16/01/2015

INFORMATION SECURITY

Xavier Genet

BUILDING TEAM SPIRIT TOGETHER

SOCIETE GENERALE
Corporate & Investment Banking

DAUPHINE
UNIVERSITÉ PARIS

TELECOM
&Management
SudParis

AGENDA

- **Definition and concepts**
- **Threats**
- **Why Information Security ?**
- **Setting up an Information Security Organization**
- **Implementing a Security Policy**
  - Get ISec Incident Responses capabilities
  - Build the Information Security Operational Center
  - Managing and controlling Information Access Control
  - Third party Access Management
  - Data privacy regulations
  - Evaluation & measure of Information Security efficiency
  - The Information Security Team
  - Information Security trends
- **Information Security for dummies : do / don’ts**
- **Information Security : conclusion**
- **Business Intelligence : a quick overview**
- **Future Fiction**

INFORMATION SECURITY

DEFINITION AND CONCEPT

CHANGES VS SECURITY …

- The Changing World
- Business, anywhere, everywhere, at the speed of light

- The Changing Technology
- Vulnerabilities, vulnerabilities !

- The Management challenge
- We need to know more, measure more and prove more

DRIVERS FOR SECURITY

Shareholders

Law & regulations

Norms & methodologies

Customers

Suppliers & partners

Society & Environment

Business strategy

Security is considered as a business driver

INFORMATION SECURITY : DEFINITION

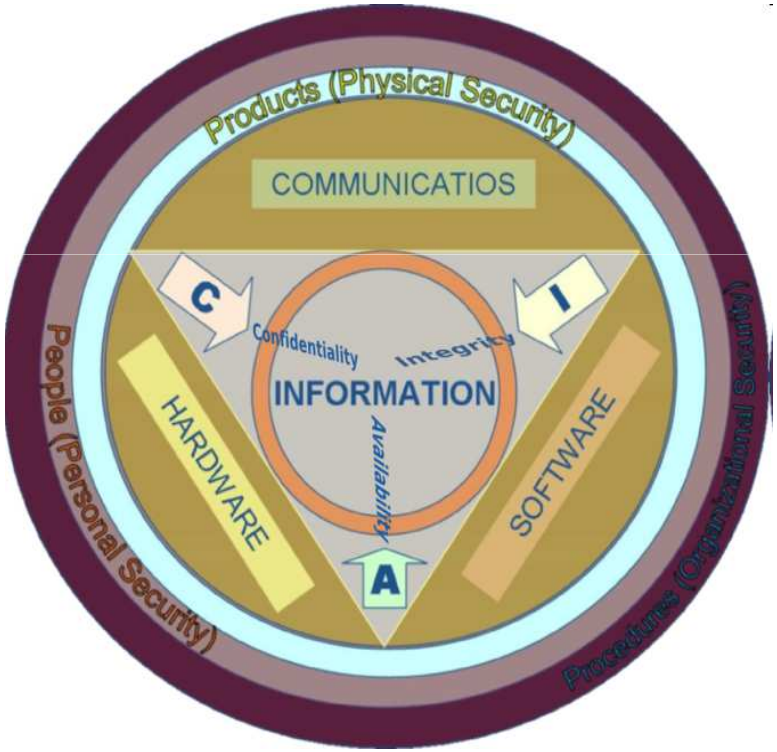
- **Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.**

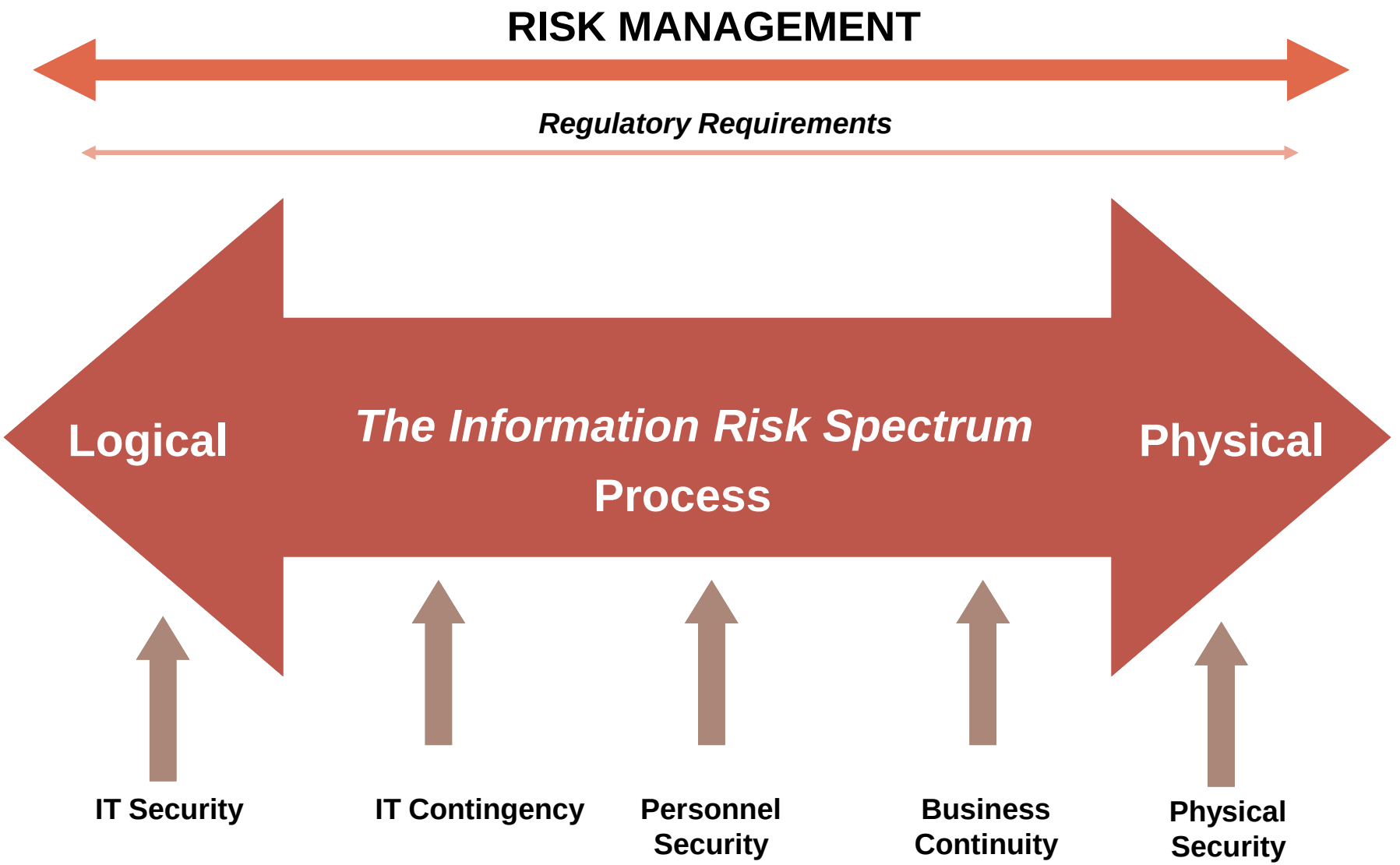
  - Identify and apply information security industry standards, as mechanisms of protection and prevention, at three levels or layers: Physical, personal and organizational.

  - Protecting the confidentiality, integrity and Availability of information.

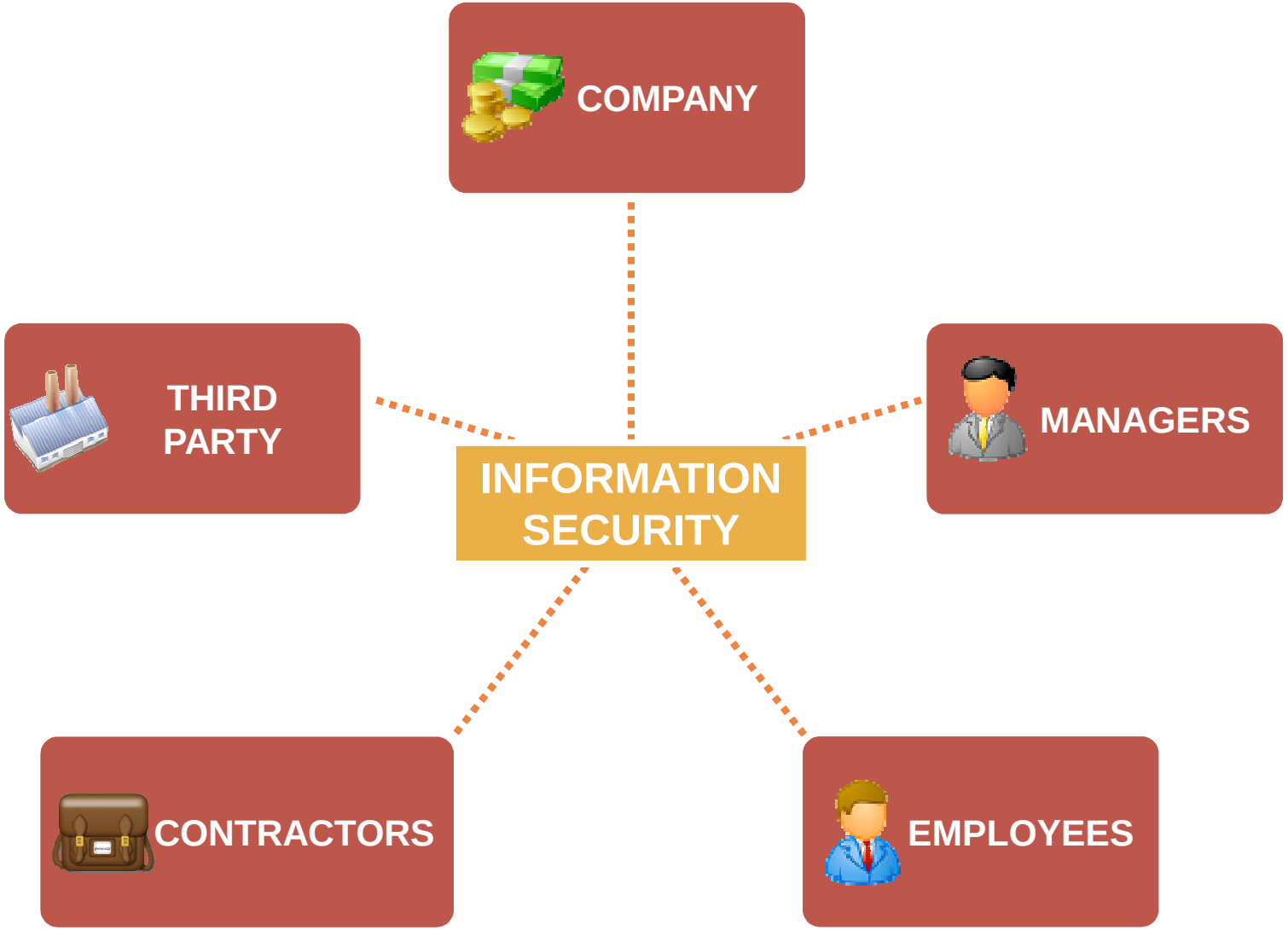
  - Protecting Information Systems : hardware, software and communications.

  © Wikipedia




RISK MANAGEMENT
Regulatory Requirements
Logical
The Information Risk Spectrum
Process
Physical
IT Security
IT Contingency
Personnel Security
Business Continuity
Physical Security

INFORMATION SECURITY : WHO IS ACCOUNTABLE ?



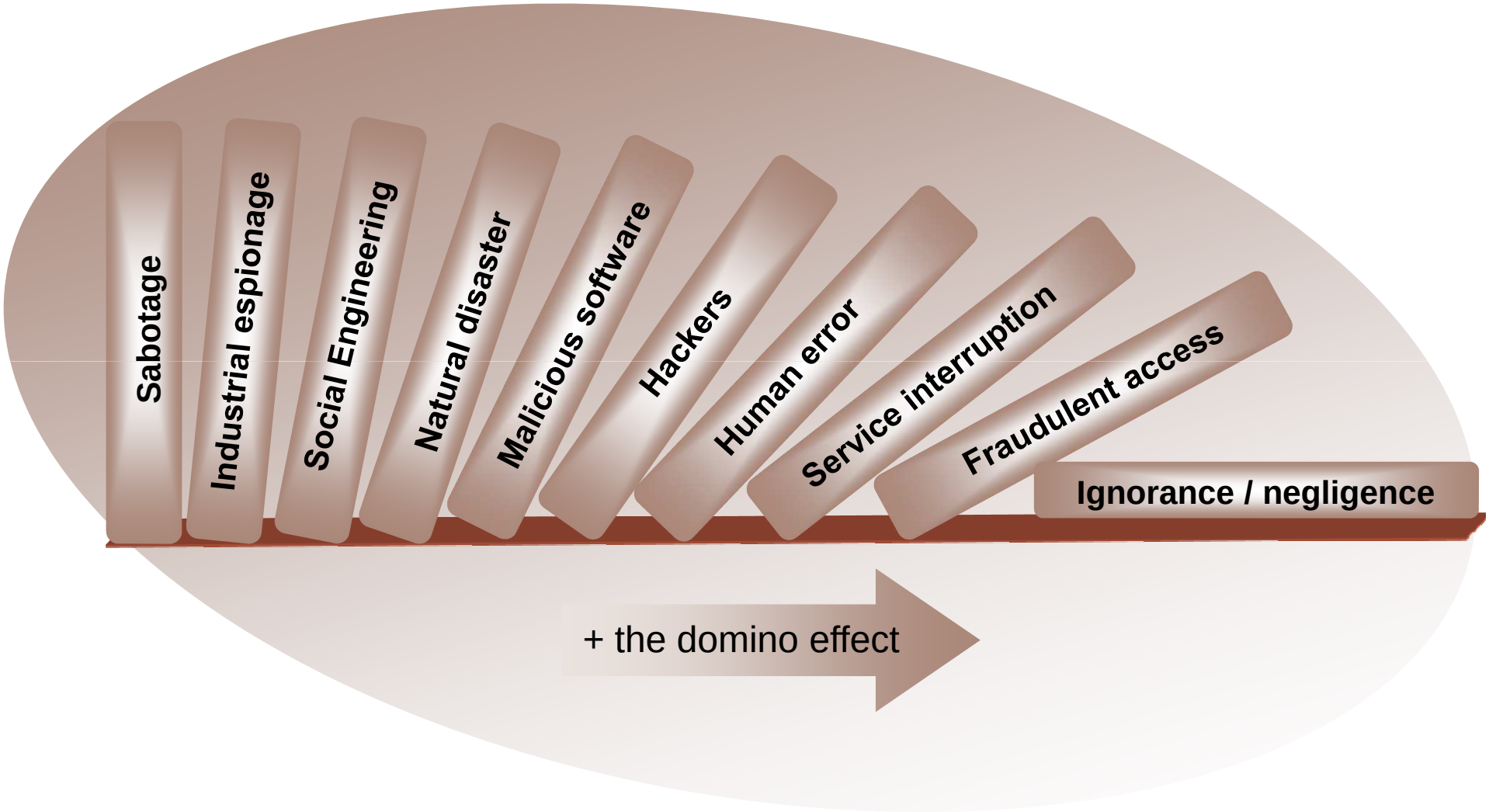
INFORMATION SECURITY : KEY CONCEPTS

- **Confidentiality : ensuring that information is accessible only to those authorized to have access.**
- **Integrity : data cannot be modified without authorization.**
- **Availability : IT systems used to store and process the information, security controls used to protect it, and communication channels used to access it must be functioning correctly.**
- **Authenticity : ensure that the data, transactions, communications, documents (electronic or physical) or even people are genuine.**

