DCI

Corporate Governance in Information Security

CSI in Government: Challenges in Securing IT in Government

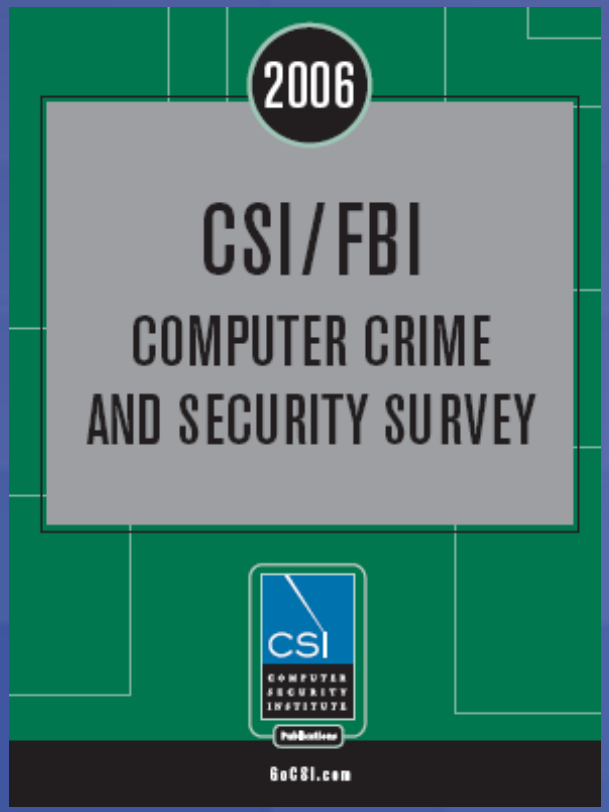
CIO Forum, 23 November 2006

Crowne Plaza Hotel, Ortigas Center

Peter Drucker in 'Management Challenges for the 21st Century'

The diffusion of technology and the commodification of information transforms the role of information into a resource equal in importance to the traditionally important resources of land, labor and capital.

2006 CSI/FBI Computer Crime and Security Survey

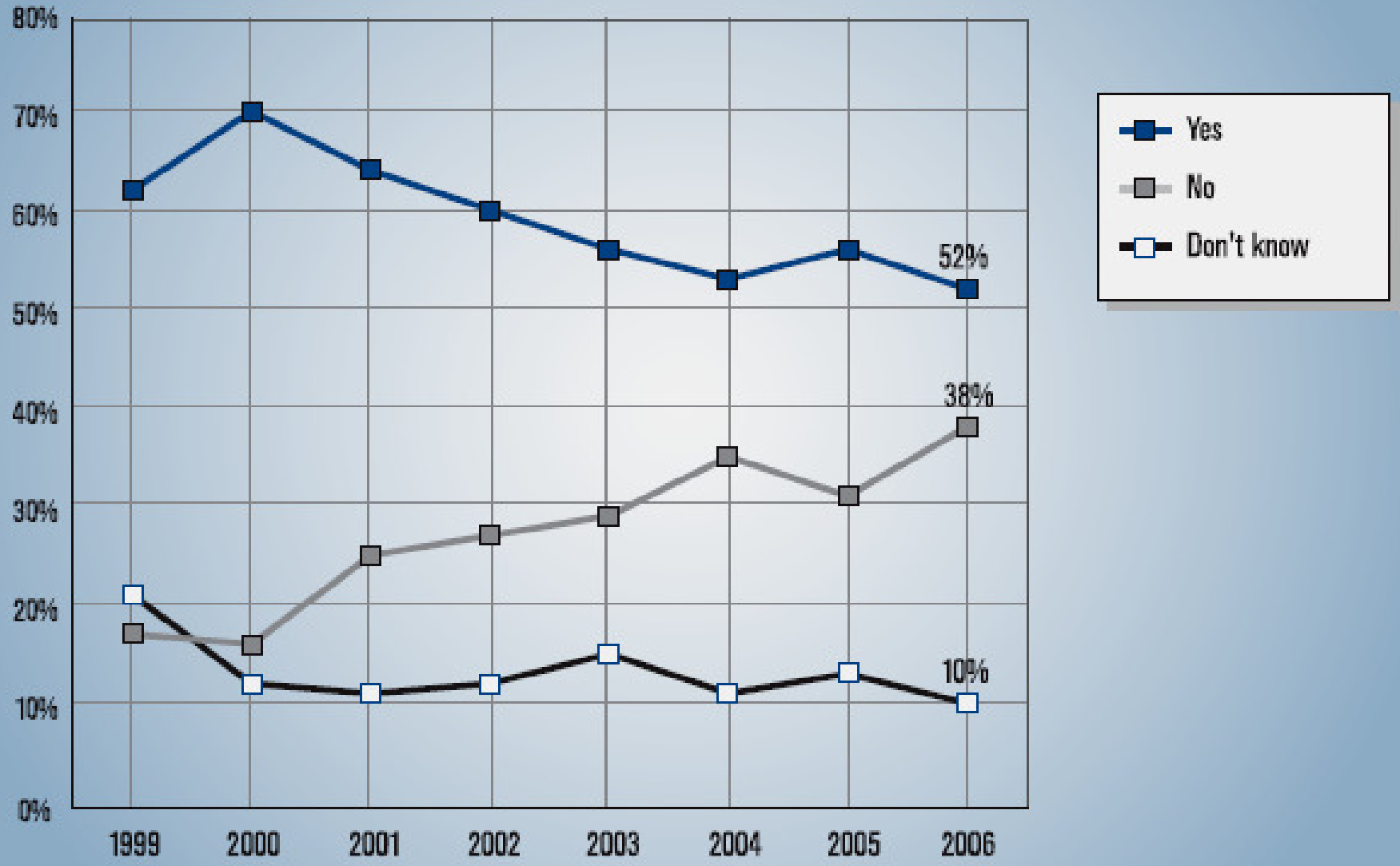


- **Conducted by the Computer Security Institute (CSI) with the participation of the San Francisco Federal Bureau of Investigation's Computer Intrusion (CIS) Squad**
- **Survey is now in its 11th year**
- **The longest-running continuous survey in the information security field**
- **Survey results are based on the responses of 616 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities**

