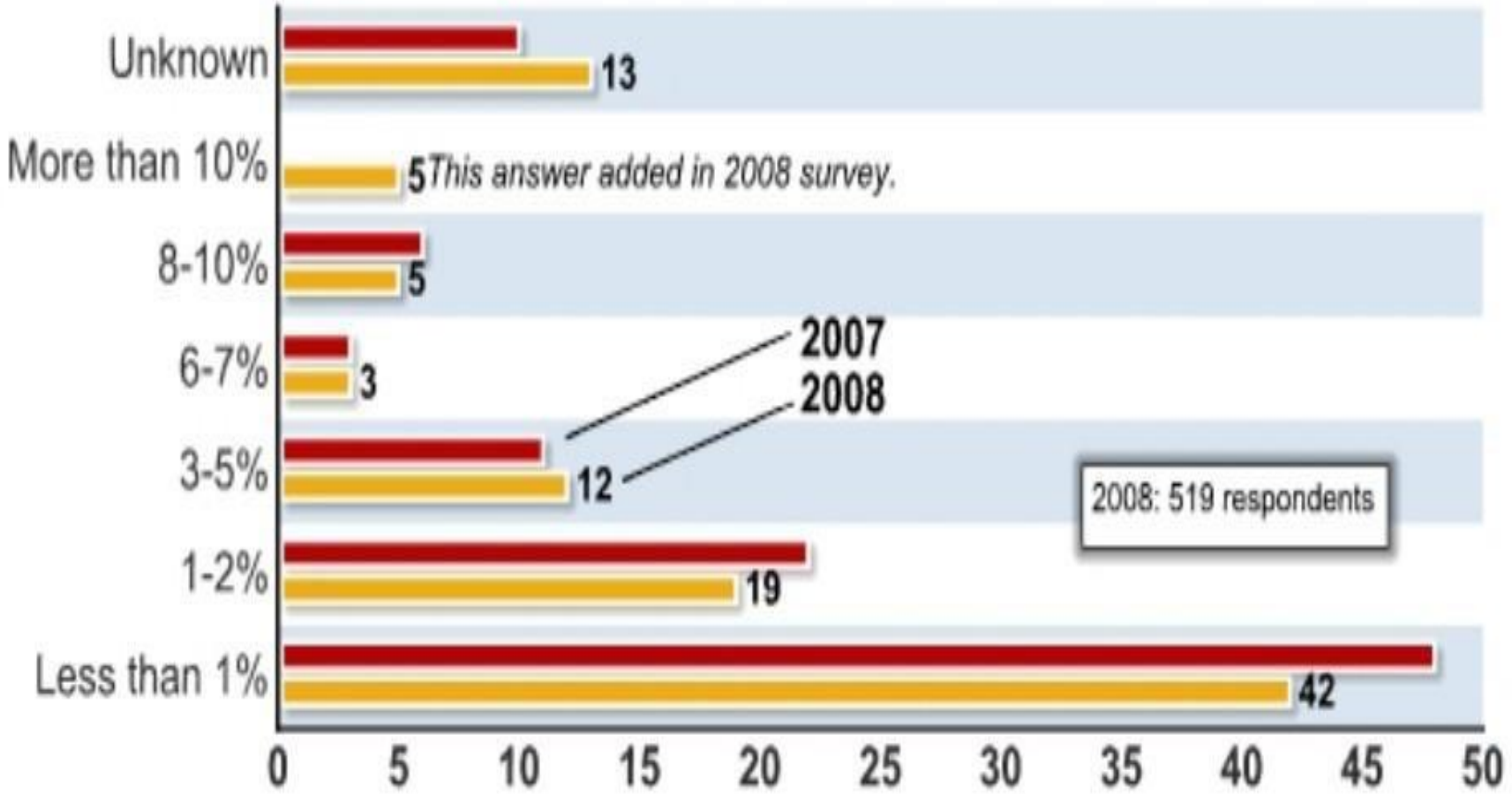
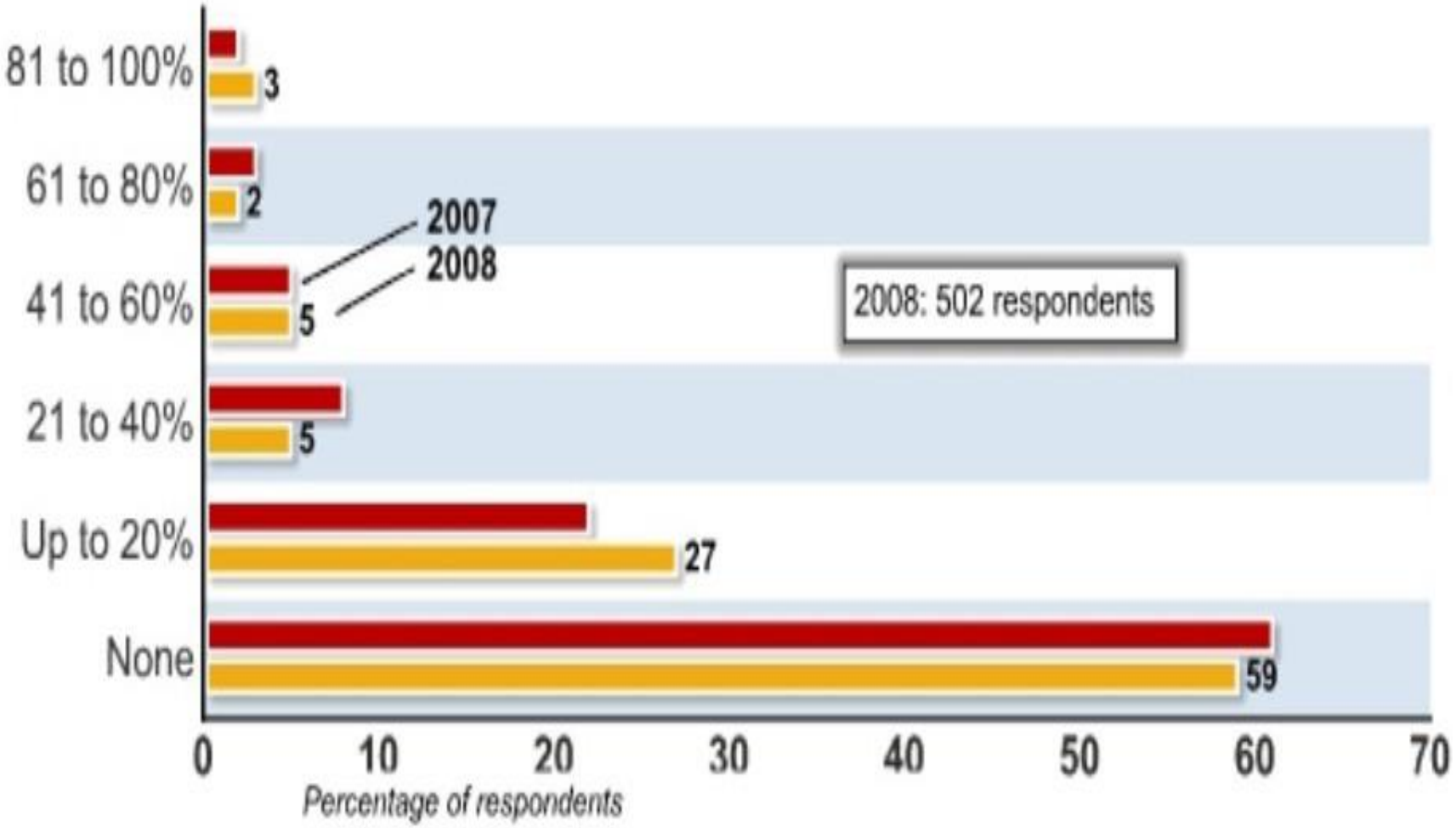