INFORMATION SECURITY

THREATS

INFORMATION SECURITY : EXAMPLES OF THREATS



INFORMATION SECURITY : THREATS VS RISKS

RISKS

Social Engineering
- E-mail (phishing), phone
- Elevators, public places

Human Error
- Negligence
- Production access

Technical
- Virus, Malware
- Physical attacks

Access to payment systems
- Key logger
- Confidential information usage

IMPACT

Information Leak
- Advantage for competitors
- Knowledge loss

Financial loss
- Money transfer
- Non conformity to regulations

Image Loss
- Non secure company
- Public display

Operational
- Infected infrastructure
- Information unavailable

INFORMATION SECURITY : RISKS VS SOLUTIONS

RISKS	SOLUTIONS
Confidentiality	USB Key, Burning, etc. control Printing logging
Money Transfer	Strong authentification Strong passwords Trainings
Human Error	Segregation of environment Awareness campaign
Infected Systems	Restricted Web mail & chat Secure infrastructure Surveillance Response team

INFORMATION SECURITY : BASIC VOCABULARY

BASIC VOCABULARY: SPYWARE

- A **Spyware** is computer software that is installed surreptitiously on a personal computer to intercept or take partial control over the user's interaction with the computer, without the user's informed consent.

BASIC VOCABULARY: ADWARE

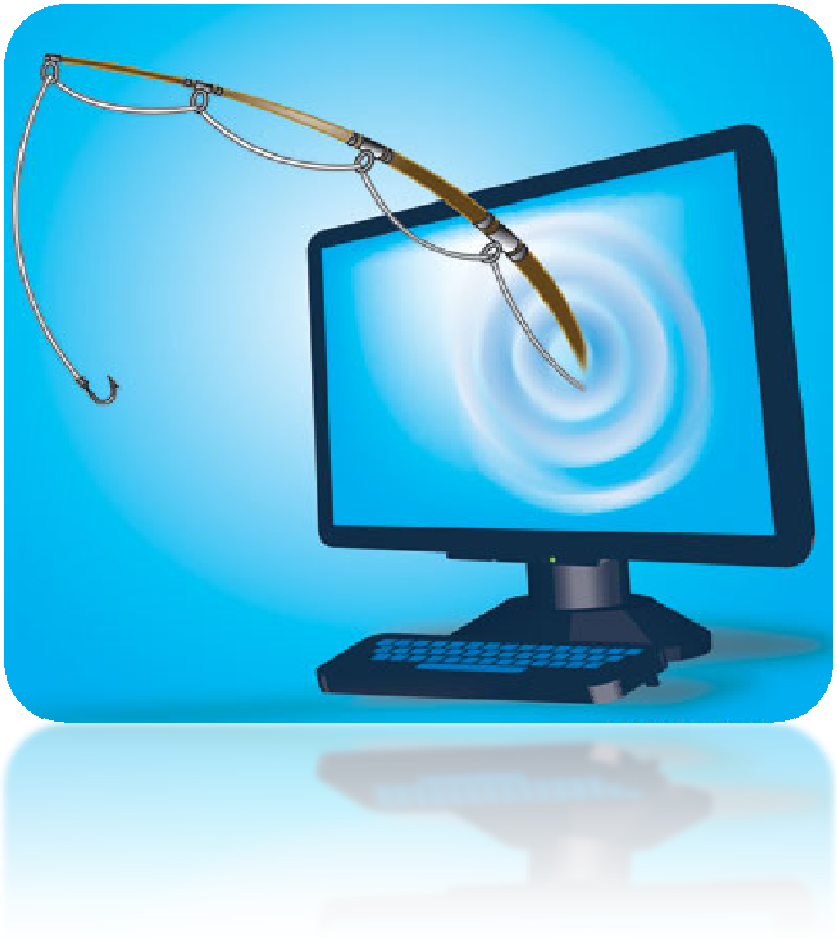
- An **Adware** is any software package which automatically displays or downloads advertisements to a computer after the software is installed on it or while the application is being used. Some types of adware are also spyware and can be classified as privacy-invasive software.

BASIC VOCABULARY: VIRUS

- A **computer** virus is a computer program that can copy itself and infect a computer without permission or knowledge of the user. The term "virus" is also commonly used, albeit erroneously, to refer to many different types of malware and adware programs

BASIC VOCABULARY: PHISING

- **Phishing** is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication.



BASIC VOCABULARY: SOCIAL ENGINEERING

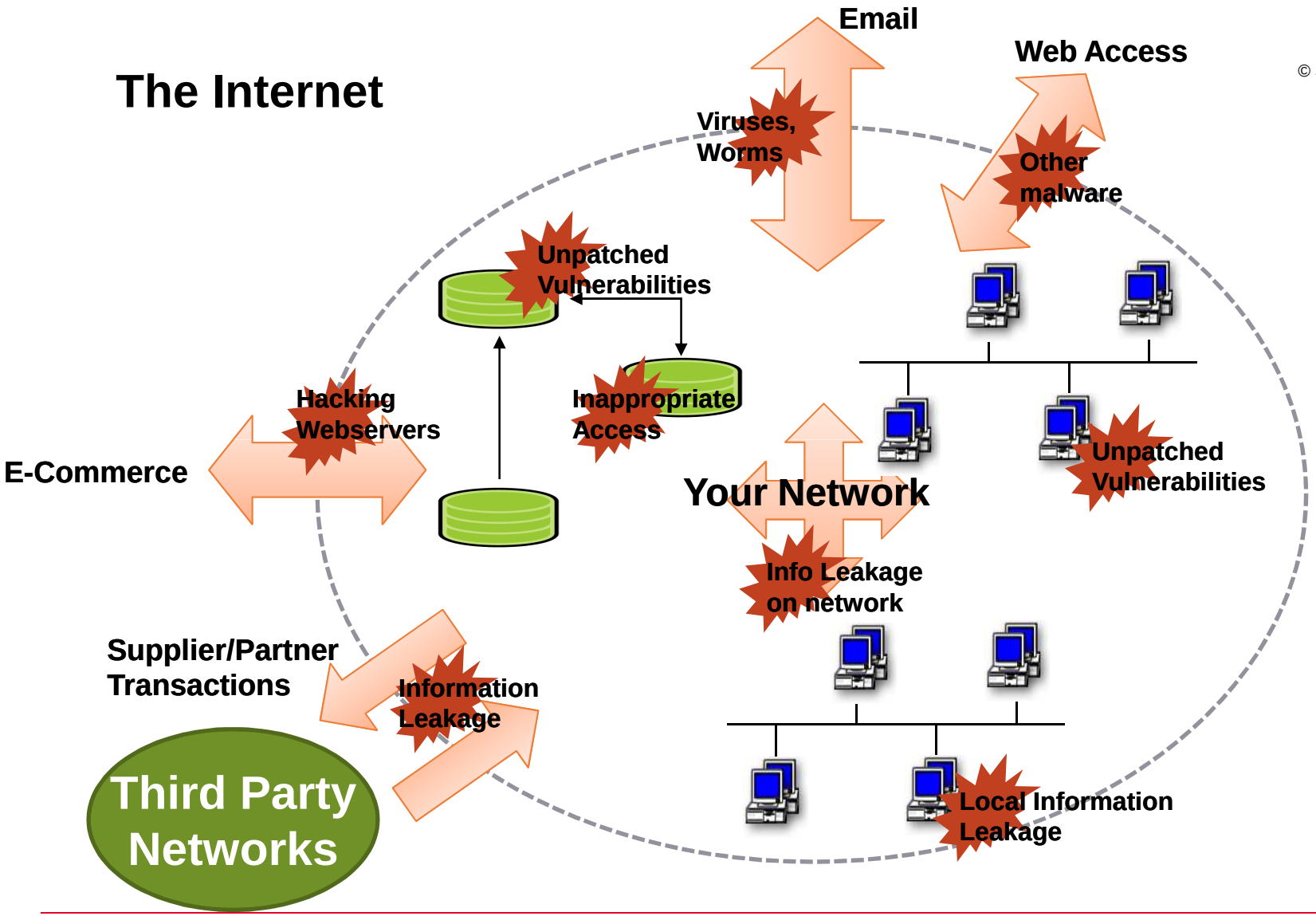
- **Social engineering** is a collection of techniques used in cybercrime to manipulate people into performing actions or divulging confidential information

Social Engineering is a growing threat ■ Stay vigilant with emails, phones calls, etc., you receive from unknown people ■ Information disclosed in e-mail or casual conversation could open doors to business critical assets or to identity theft

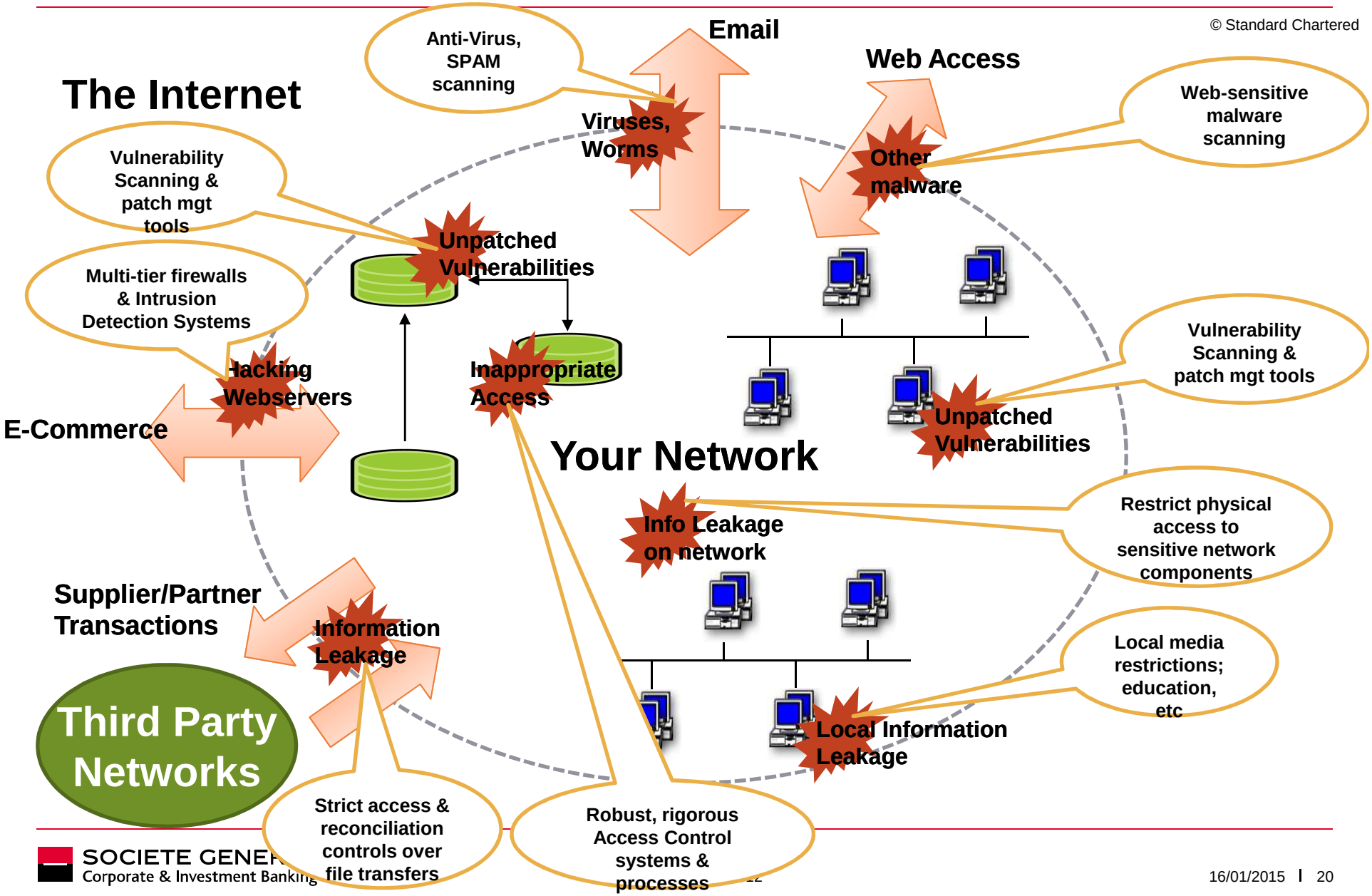
For more information: http://itecdirect.fr.world.socgen/secnet