Major Issues of the Survey

- Unauthorized use of computer systems
- Number of incidents from outside and inside an organization
- Types of attacks or misuse detected
- Actions taken in response to computer intrusions
- Techniques organizations use to evaluate the performance of their computer security investments;
- Security training needs of organizations
- Organizational spending on security investments
- Impact of outsourcing on computer security activities
- Use of security audits and external insurance
- Role of the Sarbanes–Oxley Act of 2002 on security activities
- Portion of the information technology (IT) budget organizations devote to computer security

Figure 12. Unauthorized Use of Computer Systems Within the Last 12 Months

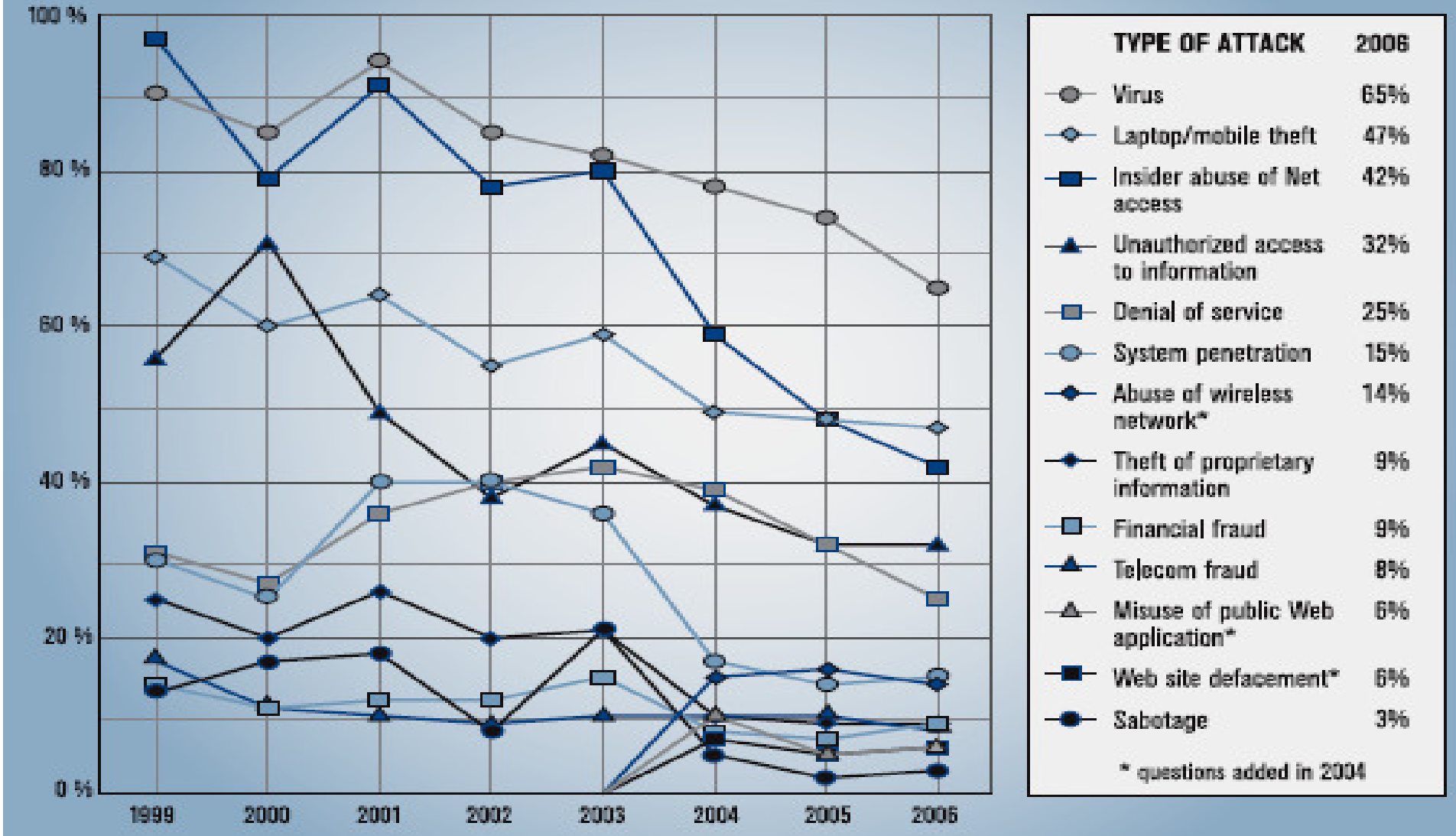


CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 616 Respondents

Figure 14. Types of Attacks or Misuse Detected in the Last 12 Months

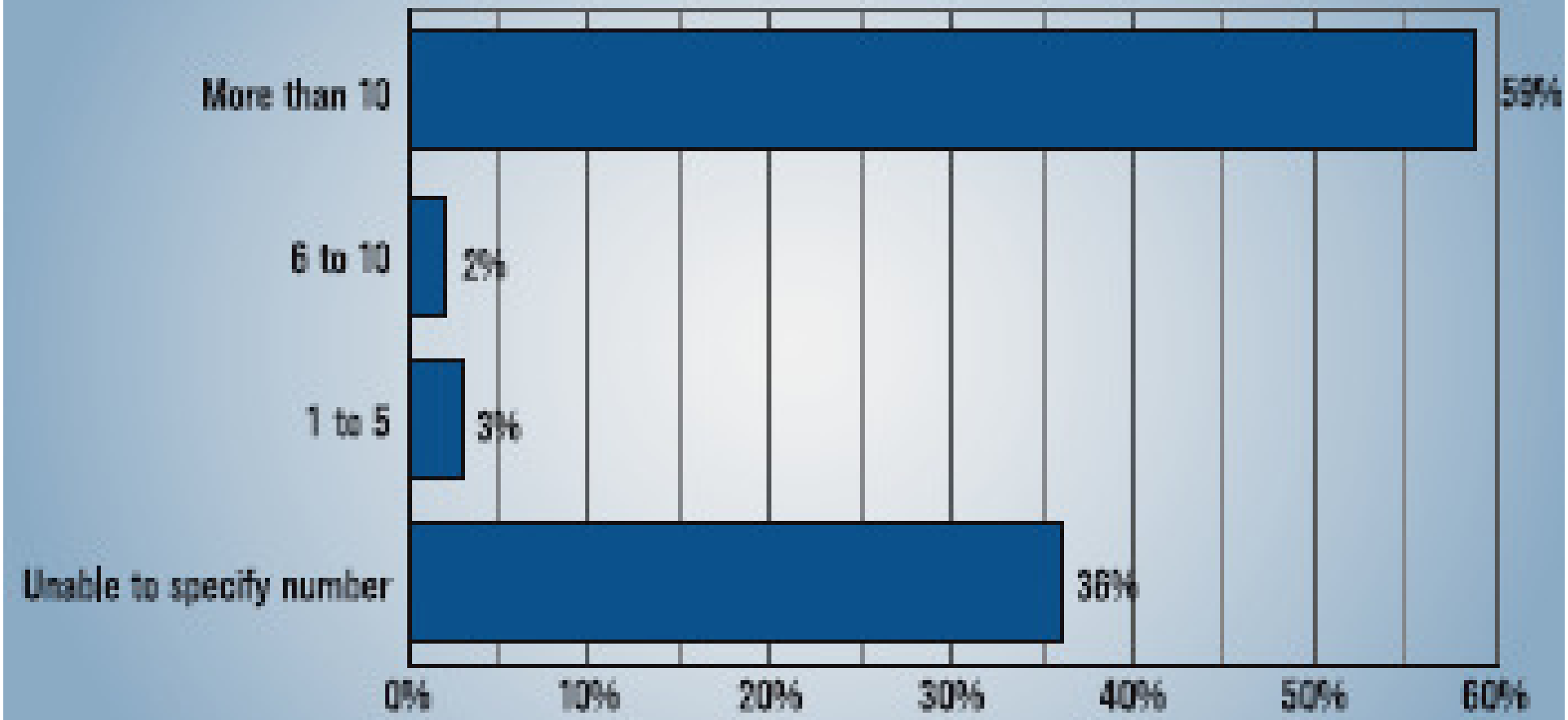
By Percent of Respondents



CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 616 Respondents

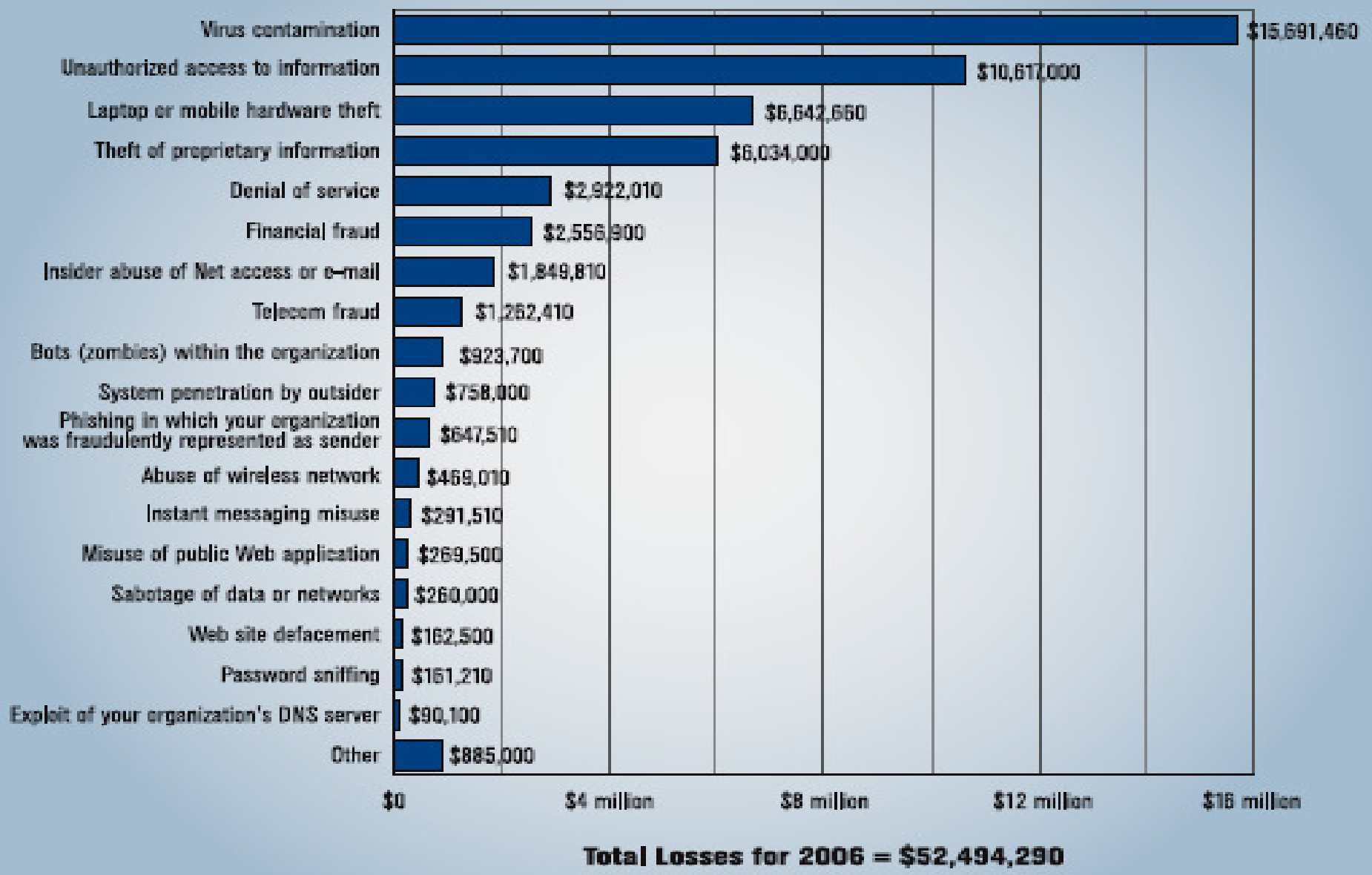
Figure 15. Percentage Experiencing Web Site Incidents



CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 272 Respondents

Figure 16. Dollar Amount Losses by Type



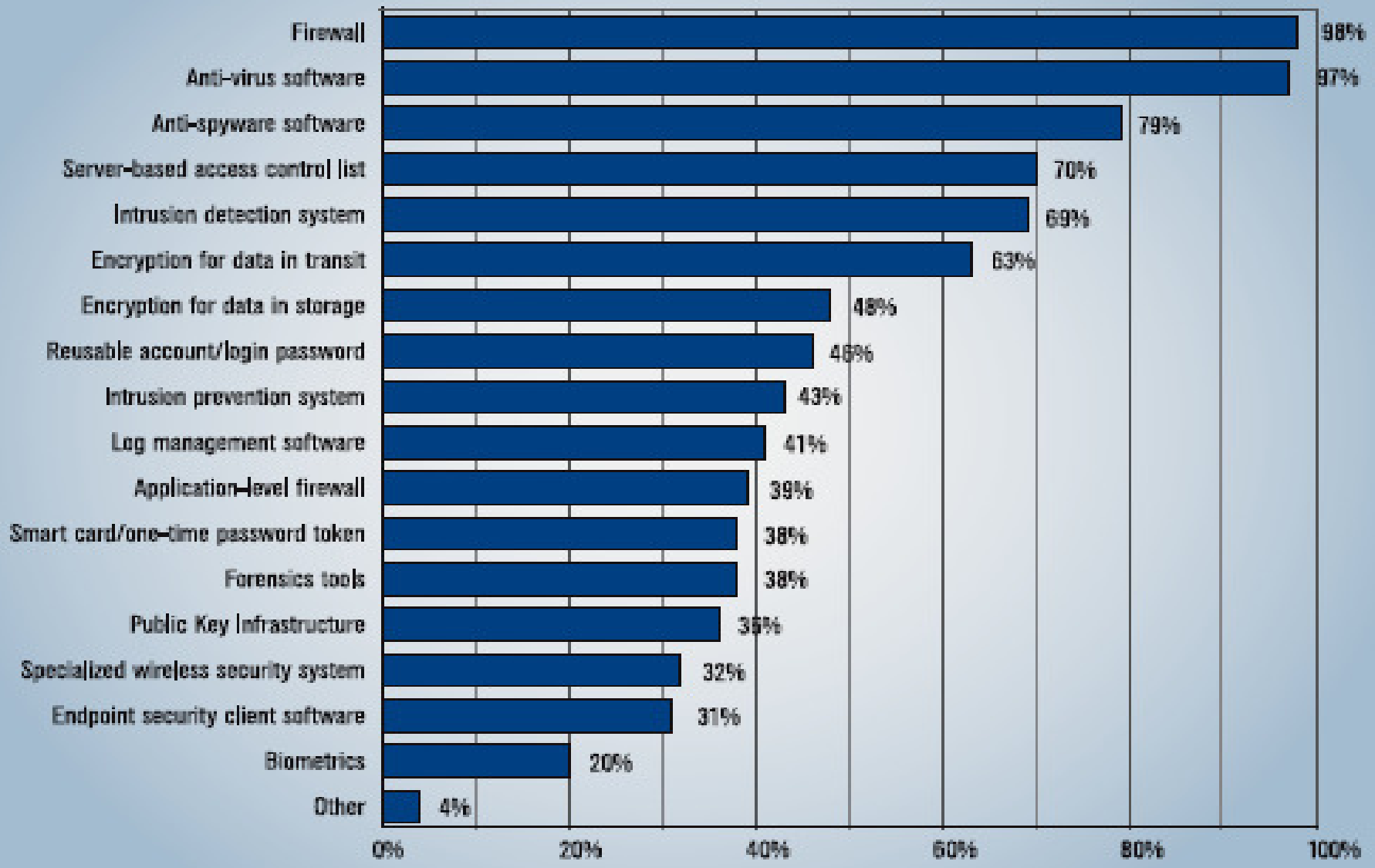
Total Losses for 2006 = $52,494,290

CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 313 Respondents

Figure 17. Security Technologies Used

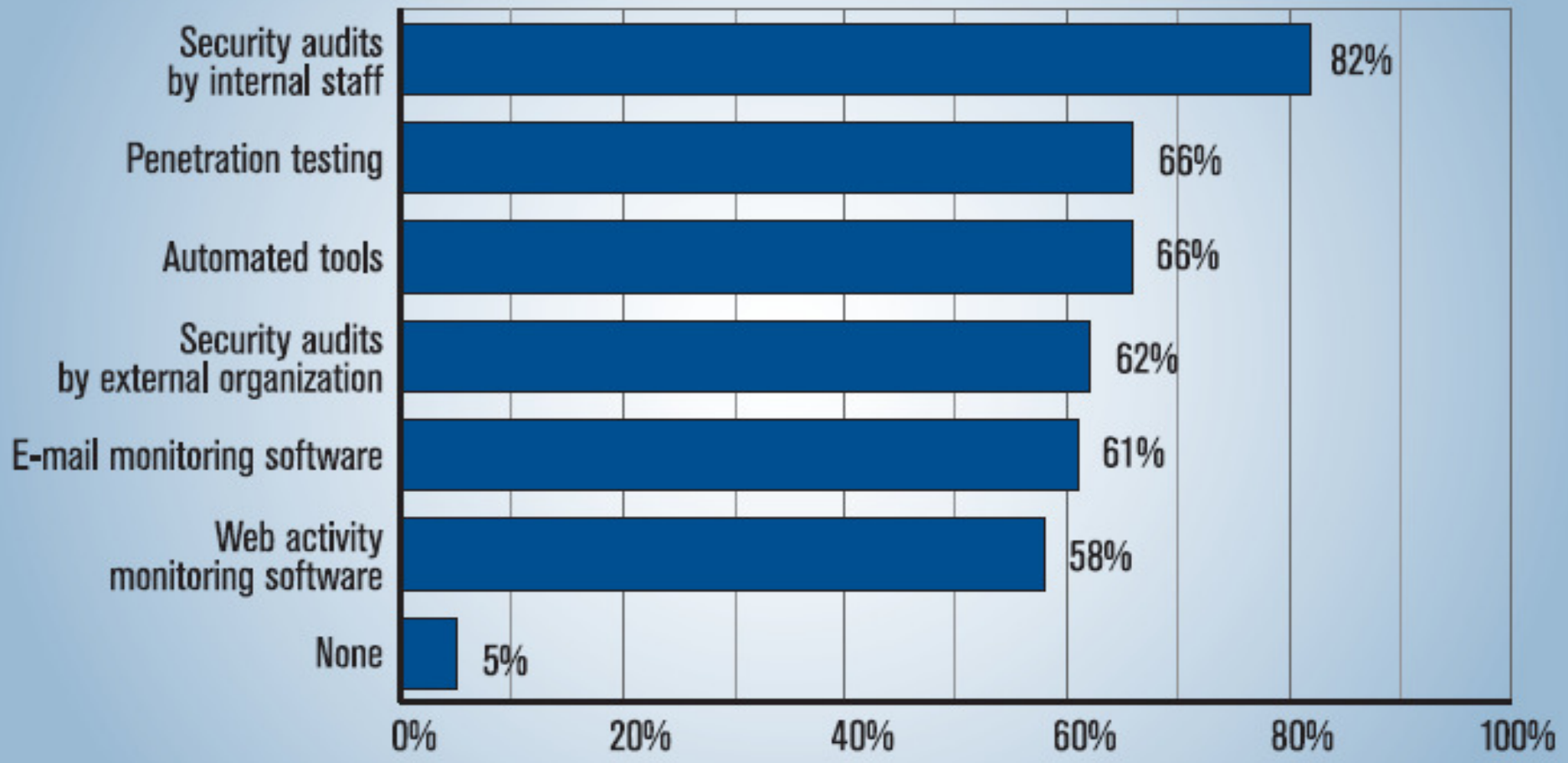
By Percent of Respondents



CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 616 Respondents

Figure 18. Techniques Used to Evaluate Effectiveness of Security



CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 597 Respondents

Realities of Today

- Organisations continue to witness information-related crime
- Vandalism is becoming the choice of a growing global criminal element
- Financial gain is now one of the biggest motives for cybercrimes
- Existing institutions burdened by countless conflicting jurisdictions and inadequate resources
- Large portion of the task of protecting critical information resources falls squarely on the shoulders of executives and boards of directors

IT Governance as Part of Corporate Governance

- **Information security is not only a technical issue**
- **It is a business and governance challenge that involves adequate risk management, reporting and accountability.**
- **Effective security requires the active involvement of executives to assess emerging threats and the organization's response to them.**

IT Governance Institute

- **The IT Governance Institute (ITGITM) (*www.itgi.org*)**
- **Established in 1998 to advance international thinking and standards in directing and controlling an enterprise's information technology**
- **Offers original research, electronic resources and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities**

ITGI Governance Publication

The IT Governance Institute (the "Owner") has designed and created this publication, titled *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition* (the "Work"), primarily as an educational resource for boards of directors, executive management and IT security professionals.