Figure 8: Percentage of Security Outsourced



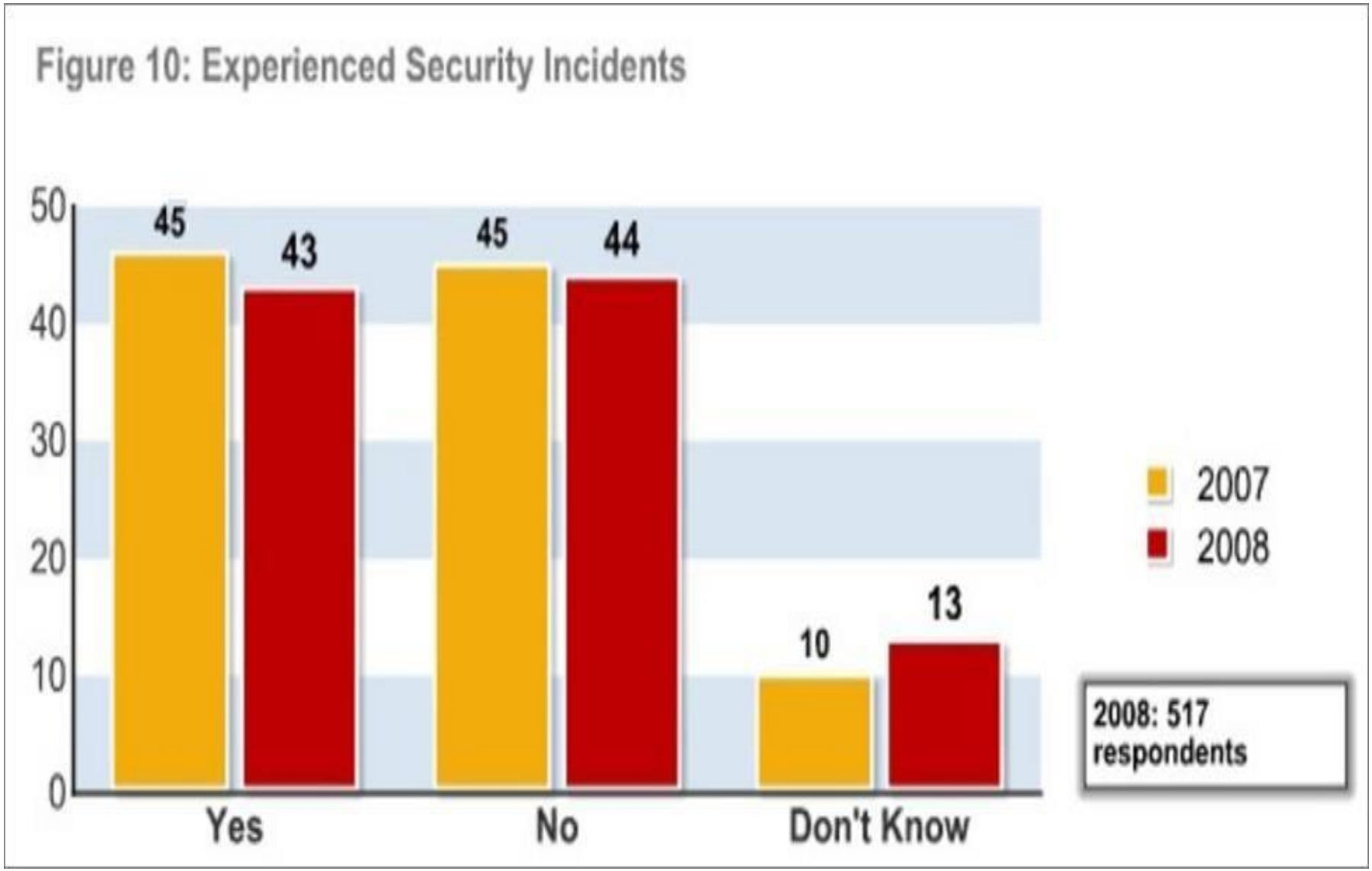


Figure 10: Experienced Security Incidents
50
40
30
20
10
0
45
43
45
44
10
13
Yes
No
Don't Know
2007
2008
2008: 517 respondents