SOCIETE GENERALE
Corporate & Investment Banking

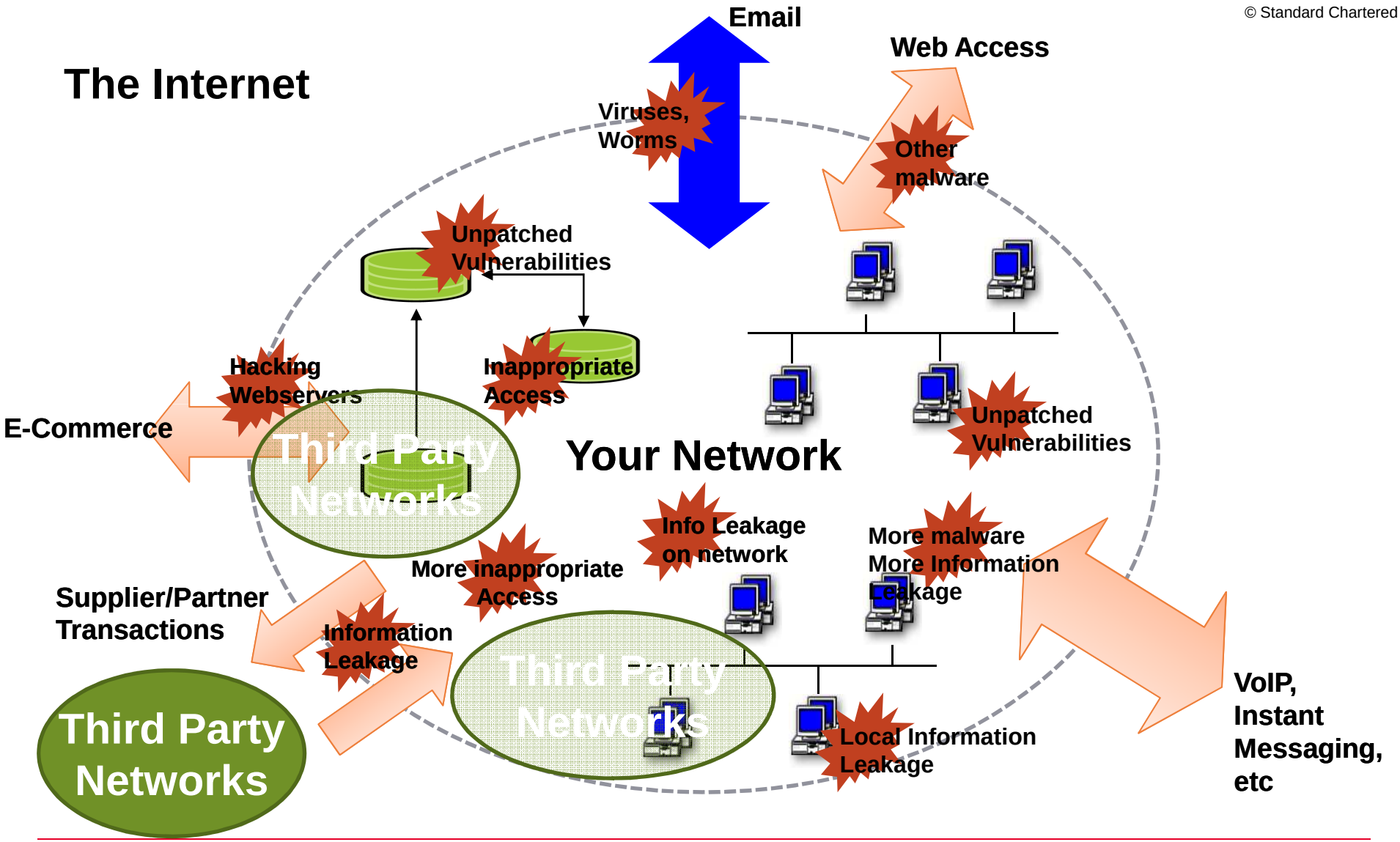
THREAT EVOLUTION : YESTERDAY'S NETWORKS



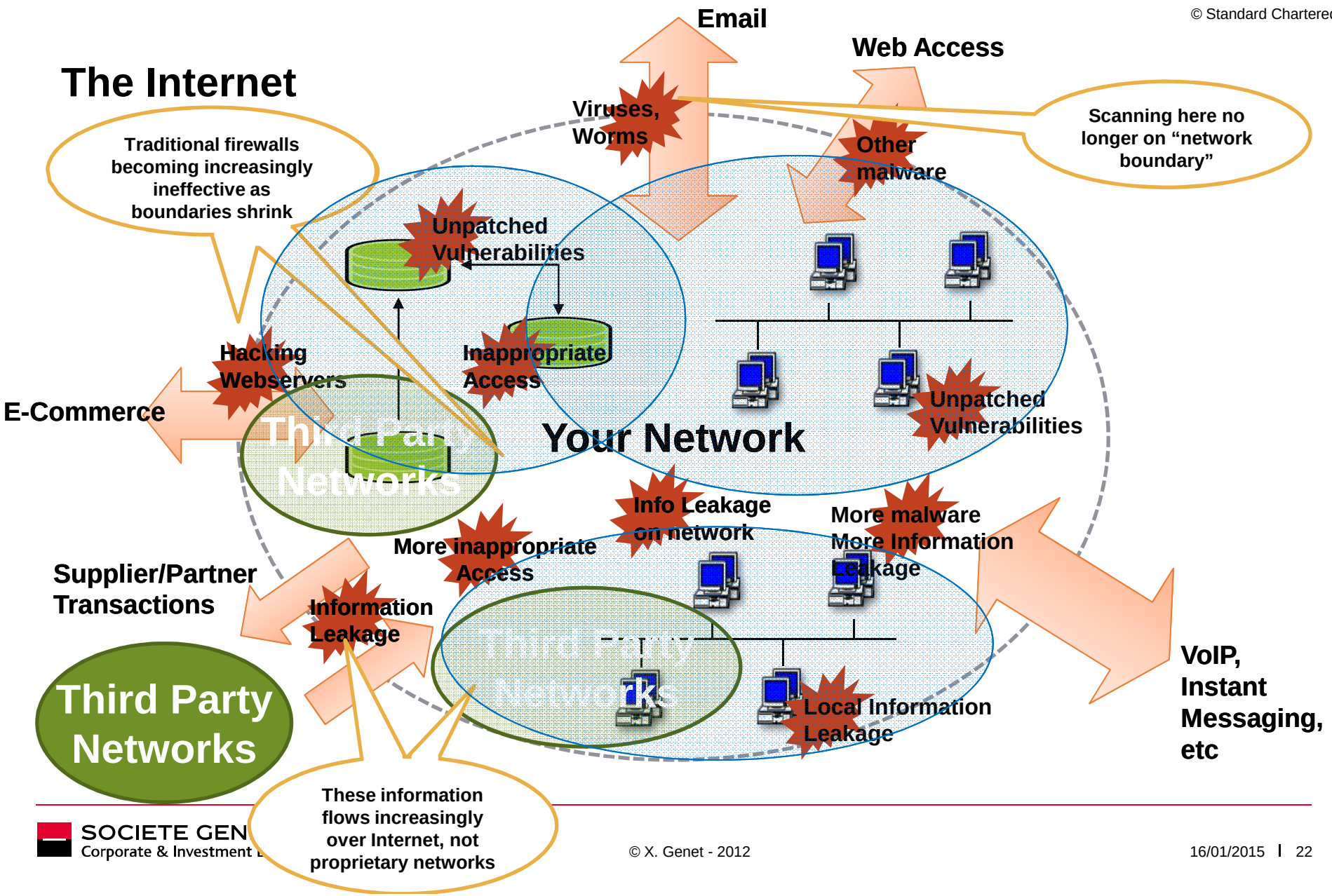
THREAT EVOLUTION : YESTERDAY'S NETWORKS



THREAT EVOLUTION : TODAY'S NETWORKS



THREAT EVOLUTION : TOMORROW'S NETWORKS



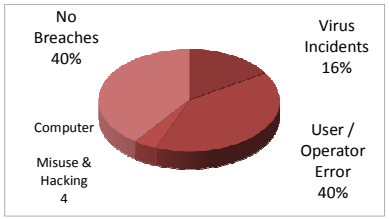
INFORMATION SECURITY

WHY INFORMATION SECURITY ?

WHY INFORMATION SECURITY : A STRONG EVOLUTION OF MALEVOLENCE

More threats, attacks more complex

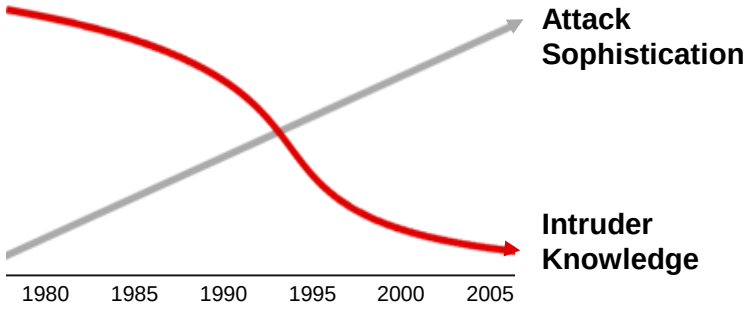
Hackers organization more active



60% of all surveyed organizations reported a security breach in the last 2 years

Increasingly sophisticated attacks … with less knowledge required:

- Anyone ill-intentioned can find on internet hacking guidelines
- Free tools can be downloaded



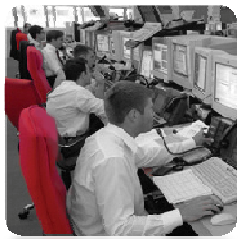
WHY INFORMATION SECURITY : WHAT DO “CRACKERS” WANT ?

In the past, they wanted to be famous and acted on their own

- Robert Morris (first « worm » creator in order to test the internet)
- Kevin Mitnick (The Pentagone first « visitor »)

Now they are organized and are looking for money

- « Mafia » type organisation
- Blackmail
- misappropriation of funds
- Specialised virus création
- Networks of “zombies” PCs for sale



Financial institutions are now more and more attacked

- March 05 - SUMITOMO BANK: key logger . Target €315 Millions.
- BNP Paribas, CCF, CIC (May 05), Banque de France (June 05), AGF (Sept 05): Phishing attacks,

WHY INFORMATION SECURITY IN FINANCIAL ACTIVITIES ?

- **Following the financial scandals in 2000 and the 2008 crisis, the objective is to improve the financial security and the companies governance.**

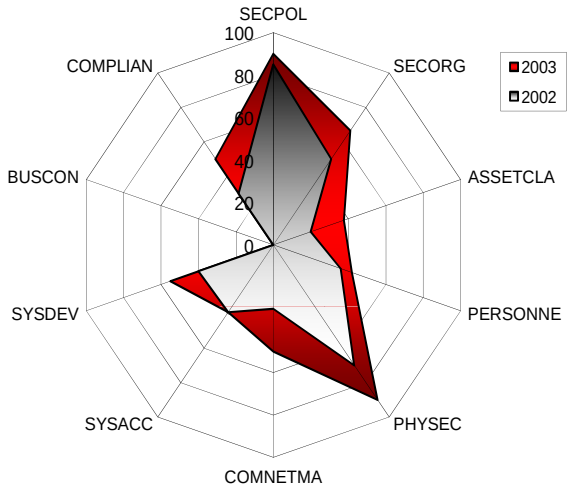
- **Banks need to comply to numerous standards and laws :**
  - In France : 3 main principles :
    - Article 511- 33 from “Code monétaire et financier” « Secret Bancaire »
    - Law of the 6/01/1978 named « Informatique et libertés »
    - Instruction 97-02 from “Comité de la Réglementation Bancaire” « Contrôle Interne »
  - In Europe : Basle 2 regulations
  - USA : FED / SEC standards : SOX , Gramm-Leach-Bliley Act, Security Exchange Act

REGULATORY COMPLIANCE ≠ ADEQUATE SECURITY

INFORMATION SECURITY

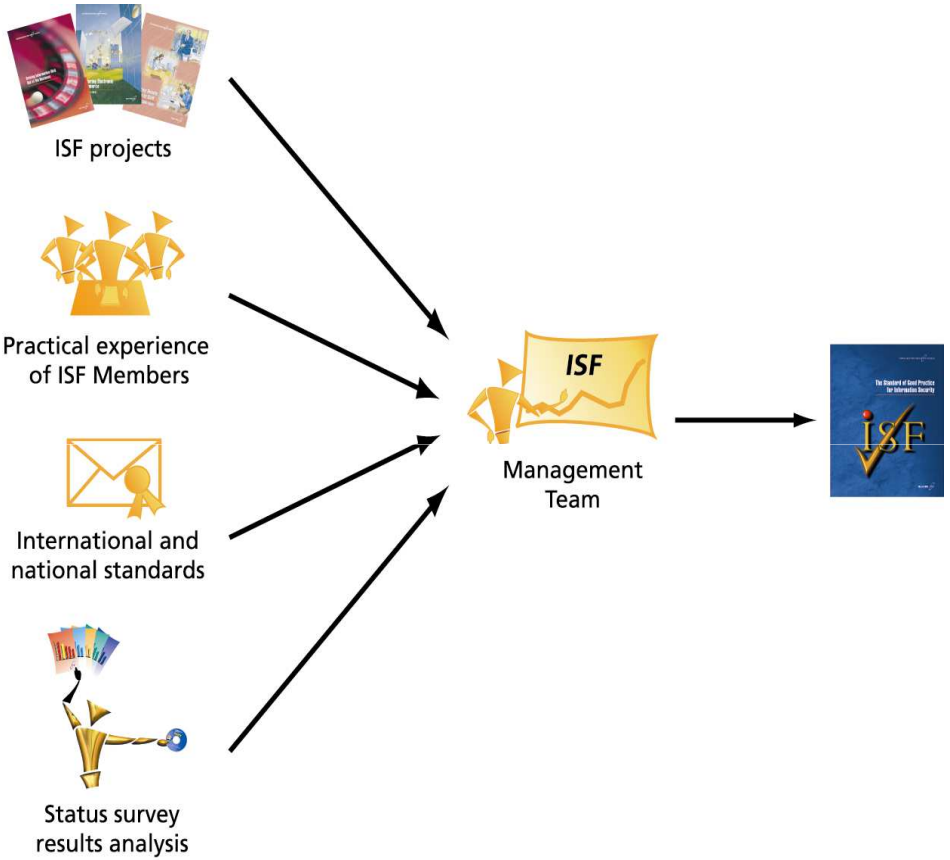
SETTING UP AN INFORMATION SECURITY ORGANIZATION

- **An Internationally recognised standard for Information Security Management. There are 127 controls and over 500 detailed controls organised into 10 sections.**
  - Security Policy (SECPOL)
  - Security Organisation (SECORG)
  - Asset Classification and Control (ASSETCLA)
  - Personnel Security (PERSONNE)
  - Physical and Environmental Security (PHYSEC)
  - Communications and Operations Management (COMNETMA)
  - Access Control (SYSACC)
  - System Development and Maintenance (SYSDEV)
  - Business Continuity Management (BUSCON)
  - Compliance (COMPLIAN)



www.17799central.com
See also :
800-12 : "Computer Security Handbook "
800-14 : "Generally Accepted Principles and Practices for Securing Information Technology;"
800-26 : "Security Self-Assessment Guide for Information Technology Systems".