IT Governance and Management

Company's boards should provide strategic oversight regarding information security:

- **Understanding the criticality of information and information security to the organization**
- **Reviewing investment in information security for alignment with the organization strategy and risk profile**
- **Endorsing the development and implementation of a comprehensive information security program**
- **Requiring regular reports**

Boards and Executive Management Considerations of IT Governance

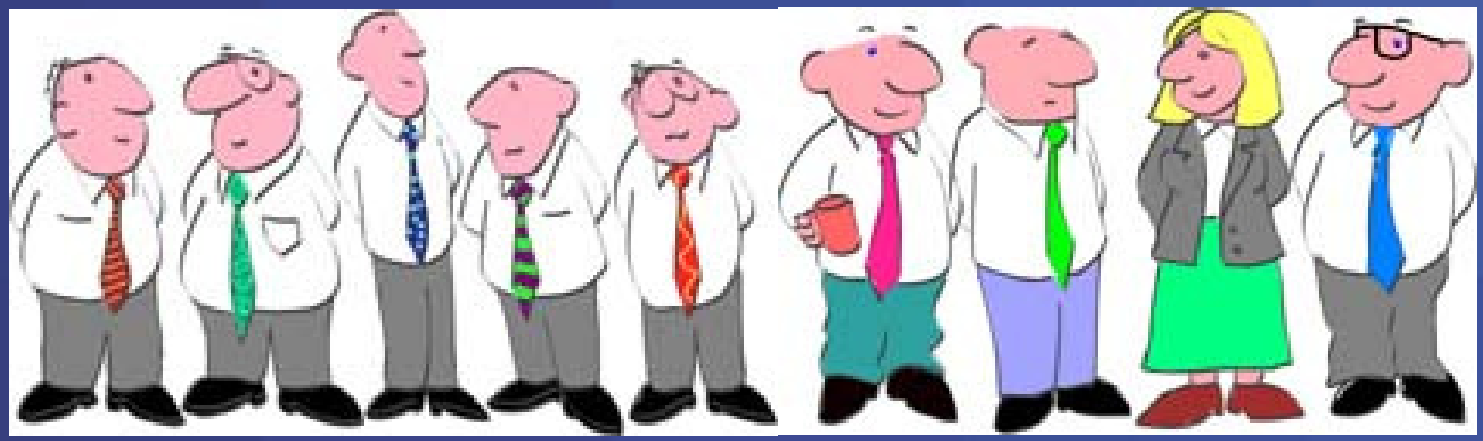
- **Scale and return of the current and future investments in information resources to ensure that they are optimized**
- **Potential for technologies to dramatically change organizations and business practices**
- **Increasing dependence on ICT that deliver the information**
- **Dependence on entities beyond the direct control of the enterprise**
- **Increasing demands to share information with partners, suppliers and customers**
- **Impact on reputation and enterprise value resulting from information security failures**
- **Failure to set the tone at the top with regard to the importance of security**

Principles of IT Governance: Fundamental Issues

- **What is information security governance?**
- **Why is it important?**
- **Who is responsible for it?**
- **What information security governance should deliver**
- **Questions to ask regarding information security governance**
- **How information security governance is evolving**
- **How to measure an organization's maturity level relative to information security governance**

What Is Information Security Governance?

Governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.



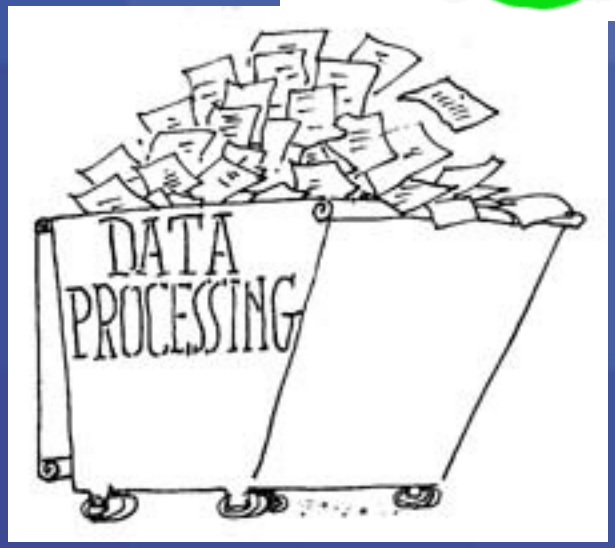
Desired Outcomes of Information Security Governance

The five basic outcomes of information security governance should include:

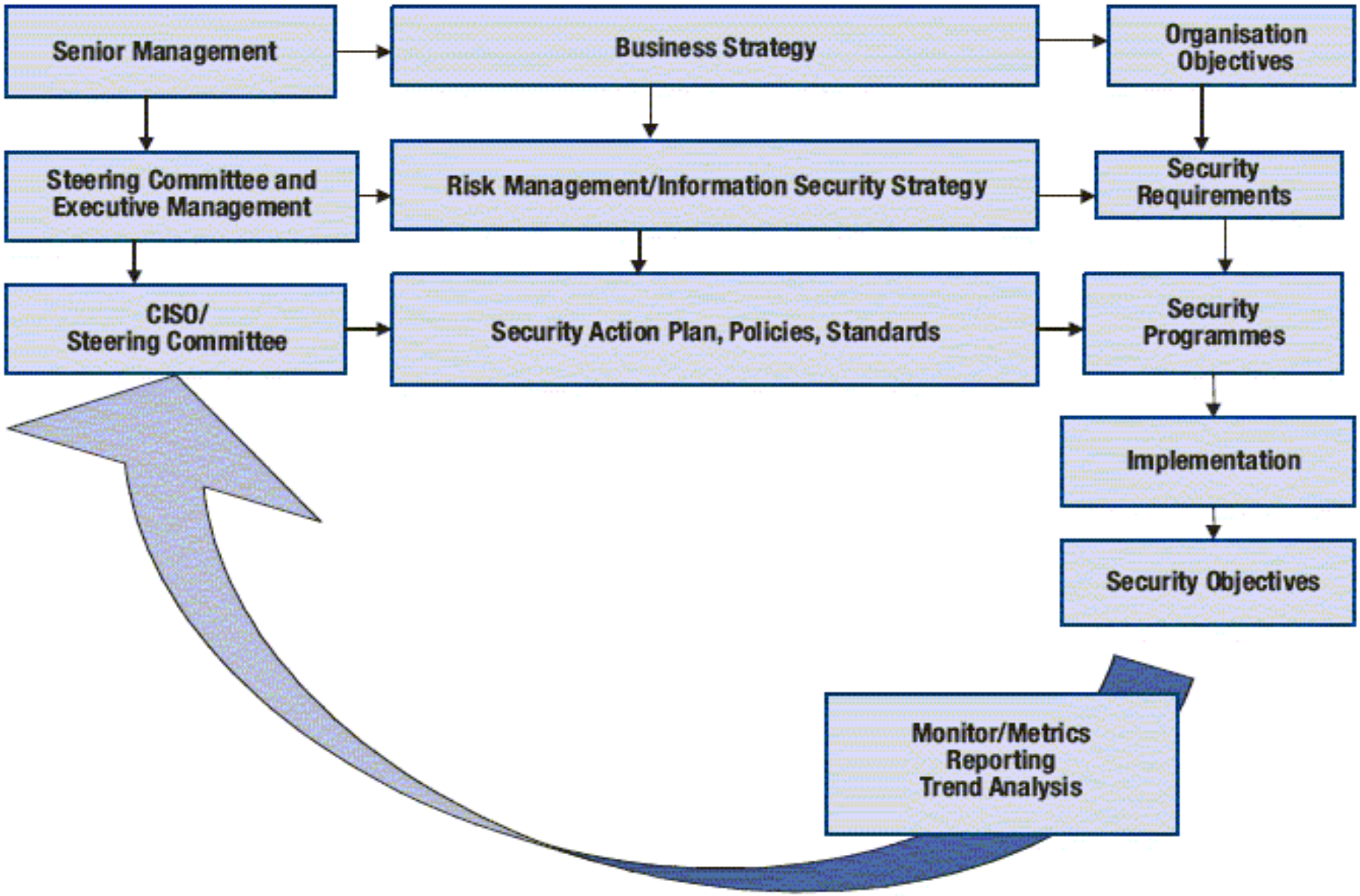
1. **Strategic alignment of information security with business strategy to support organizational objectives**
2. **Risk management by executing appropriate measures to manage and mitigate risks and reduce potential impacts on information resources to an acceptable level**
3. **Resource management by utilizing information security knowledge and infrastructure efficiently and effectively**
4. **Performance measurement by measuring, monitoring and reporting information security governance metrics to ensure that organizational objectives are achieved**
5. **Value delivery by optimizing information security investments in support of organizational objectives**

Why Are Information Security and Information Security Governance Important?

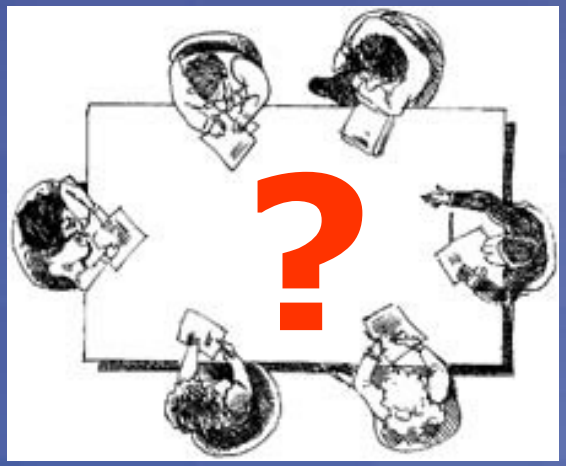
Information security addresses the protection of information, confidentiality, availability and integrity throughout the life cycle of the information and its use within the organization.



Conceptual Information Security Governance



Who Should Be Concerned With Information Security Governance?



Boards of Directors/Trustees **– Has the fundamental responsibility to protect the interests of the organization's stakeholders**

Executives **– Implements effective security governance and defines the strategic security objectives of an organization and requires leadership and ongoing support from executive management to succeed**

Steering Committee **– A steering committee of executives should be formed whose members may include the CEO or designee, business unit executives, the CFO, the CIO/IT director, CSO, CISO, human resources, legal, risk management, audit, operations and public relations to ensure that all stakeholders affected by security considerations are involved**

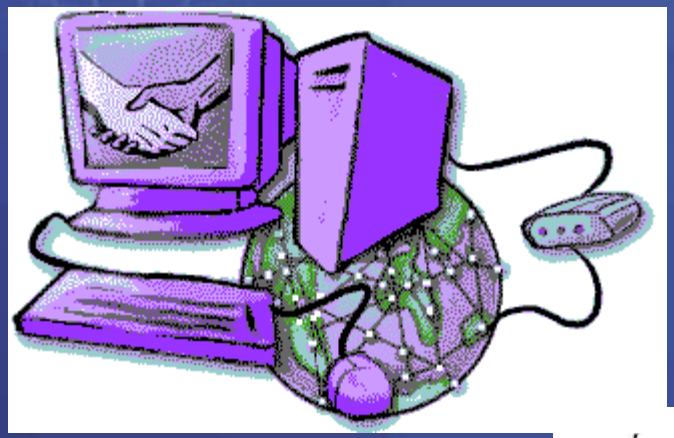
Chief Information Security Officer **– All organizations MUST have a CISO even when there is an information security office or director in place; the scope and breadth of information security concerns are such that the authority required and the responsibility taken inevitably end up with a C-level officer or executive manager**

What Should the Board of Directors/Trustees and Senior Executives Be Doing?