Figure 11: Number of Incidents by Percentage

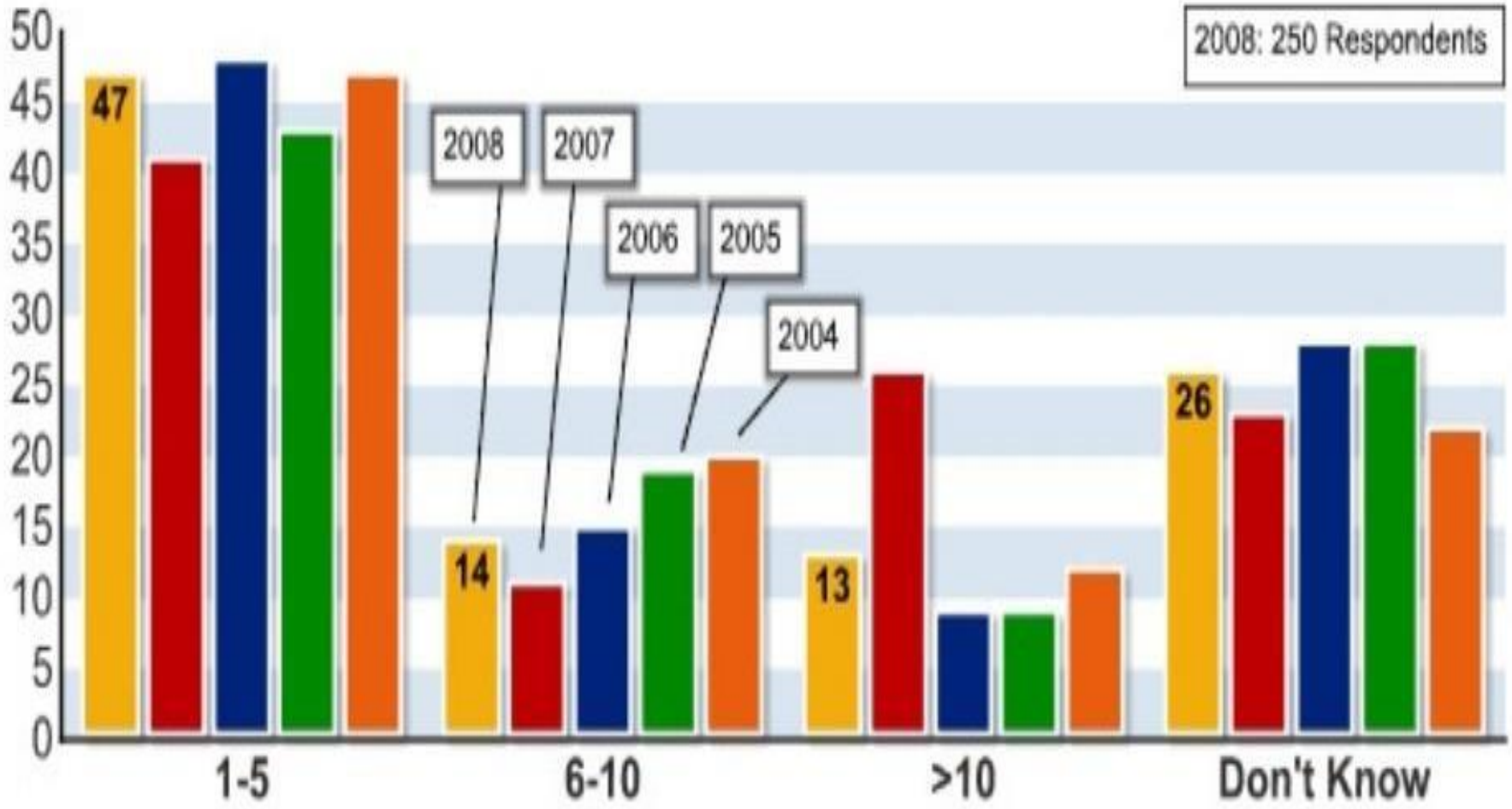
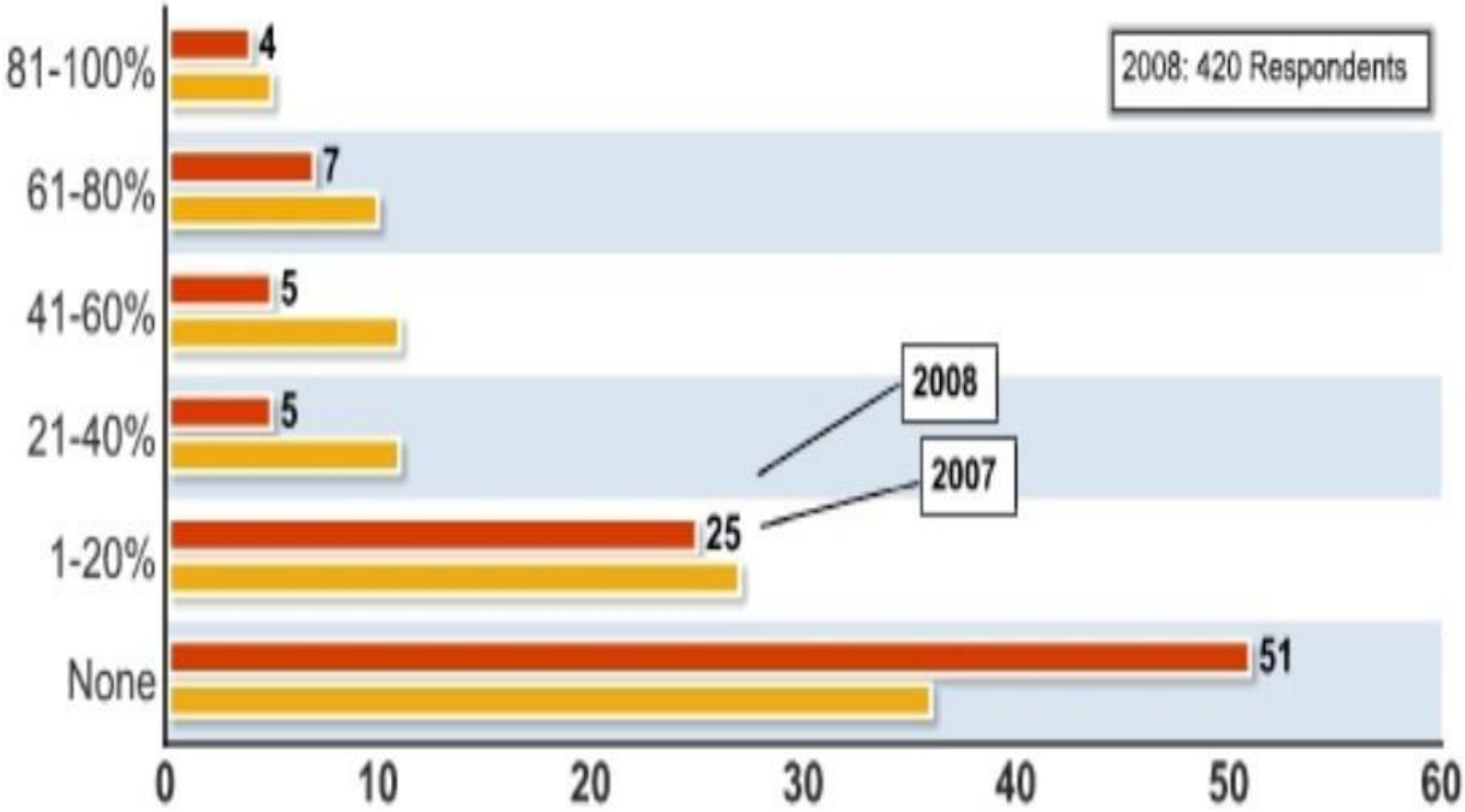