THE (SOGP) IS A SOUND MODEL FOR ORGANIZING AN INFORMATION SECURITY MANAGEMENT PROGRAM



- **Consider adopting the ISF's *Standard of Good Practice for Information Security* as input and reference model for the Info Sec Program**
  - **Run the Survey** (or Health check) on a representative subset of organizations
  - **Measure the effectiveness** information security arrangements
  - **Compare** them with those of other leading organizations
  - and **assess** how well they are performing against the ISF's *Standard of Good Practice for ISec*

SETTING UP THE INFORMATION SECURITY ORGANIZATION

Objectives

- Define the organizational model and associated roles and responsibilities
- Design and provide implementation support for key security management processes

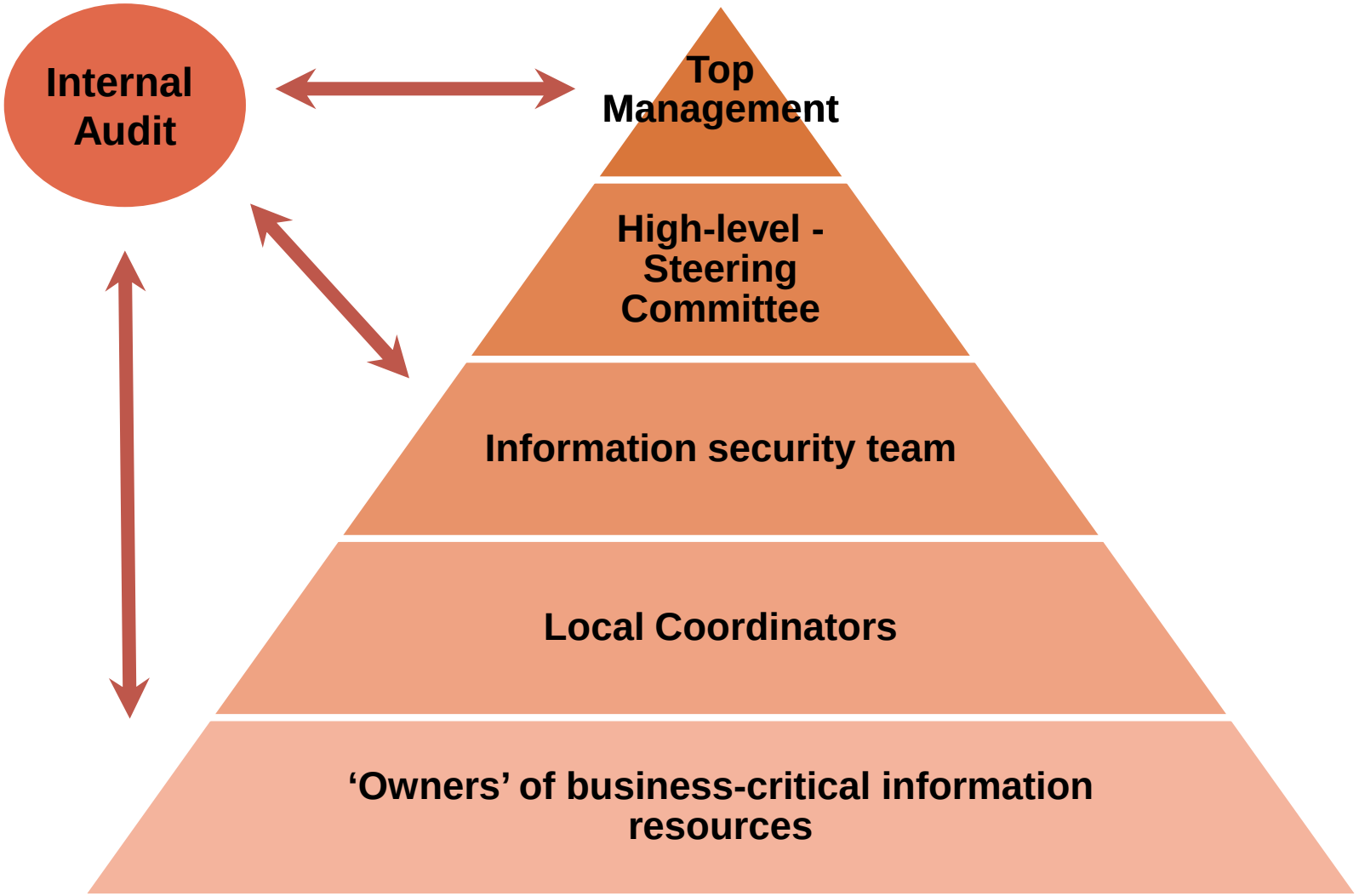
Why

- While Information Security is everyone's responsibility, roles and responsibilities have to be clearly established so that security controls are properly executed

Guiding principles

- IS organization in direct relationship with top managers
- IS organization at every level of the organization (Think global / act local)

OVERALL ISEC ORGANIZATIONAL MODEL



IMPLEMENTING A SECURITY POLICY

INFORMATION SECURITY POLICY IMPLEMENTATION (SECPOL)

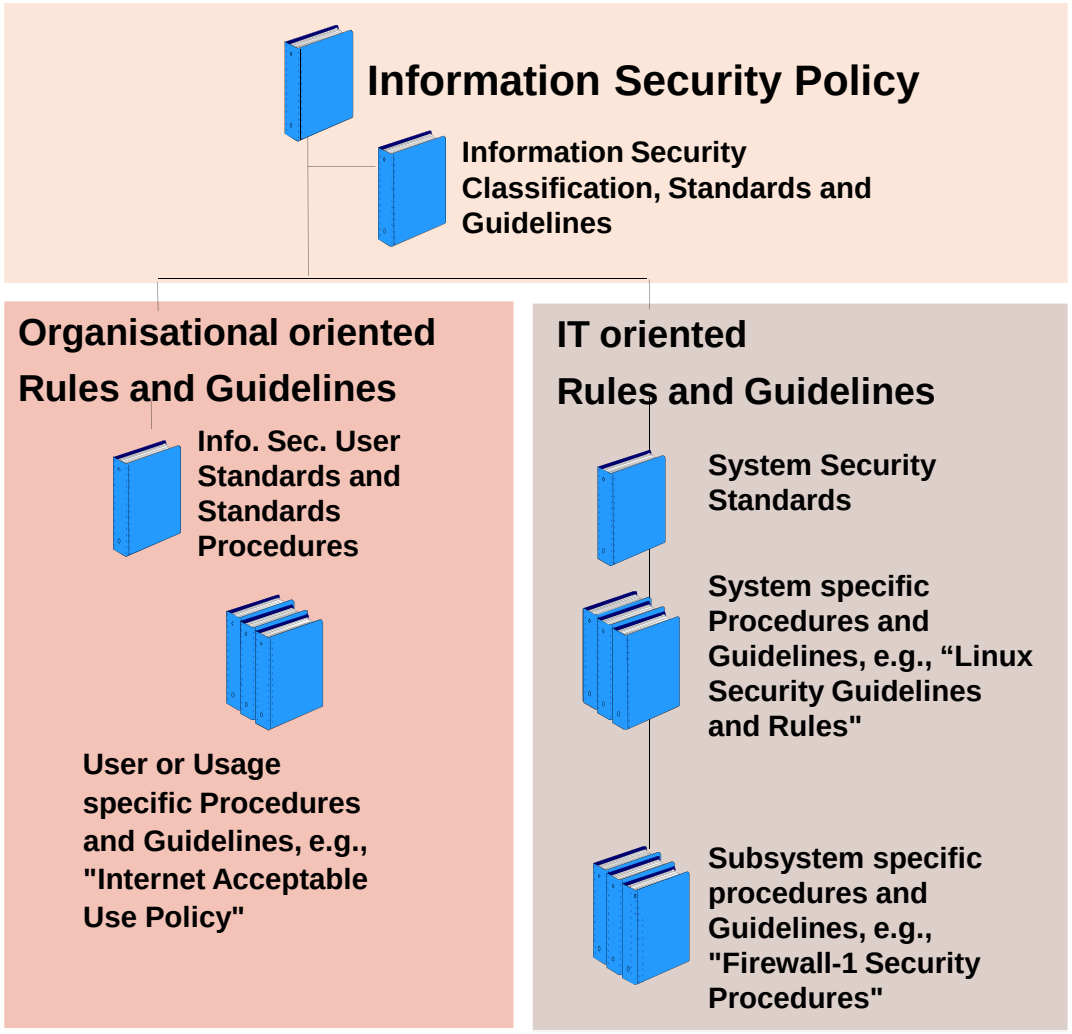
Why ?

- Info security is about protecting the company business and therefore people's own job and privacy
- benefits of security practices in day-to-day activities must be understood by all involved parties
- Well defined 'metrics' must be measurable to establish the success of the information security program

Objectives

- Make available and inform all interested parties about the Information Security Policy
- Ensure that all interested parties understand and abide to the policy
- Make sure that Business Lines and support functions' processes are aligned with this policy
- Define and implement the ISec compliance monitoring process / permanent supervision

EXAMPLE OF INFORMATION SECURITY RULES, RESPONSIBILITIES & GUIDELINES



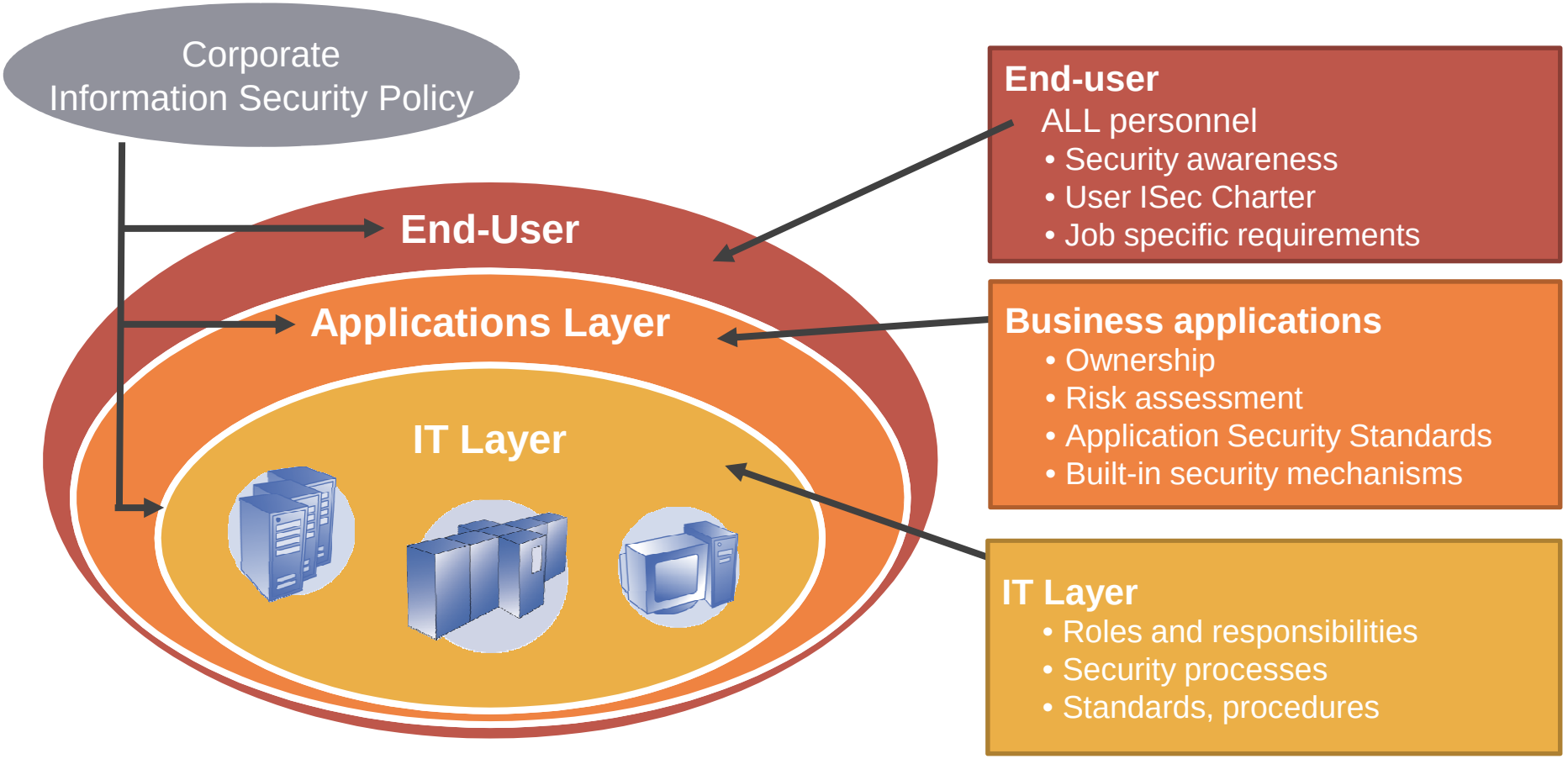
Management commitment and support for information security. Published and communicated, as appropriate, to all employees.

Translation of Policies into high level Standards and Guidelines

Translation of Policies and high level Standards and Guidelines into detailed procedures and Guidelines

© IBM / SG

INFORMATION SECURITY POLICY IMPLEMENTATION: 3 LAYERS



GET ISEC INCIDENT RESPONSES CAPABILITIES

ISEC INCIDENT RESPONSE CAPABILITIES

Objectives

- Make available legal, business, communication, technical and security resources organized to respond to ISec incident in appropriate way
- Produce dedicated processes, guidelines and reflex sheets

Why ?