Boards and management have several fundamental responsibilities to ensure that information security governance is in force:

- **Understand Why Information Security Needs to Be Governed**
- **Take Board-level Action**
- **Take Senior Management-level Action**

What Are Some Thought-Provoking Questions to Ask?



- **Questions to Uncover Information Security Issues**
- **Questions to Find Out How Management Addresses Information Security Issues**
- **Questions to Self-assess Information Security Governance Practices**

What Should Information Security Governance Deliver?

- ***Strategic Alignment*** **– achieve the goal of strategic alignment of information security in support of organisational objectives**
- ***Risk Management*** **– manage and mitigate risks and reduce potential impacts on information assets to an acceptable level**
- ***Resource Management*** **– Efficient and effective use of information security knowledge and infrastructure**
- ***Performance Measurement*** **– Measuring, monitoring and reporting on information security processes ensures that organisational objectives are achieved**
- ***Value Delivery*** **– Security investments should be optimized to support organisational objectives**

How Is Information Security Governance Evolving?

- Requirement to improve information security governance will continue into the foreseeable future
- Traditional focus on technical solutions must give way to the understanding that security is fundamentally a management problem to be addressed at the highest levels
- Momentum is growing globally to address issues of privacy and cybercrime, with stringent regulations regarding operational risk management, full financial disclosure and privacy protection
- Organizations must consider that failing to provide adequate protection of critical information assets is becoming more visible and less acceptable
- Management should also consider that the risks of large negligence awards and the direct financial consequences may be overshadowed by public exposure of poor governance and substandard practices

What Can Be Done to Successfully Implement Information Security Governance?

Questions for Directors

- **Does the board understand the organization's dependence on information?**
- **Does the organization recognize the value and importance of information security and set the appropriate tone at the top to foster a security conscious environment?**
- **Does the organization have a security strategy? If so, is it closely aligned with the overall business strategy?**

Questions for Management

- **How is the board kept informed of information security issues? When was the last briefing made to the board on security risks and status of security improvements?**
- **Has someone been appointed to be responsible for developing, implementing and managing the information security program, and is he/she held accountable?**
- **Are security roles and responsibilities clearly defined and communicated?**

Implementation of Information Security Governance at DCI

Internally

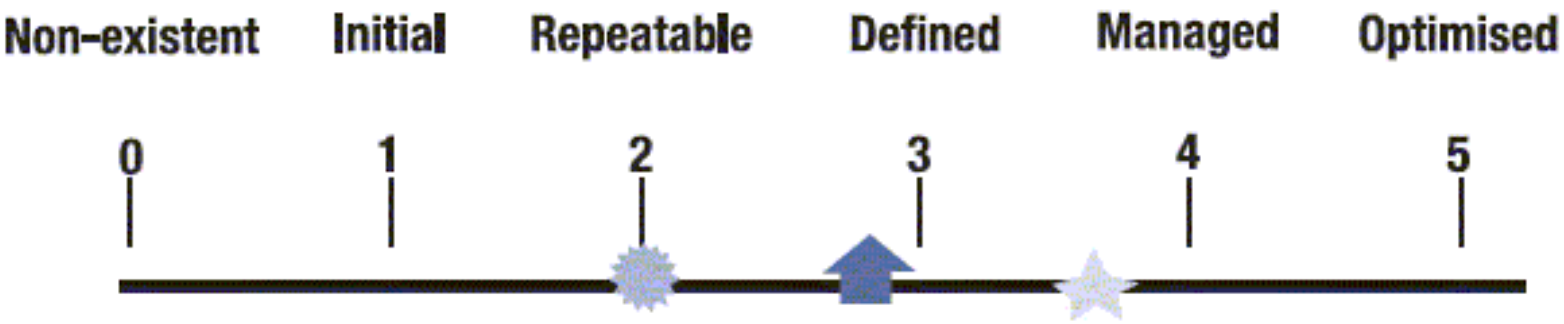
- **Training of Business Executives and Project Managers in Project Management Methodology in preparation for PMP certification**
- **Company-wide CMMI Level III certification training**
- **CISSP, CISM and CISA certifications for 2007**
- **Development of IS policies based on ISO 17799/27001 standards**

Externally

- **Training of clients' decision-makers in Strategic Information Technology Management (SITM)**
- **Inclusion of Information Security in all training modules mandatory for all client's employees**
- **Training and assistance in IS policy development based on ISO 17799/27001**

How Does My Organization Compare on Information Security Governance?

Maturity Model Dashboard



LEGEND FOR SYMBOLS USED

- Enterprise current status
- Industry average
- Enterprise target

LEGEND FOR RANKINGS USED

0—Management processes are not applied at all.
1—Processes are *ad hoc* and disorganised.
2—Processes follow a regular pattern.
3—Processes are documented and communicated.
4—Processes are monitored and measured.
5—Good practices are followed and automated.

DCI

In SECURITY…or INFORMATION SECURITY – it is always better to GET IT RIGHT THE FIRST TIME!!!

Thank You Very Much!!!