Figure 12: Percentage of Losses Due to Insiders



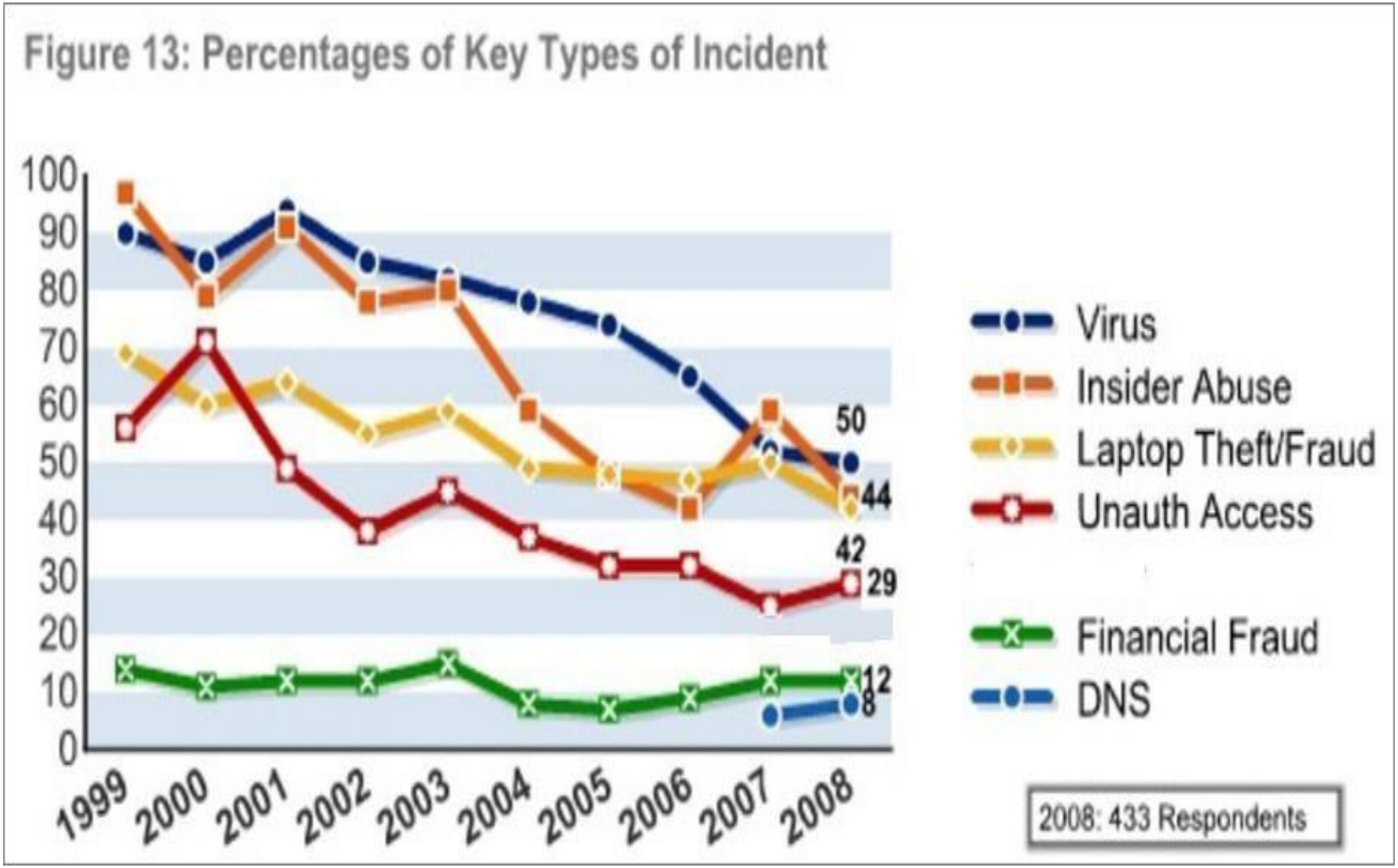


Table 1	2004	2005	2006	2007	2008
Denial of service	39%	32%	25%	25%	21%
Laptop theft	49%	48%	47%	50%	42%
Telecom fraud	10%	10%	8%	5%	5%
Unauthorized access	37%	32%	32%	25%	29%
Virus	78%	74%	65%	52%	50%
Financial fraud	8%	7%	9%	12%	12%
Insider abuse	59%	48%	42%	59%	44%
System penetration	17%	14%	15%	13%	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%