- Incident Response capability is needed to protect the business and therefore people's privacy

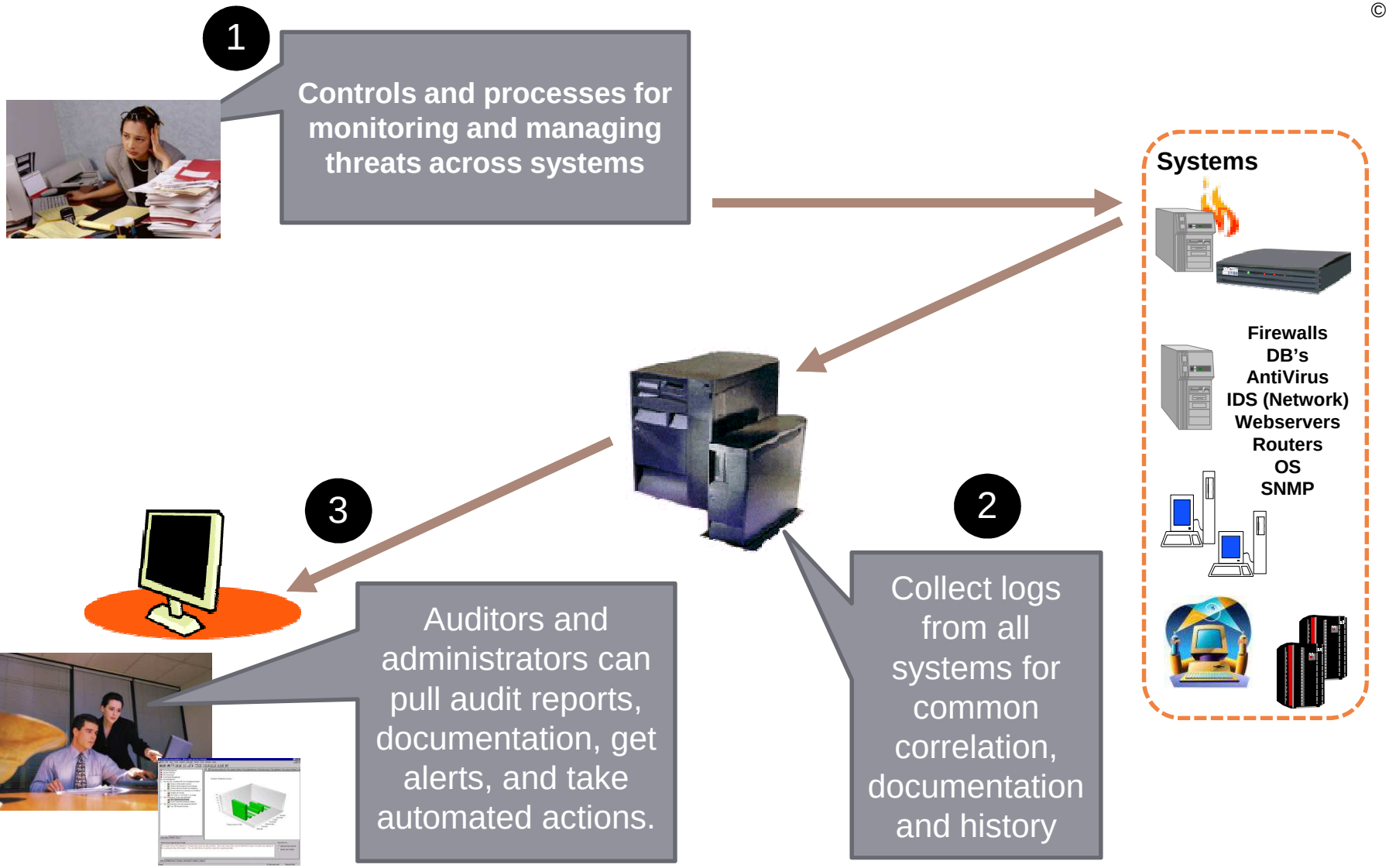
Guiding principles

- Primary focus on critical applications
- ISec-IRT must be integrated within the crisis organization, permanent supervision and ISec governance

Global guidelines must be available to :

- identify incident levels : event, incident, alert, alarm, crisis
- Define escalation levels and procedures
- Provide ISec-IRT organization

CONTROLS AND PROCESSES FOR RISK MANAGEMENT AND SECURITY THREAT MONITORING



BUILD THE INFORMATION SECURITY OPERATIONAL CENTER

BUILD THE INFORMATION SECURITY OPERATIONAL CENTER

Objectives

- Have a global and coherent security services, when appropriate
- Provide a resilient set of security services : available, reliable, scalable, flexible, secure, and manageable

Why

- Security objectives are global and aligned on Business objectives
- Risk management ISec require a consistent and permanent security level
- Security services must be easy to apply, efficient and manageable

Guiding principles

- Define the largest set of common security services
- Design and provide implementation support for key security services
- Identify the subset of security services to be shared and must be implemented in the Security Operational Center

BUILD THE INFORMATION SECURITY OPERATIONAL CENTER

- **What ?**
  - baseline security services examples :
  - Data and applications access tracking
  - ISec permanent supervision components
  - Evidence management, storage and archiving
  - Certificate, authenticators, token, biometrics and PKI management
  - Permanent and recurrent control
  - Metrics
  - Etc.

- **Manage ISec Ops related projects**

- **Relationship with Regional Security Co-coordinators**
- **Interface with local business managers**
- **Implement local or global solutions for compliance with policies and standards**

- **Participate in incident management activities ISec-IRT**

MANAGING AND CONTROLLING INFORMATION ACCESS CONTROL

MANAGING AND CONTROLLING INFORMATION ACCESS

Why ?

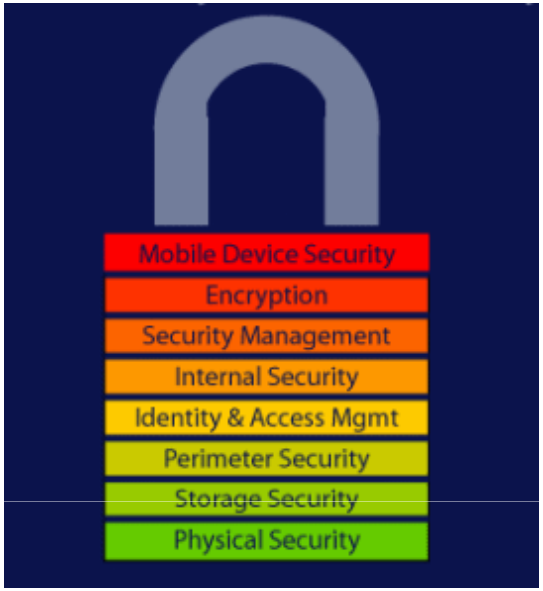
- The newest constraints of regulator authorities enforce to have detailed, completed and clear control access procedures.
- Implementation of centralized access rights management is a major change management project.
- Define classification rules to sensitive data, applications, IT infrastructures and users classes

Guiding principles

- Have the security level of access control and management endorsed by Business Lines and Supports Management
- Special focus on Third party access management

How ?

- What assets need to be protected?
  - Identify the critical assets
  - Classify the assets
  - Identify the owners
  - Classify the asset value
  - Determine how the critical assets are used
  - Identify risks and exposures



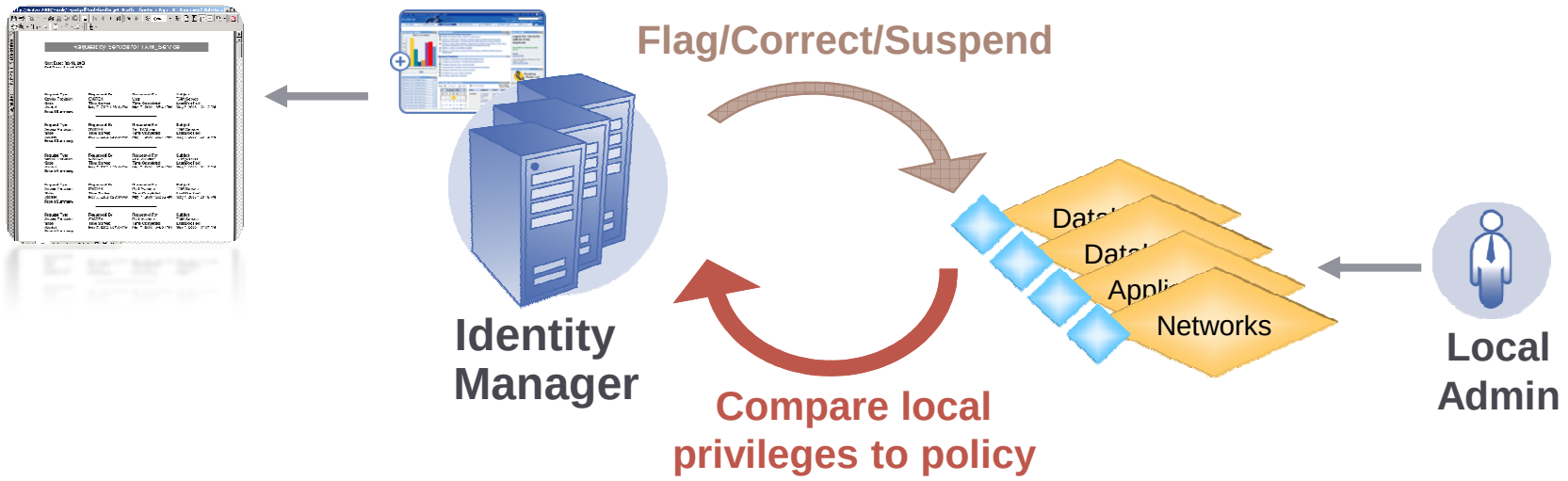
- Protect Assets to Specification
  - Develop and/or modify security policies and standards
  - Design technical solutions for secure distributed systems, secure electronic commerce applications, cryptographic key management systems, smart card applications, etc.

Information Classification example

- NC : Not Classified
- C1 : Internal Use
- C2 : Restricted Distribution
- C3 : Secret

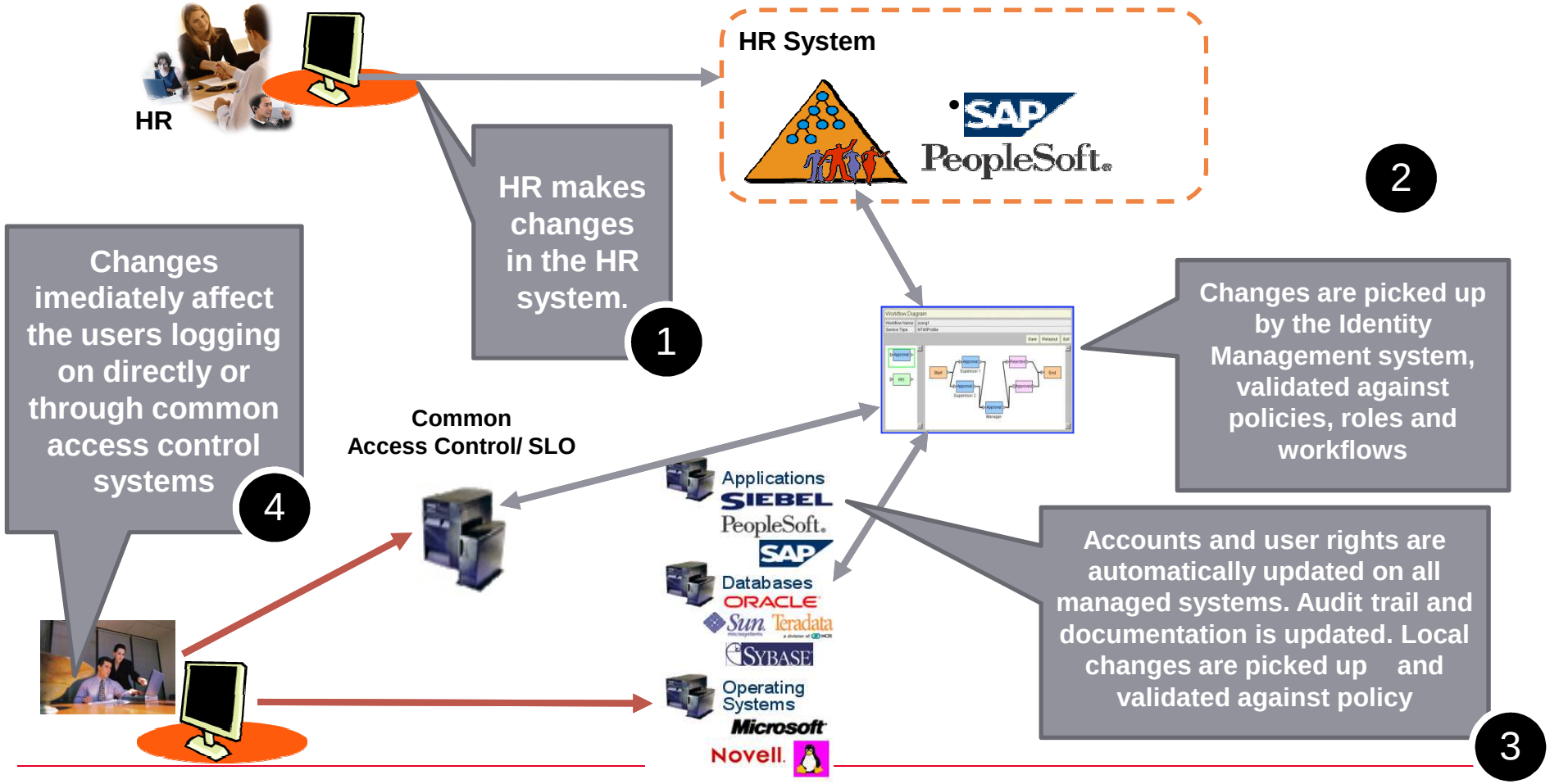
Good practice : Know which people have access to which information assets and ensure access policies are enforced

- Improve security by automatically finding, flagging, and/or removing invalid or over-privileged accounts
- Audit actual user access rights against privilege rules.
  - Know who has access to what
  - Know when access rights are violated
  - Evaluate and audit or correct changes made by local administrators



MANAGING AND CONTROLLING INFORMATION ACCESS

- **Good practice : Implement adequate controls of user IDs and association of privileges for access to business sensitive data**

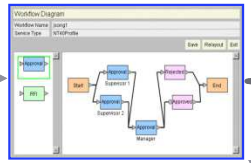


MANAGING AND CONTROLLING INFORMATION ACCESS

- **Good practice : Implement adequate segregation of duties for granting access to business sensitive information, records and data**

HR, Manager, Self-service etc.

1 **Request for employees access to business applications**



Workflow is initiated to gather approvals from the right people, in order to comply with regulations 2

Approvers get notified and approves request.

Approvals are documented within audit logs and reports 3

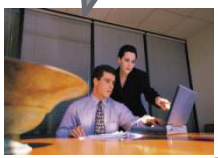
Applications: SIEBEL, PeopleSoft, SAP

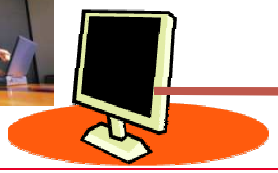
Databases: ORACLE, Sun, Teradata, SYBASE

Operating Systems: Microsoft, Novell

4 Access is provisioned to business applications

5 The right users have the rifght access to the right systems





THIRD PARTY ACCESS MANAGEMENT

THIRD PARTY ACCESS

Objectives

- Manage the risks issue from Third Party Access
- Define and drive the security of Third Party Access Management

Why

- All Third Party connections should be under the control of a specific process
- Third party connections typically include those made by external organizations (e.g. customers and suppliers), outsourcing suppliers and clients accessing the extranet

THIRD PARTY ACCESS

- **The Third Party Access Management Security Process should :**
  - restrict methods of connection
  - authenticate users in line with the type of access granted
  - restrict the type of access granted
  - grant access to the enterprise's information and systems on the principle of 'least access'
  - achieve technical compatibility
  - protect sensitive information stored on target systems or in transit to third party locations
  - log activity
  - terminate connections when no longer required
  - and provide a single point of contact for dealing with problems

INFORMATION SECURITY FORUM

DATA PRIVACY REGULATIONS

DATA PRIVACY REGULATIONS

Objectives

- Manage the risks issue from Privacy regulations (CNIL, Informatique & Libertés) applied on information systems
- Define and drive the compliance to Privacy law

Why

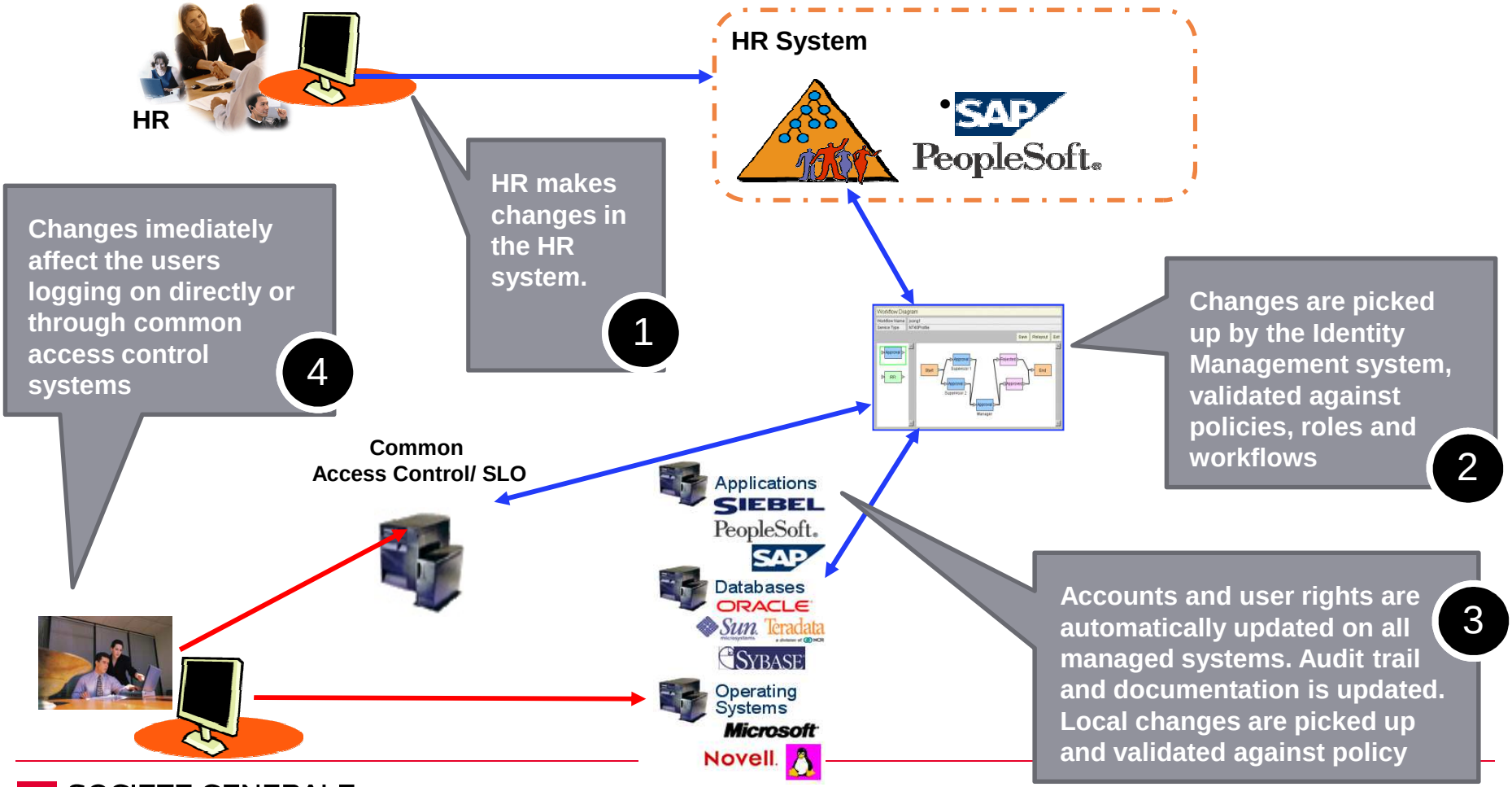
- Proper processes and controls supporting the Privacy ISec Policy must be defined and rolled-out

Guiding principles

- All private data connections should be under the control of a specific process
- As part of the process, risk analysis should take place and take into consideration the business risks associated with Privacy rules.

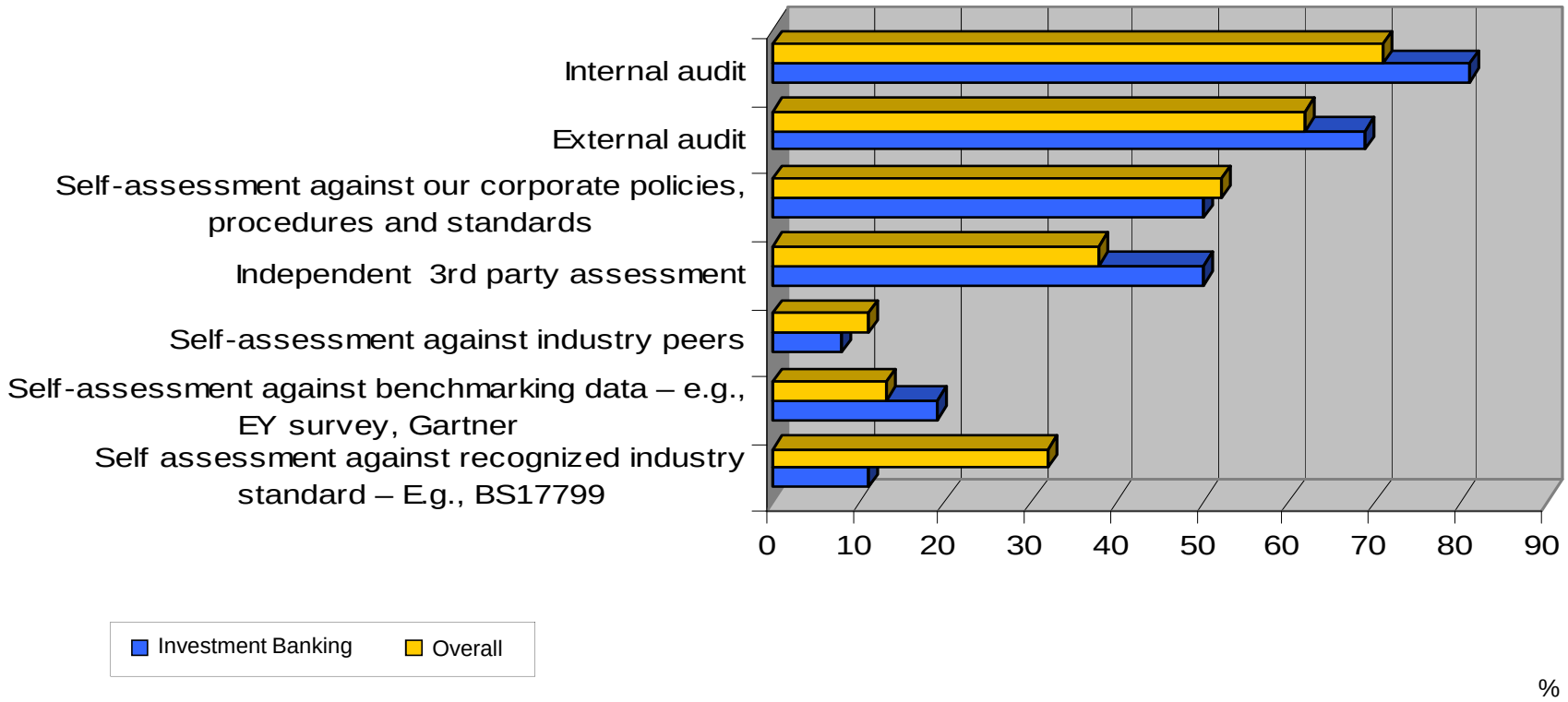
DATA PRIVACY REGULATIONS

- **Implement adequate controls of user IDs and association of privileges for access to private sensitive data**

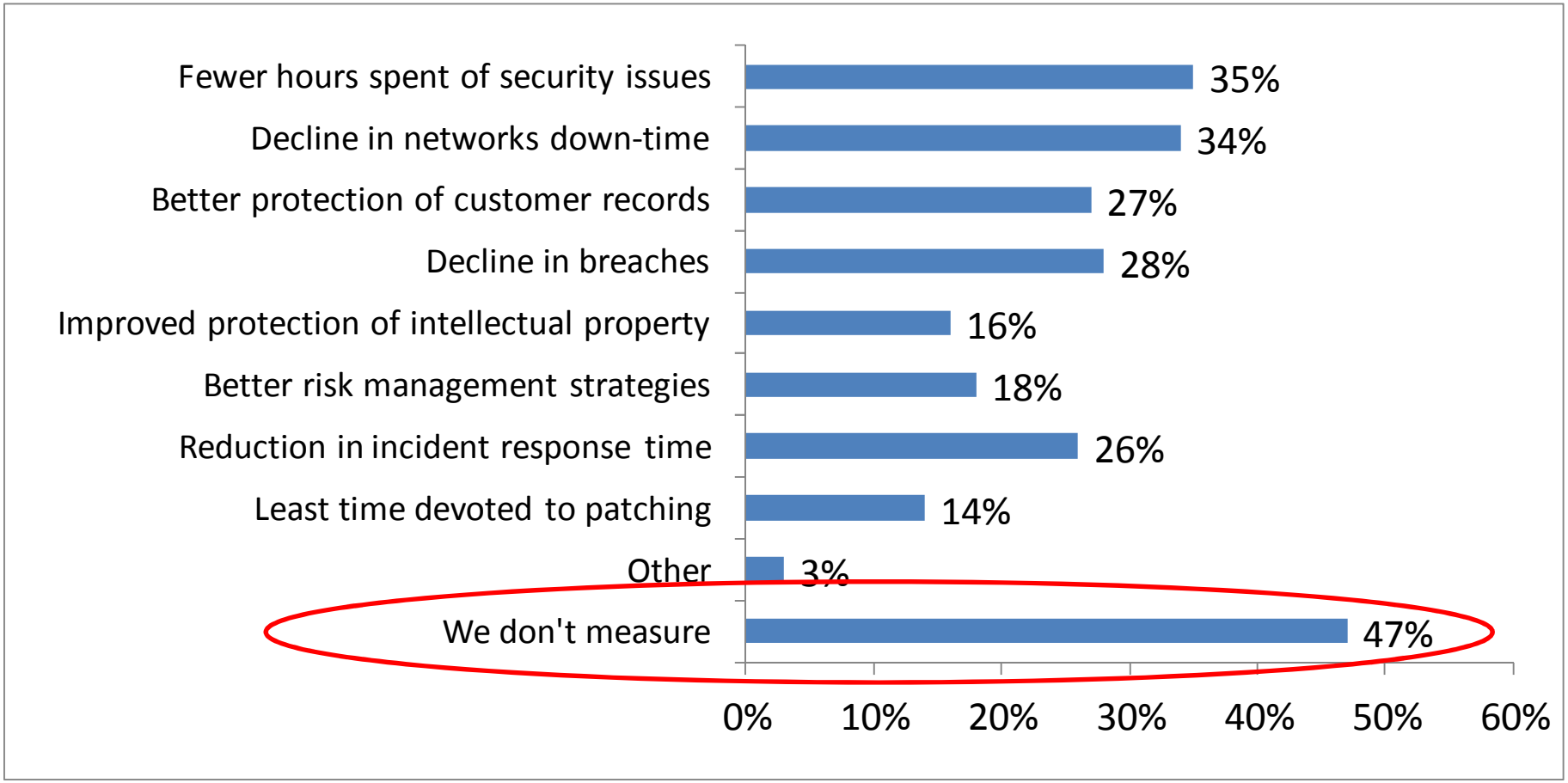


EVALUATION & MEASURE OF INFORMATION SECURITY EFFICIENCY

What are the main methods to evaluate the information security posture ?



How does your organization measure the value of your security investments ?