Figure 14: Average Losses Per Respondent

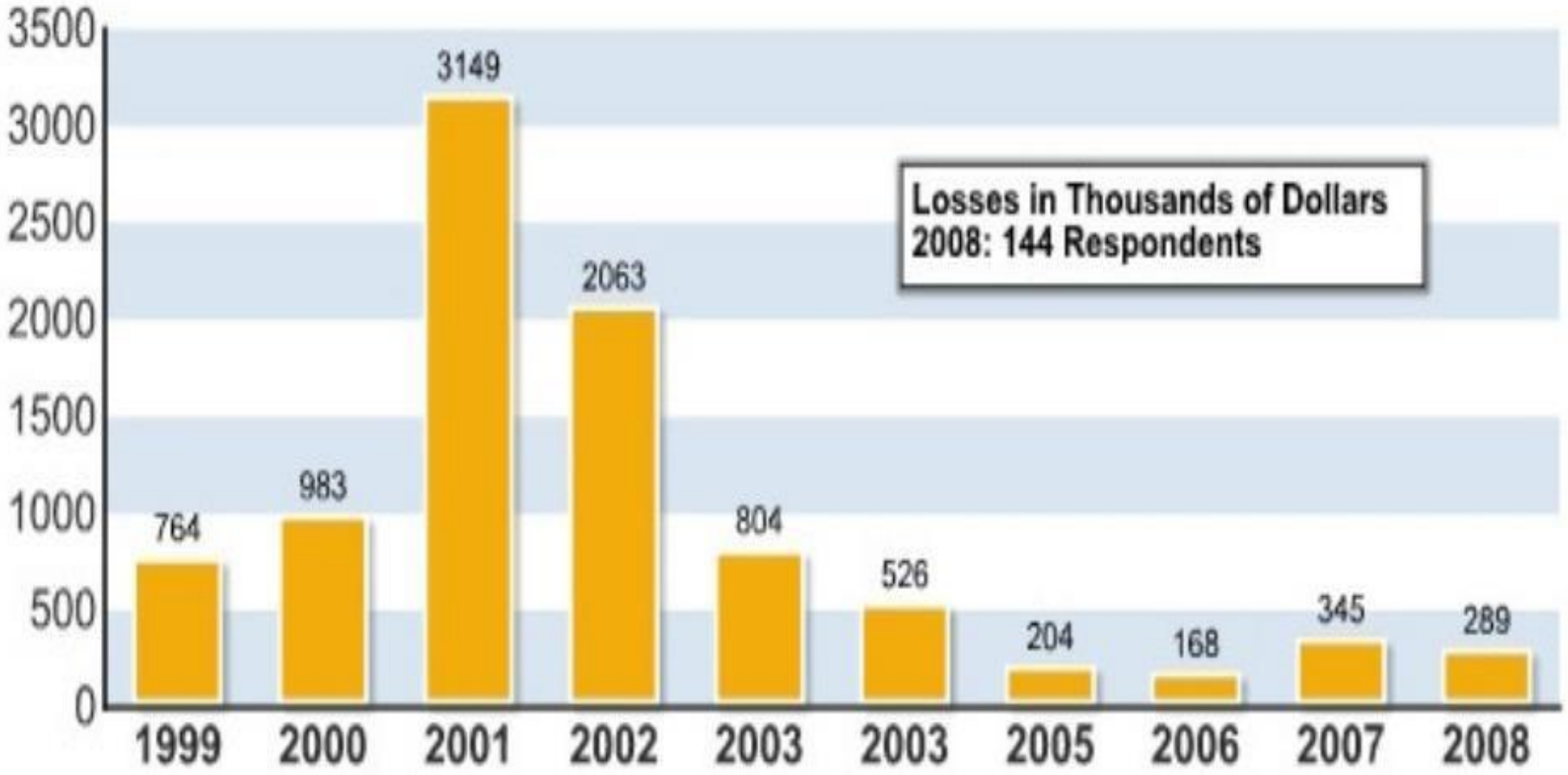


Figure 15: Number of Targeted Attacks

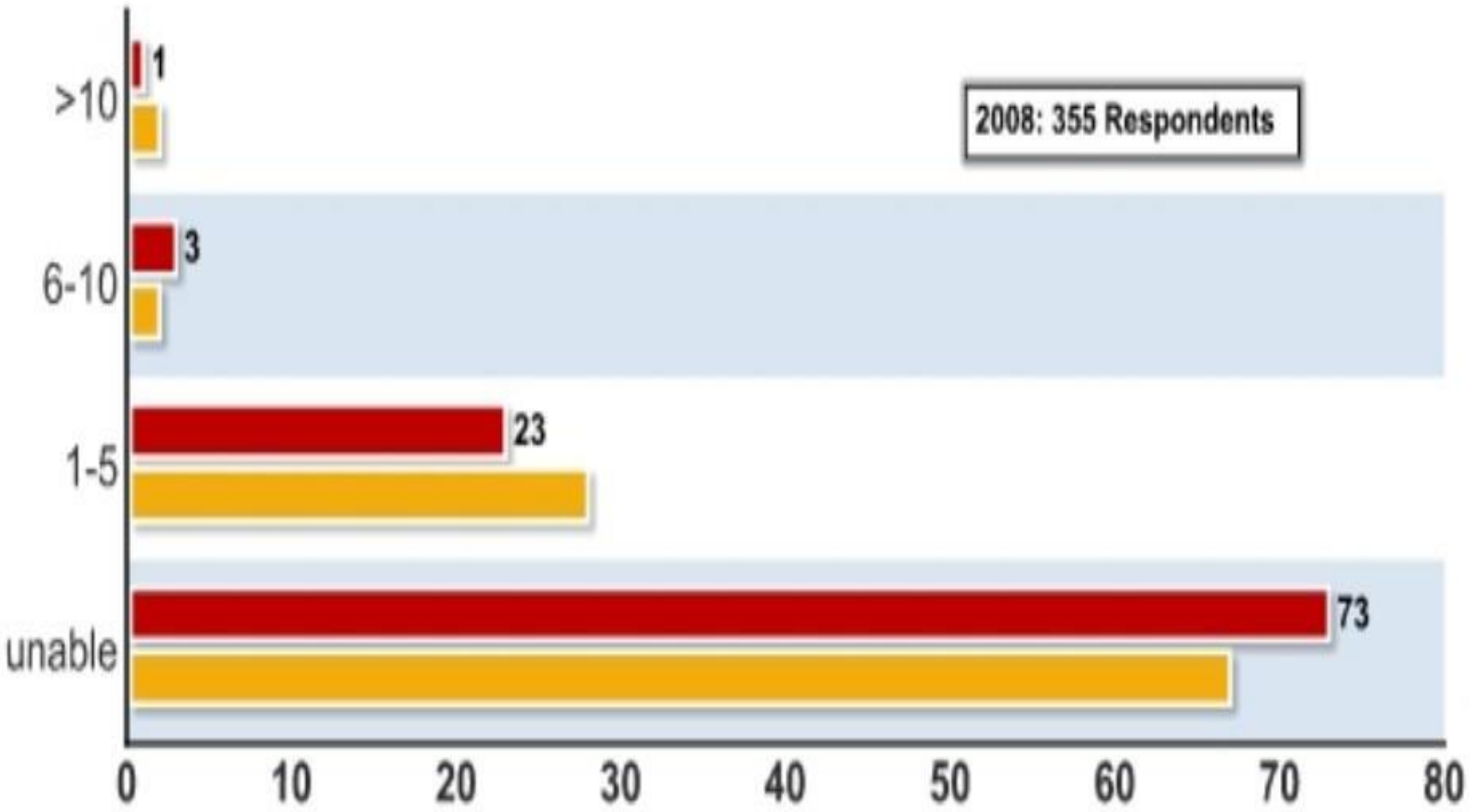


Figure 16: Security Technologies Used

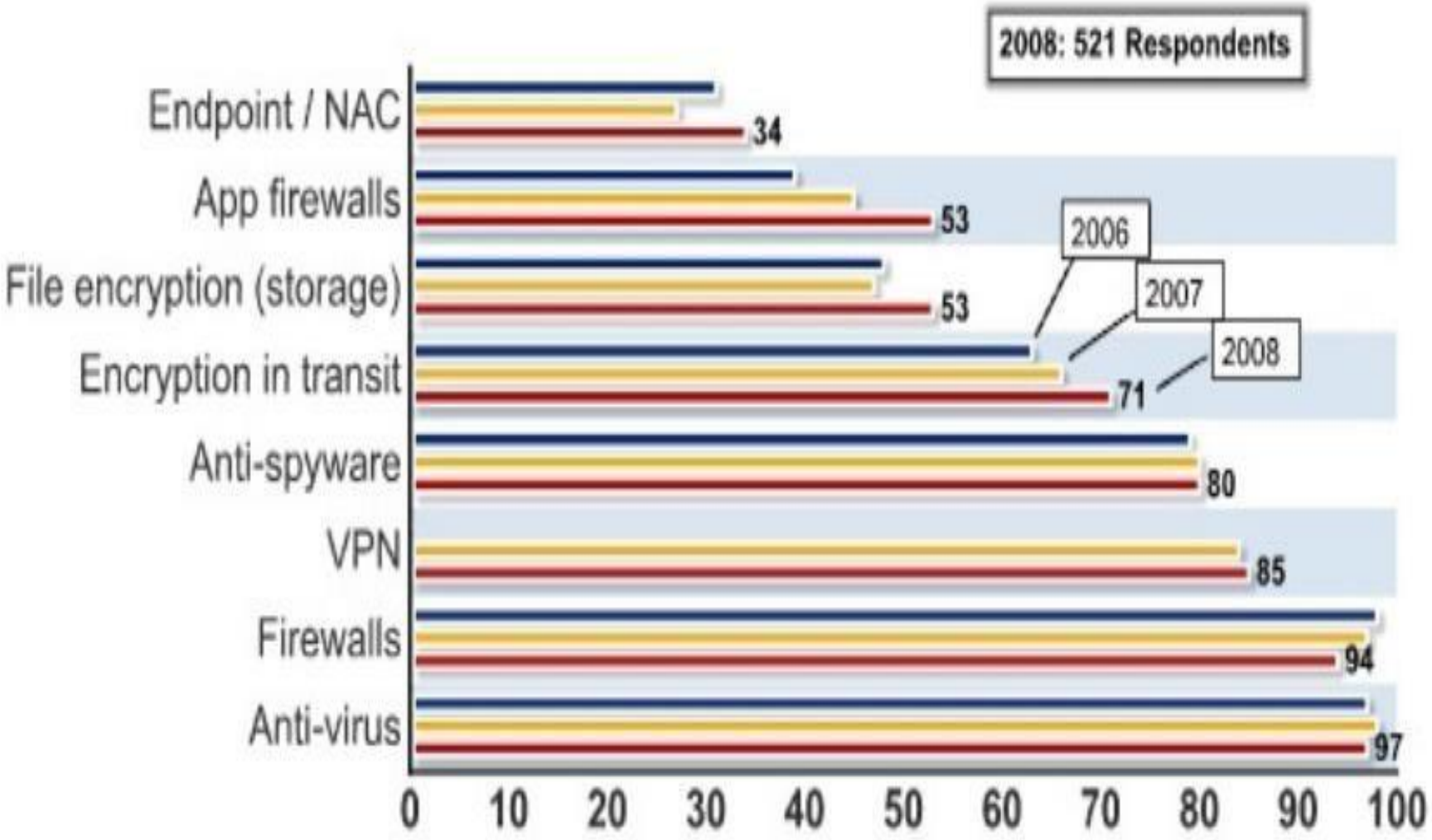


Table 2: Technologies Used	2008
Anti-virus software	97 %
Anti-spyware software	80 %
Application-level firewalls	53 %
Biometrics	23 %
Data loss prevention / content monitoring	38 %
Encryption of data in transit	71 %
Encryption of data at rest (in storage)	53 %
Endpoint security client software / NAC	34 %
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 %