SECURITY METRICS AND MEASUREMENT

- **Effective measurement programs initiate continuous improvement**
- **Change nothing if measures are not analyzed and applied**
- **Proactive measurements enable effective changes**
- **Measurement supports management as a car's dashboard supports driving**

MEASURING INFORMATION SECURITY : METRICS CATALOG

Inventory

- People: Users, sec. FTEs
- Equipment: Desktops, servers, network devices, sec. devices
- Resources: connections, applications

Program Status

- % YTD spending of security budget
- % completion of annual objectives
- % confidence of completing objectives
- % security policies refreshed
- # new policies created/implemented
- % security processes refreshed
- # new processes created/implemented

Project Status (Major, per project)

- % completion
- % project timeline elapsed
- % project budget expended
- % confidence of completion

Compliance

- # compliance deficiencies, last audit
- # remaining open compliance deficiencies
- Y/N compliance audit up-to-date
- # of policy deficiencies, last audit
- # remaining open policy deficiencies
- Y/N policy audit up-to-date

MEASURING INFORMATION SECURITY: METRICS CATALOG

- **Communications/awareness**
  - % users "made aware" during period
  - % IT personnel trained during period
- **Risk assessment status**
  - # risk assessments conducted
  - # risk assessments in progress
  - # risk assessments pending/backlogged
  - # of crit. systems with expired RA
- **Vulnerability management (incl. patch)**
  - # security alerts processed
  - # of vuln. scans in period
  - # open vuln. by criticality
  - # open vuln. "area" by criticality
  - # vuln. reduction during period (area, vol.)
- **Event/incident management**
  - # privacy violations
  - # events (total, reportable, ability to be investigated, actionable)
  - # hours induced downtime by system crit.
  - # of incidents by type (config. error, zero-day vuln., unpatched vuln., user error, hacker)
- **Security systems status/health**
  - % desktops with fresh AV
  - % of FW/IDs/VPN/etc. with fresh firmware
  - % availability of security infrastructure
- **Service requests**

INFORMATION SECURITY TEAM ROLES

INFORMATION SECURITY TEAM ROLES

Global Sponsor for any Security topics

Permanent Supervision follow-up for IT departments

Coordination with the business and the IT teams through a network of correspondants

Awareness & training

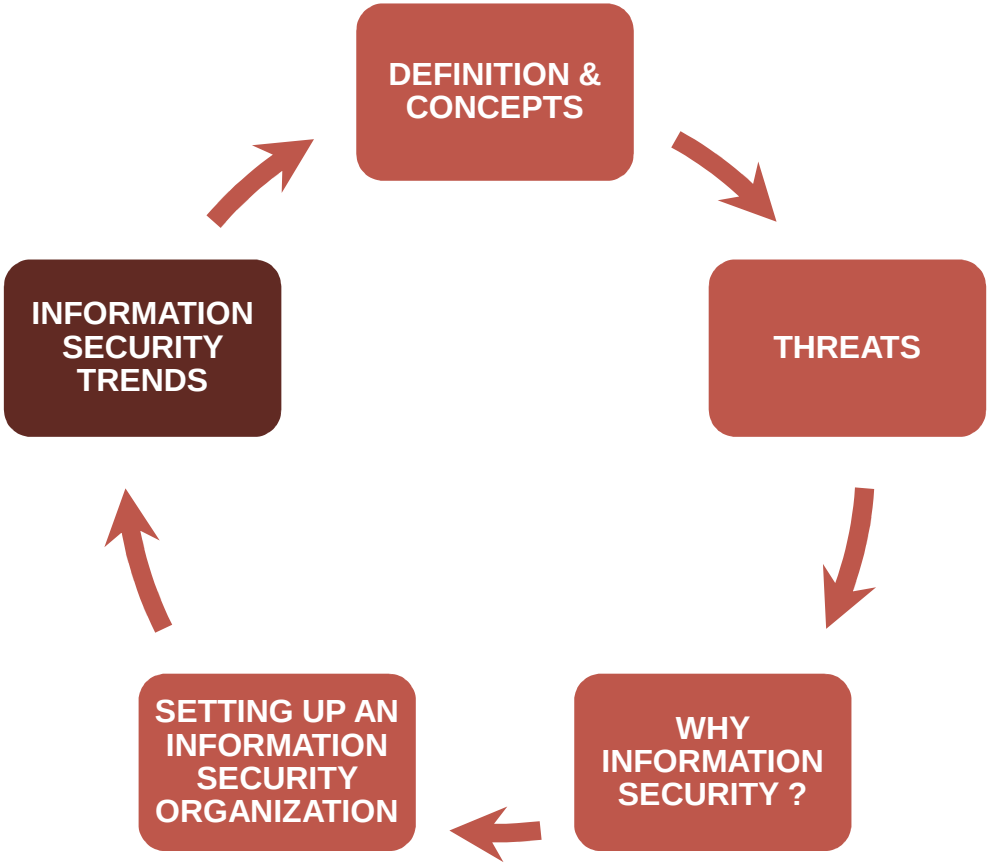
Audits follow-up

Policies, guidelines and standards governance

Projects Security expertise

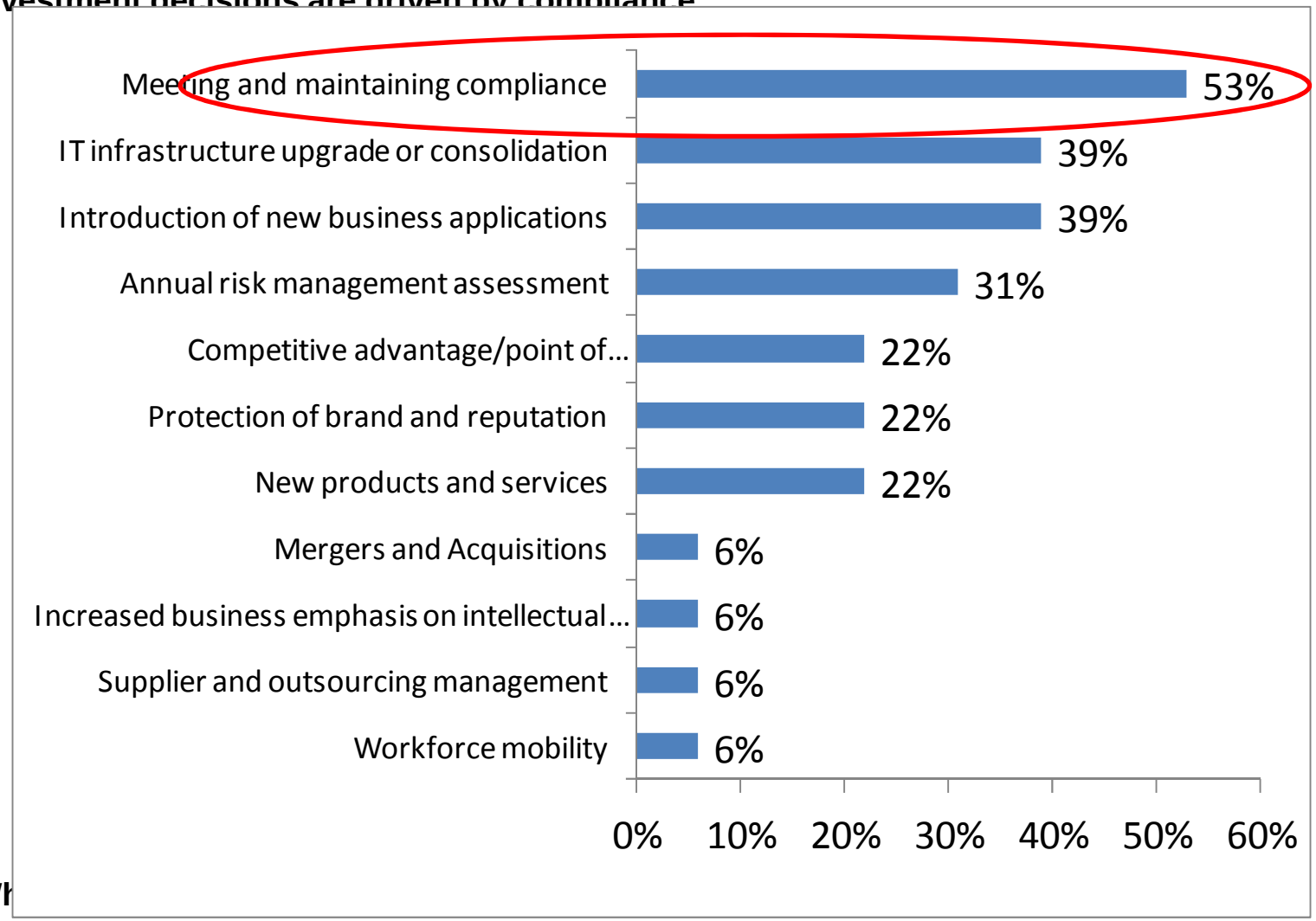
INFORMATION SECURITY

INFORMATION SECURITY TRENDS



INFORMATION SECURITY TRENDS

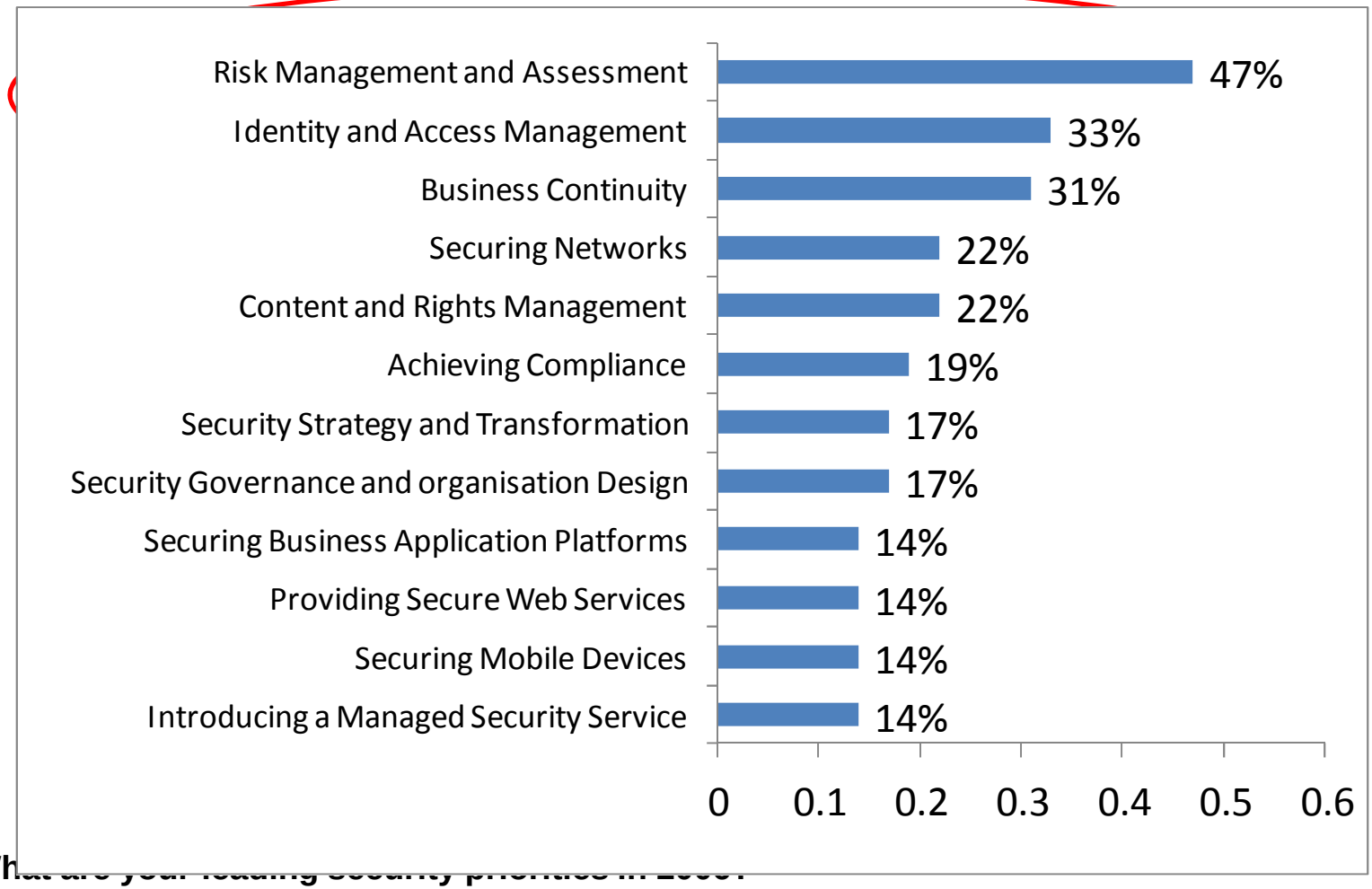
- **Investment decisions are driven by compliance**