Figure 17: Techniques Used To Evaluate Security Techology

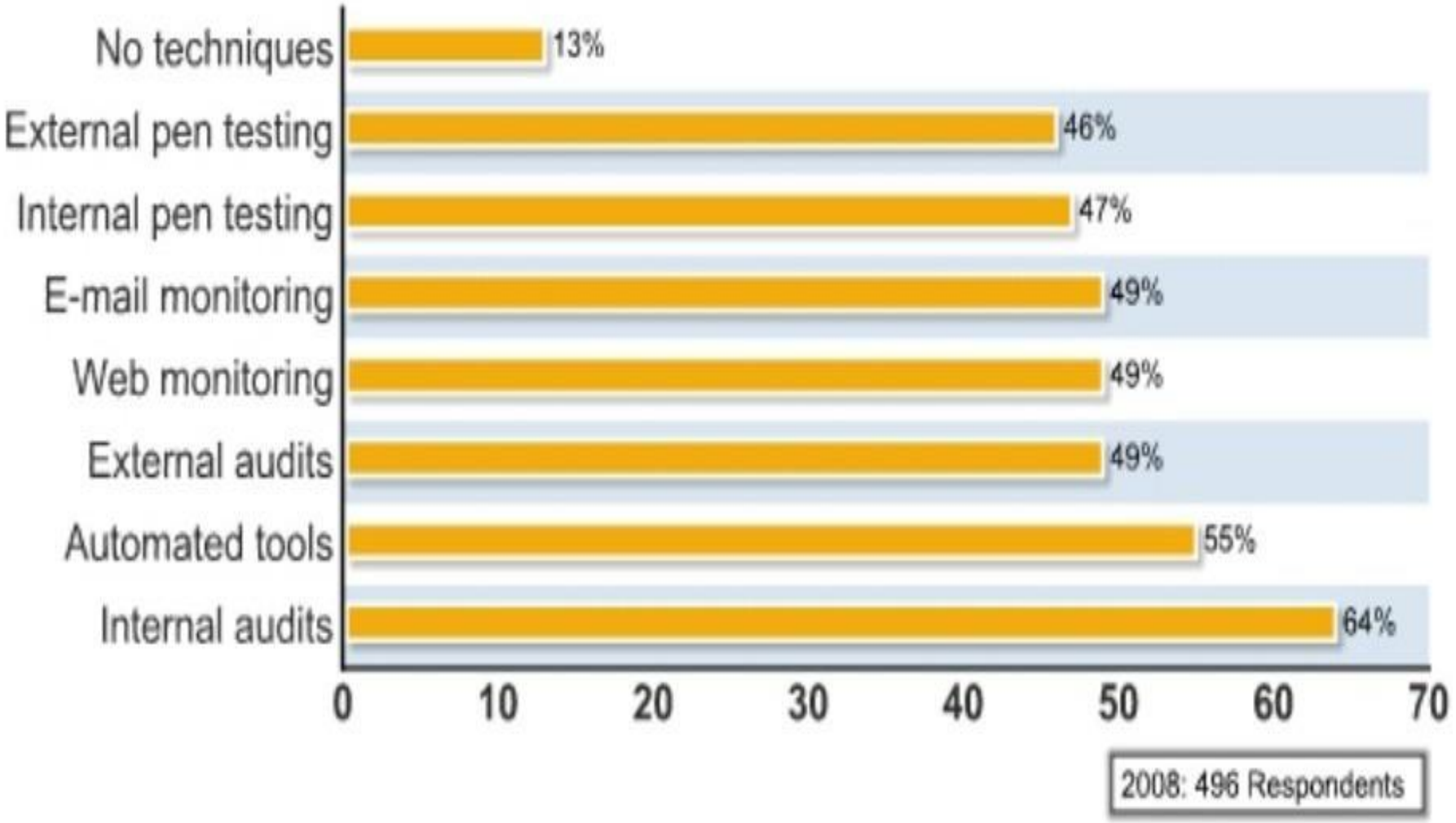
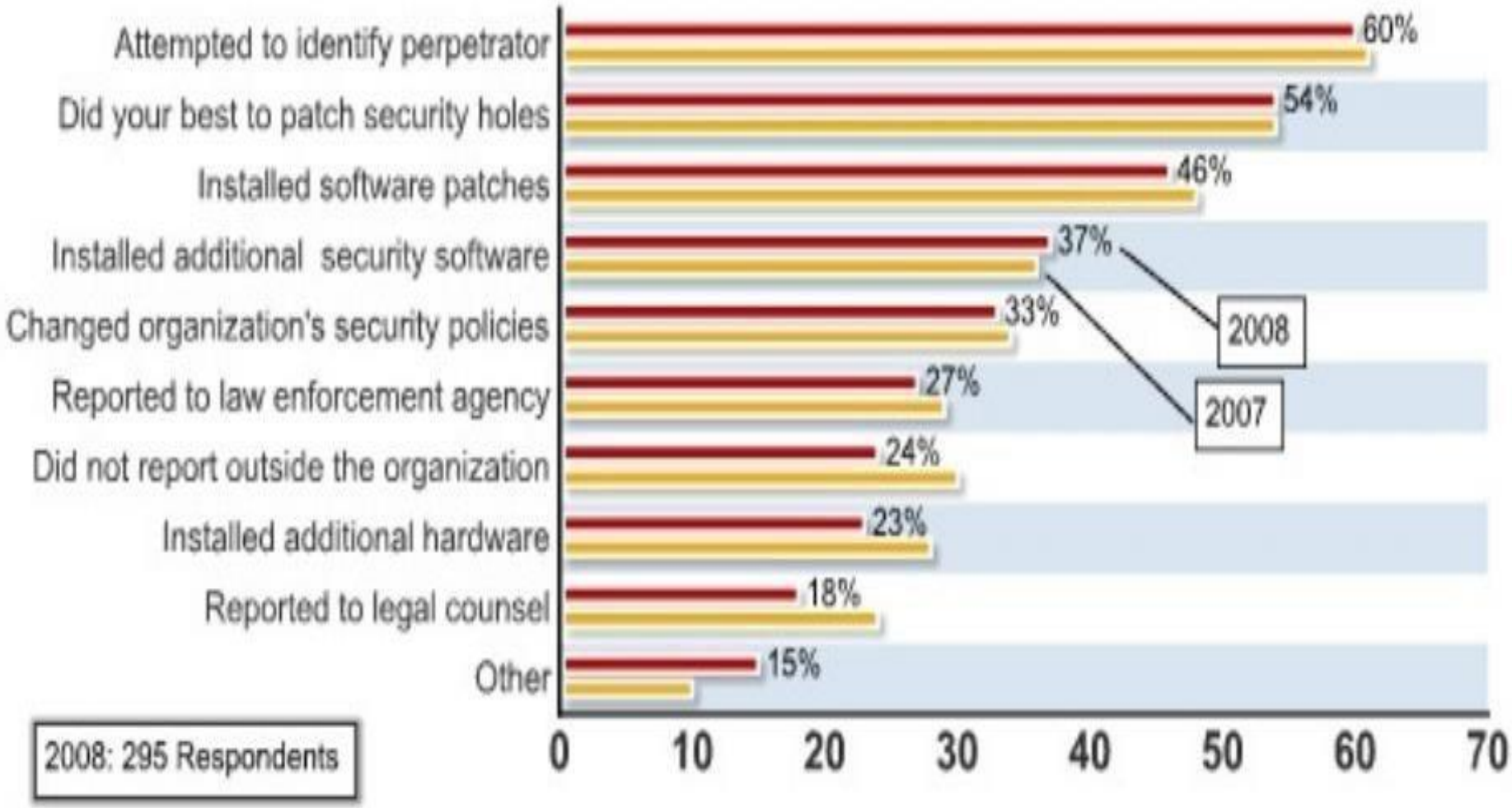


Figure 20: Actions Taken After an Incident



Tools for Attack

- Most common tools:
- Metasploit
- nmap
- snort
- hping2
- tcpdump
- ettercap
- THC hydra
- dsniff
- whisker

Cain & Abel

wireshark

netcat

kismet

john the ripper

nikto / wikto

paros proxy

net stumbler

Commercial Tools

- Core Impact http://www.coresecurity.com/
- CANVAS pro http://www.immunitysec.com/productscanvas.shtml
- Nessus (Tenable) http://www.nessus.org/
- Retina (eEye) http://www.eeye.com/