- **Wh**

INFORMATION SECURITY TRENDS

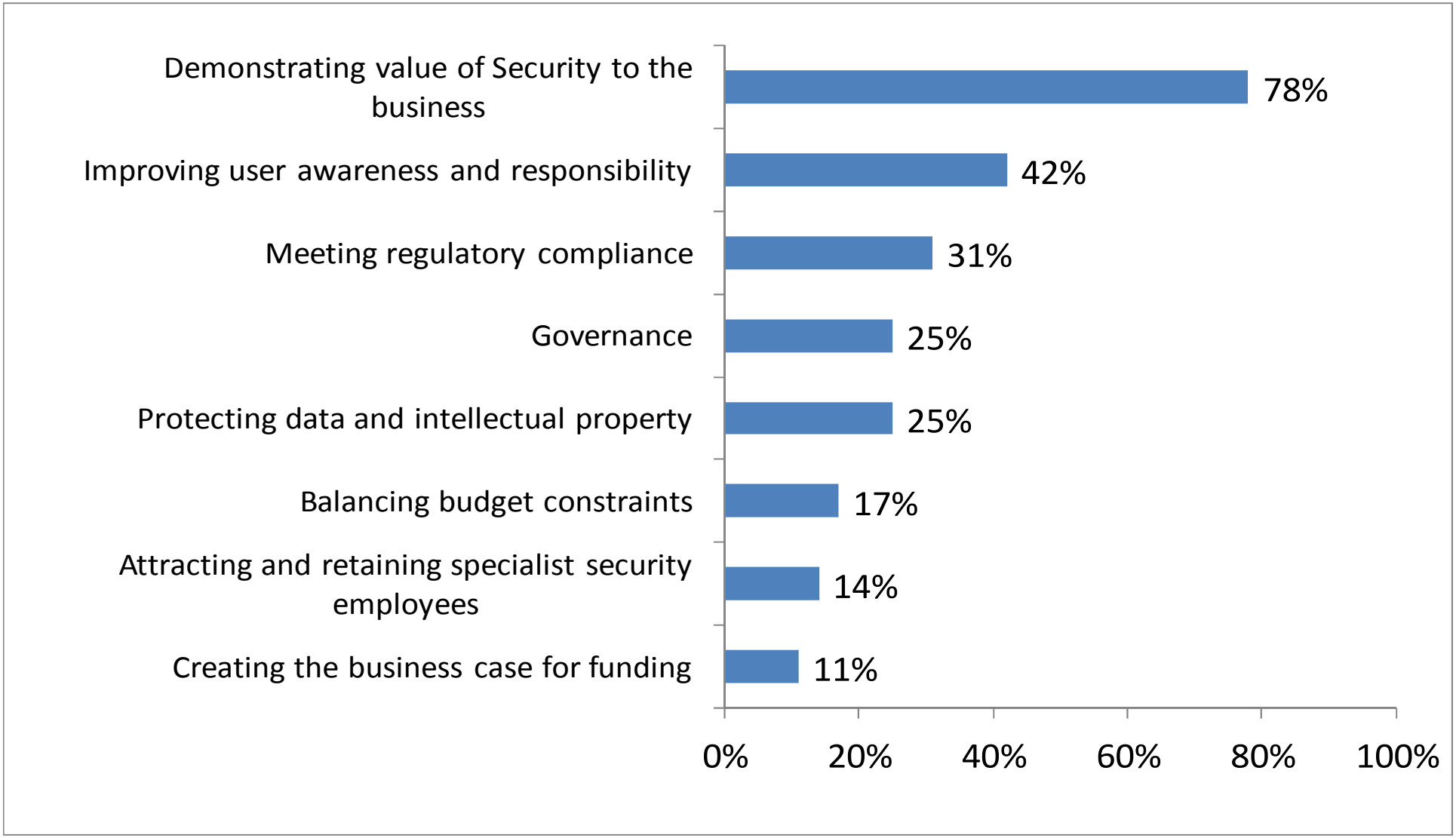
- **Identifying and managing risk is a priority**



- **Wh[illegible]**

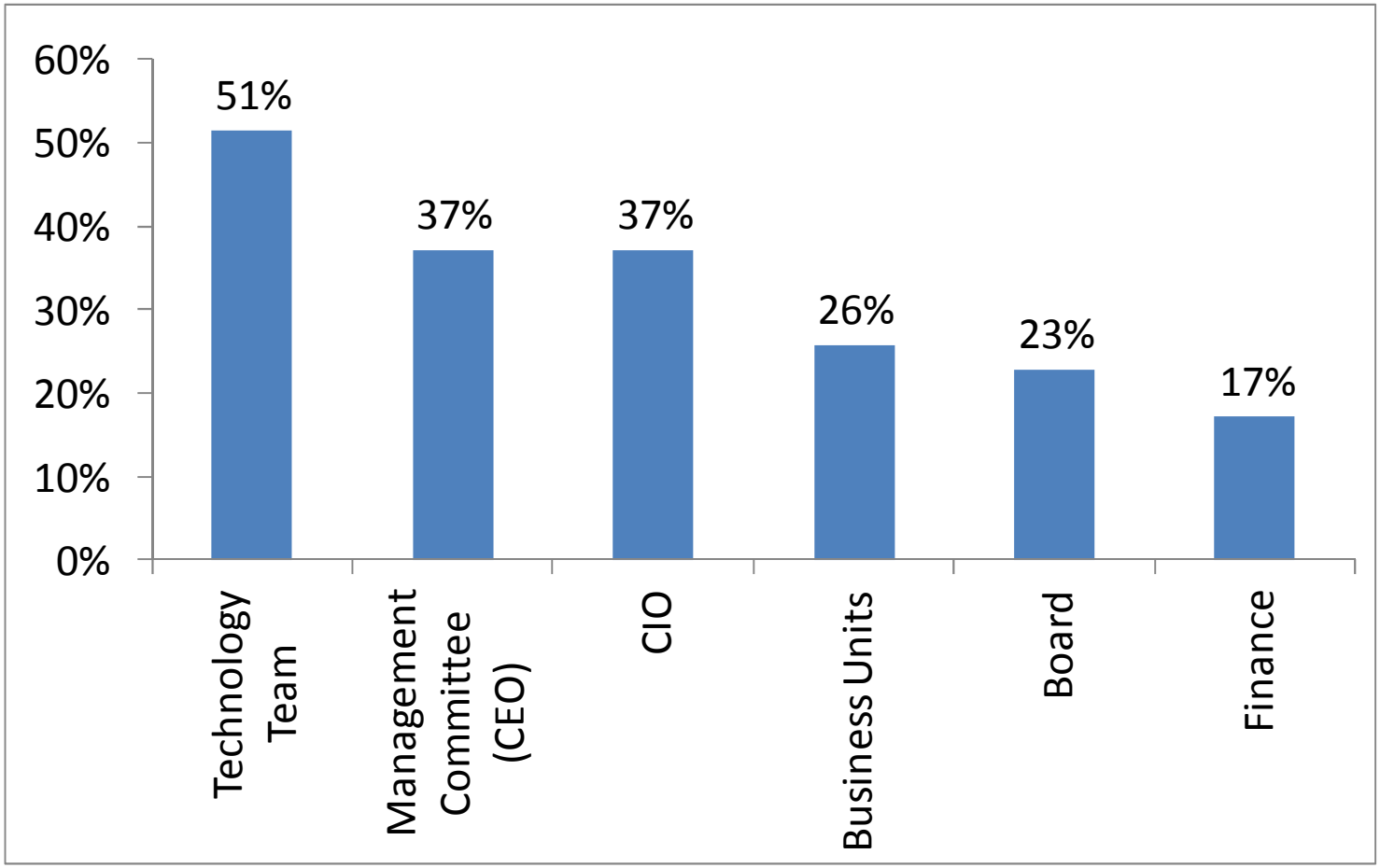
INFORMATION SECURITY TRENDS

- **Demonstrating the value of security is a major challenge**

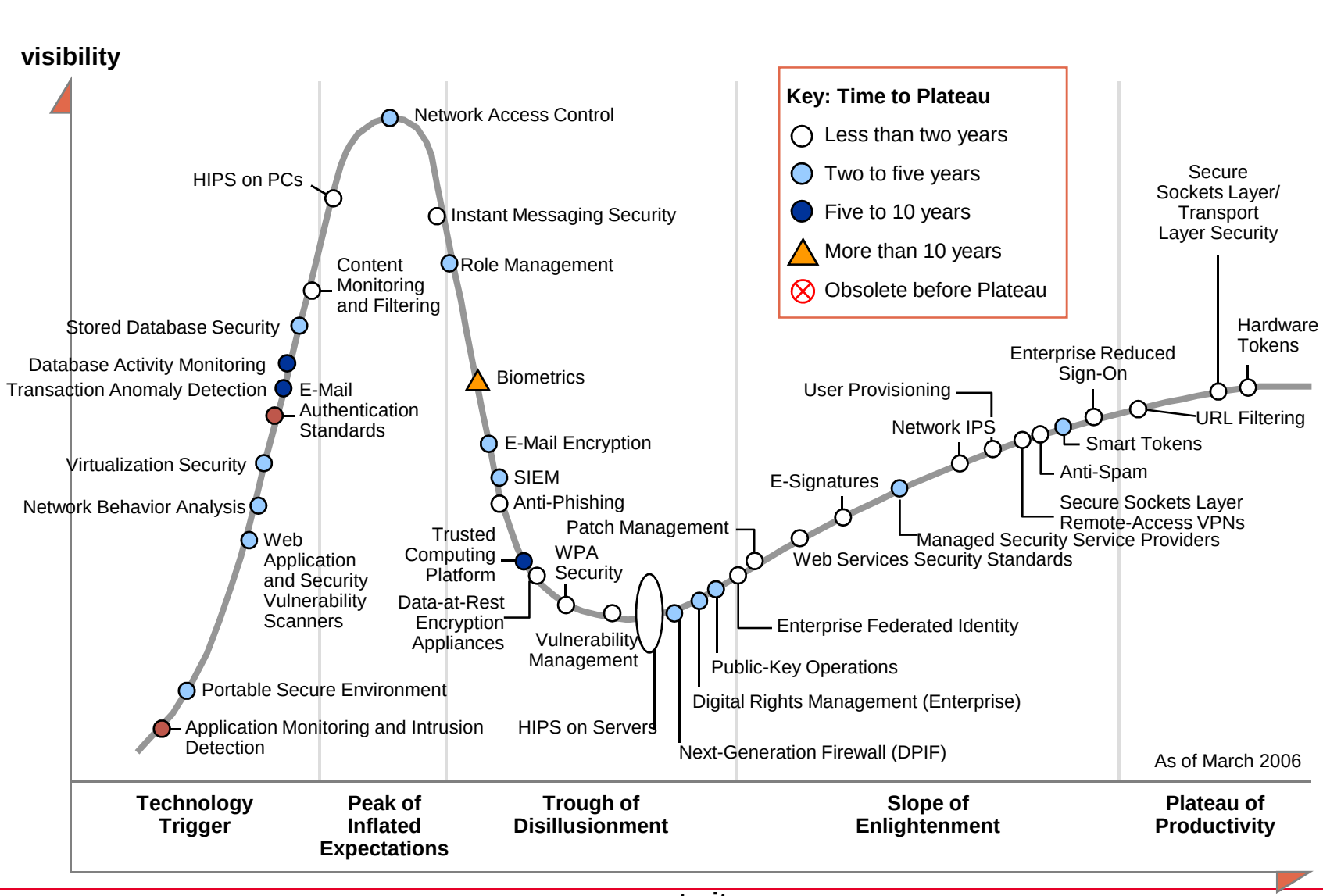


TOO OFTEN SECURITY IS SEEN AS A TECHNOLOGY ISSUE

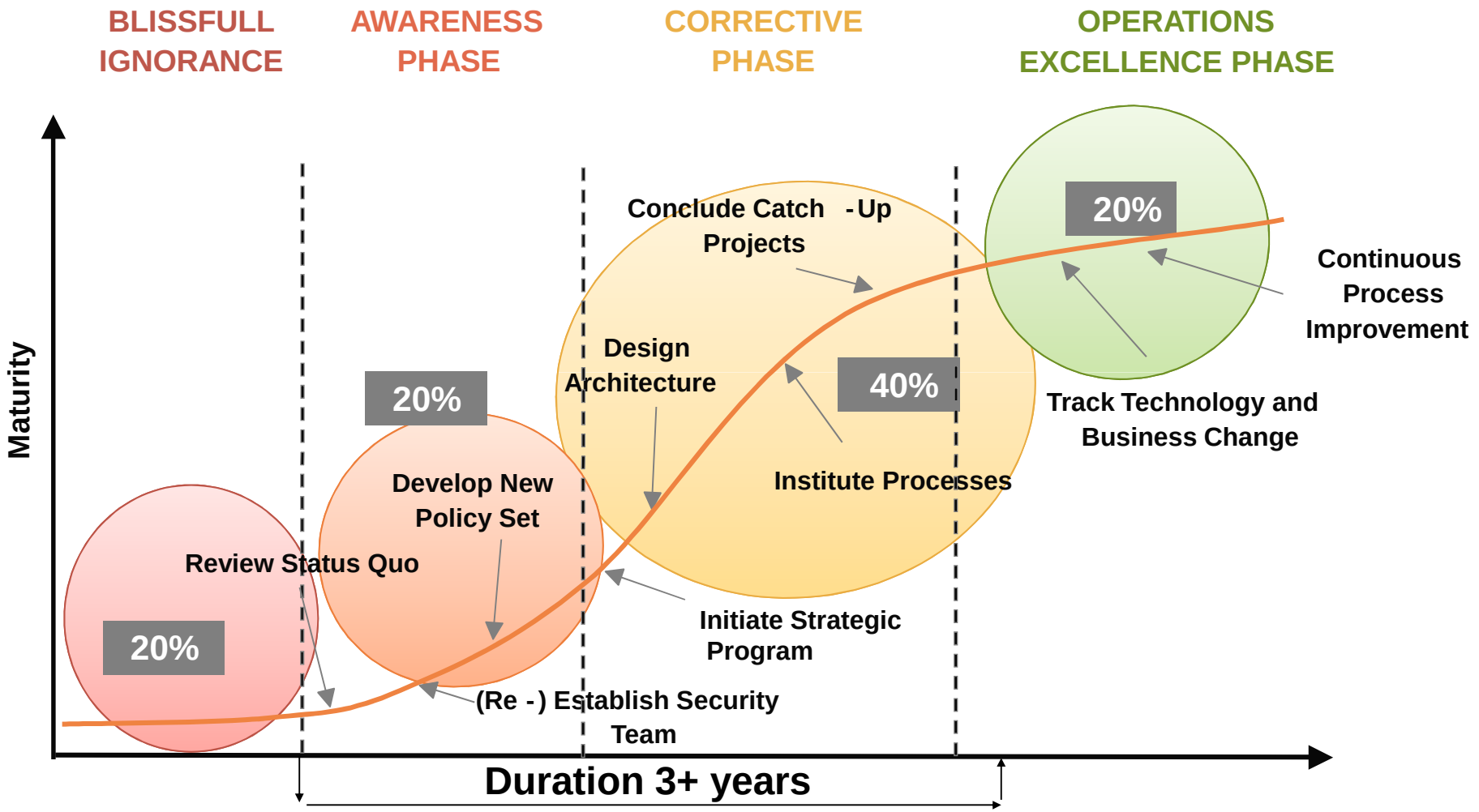
- **Who are the primary influencers of your security decisions ?**



INFORMATION SECURITY TRENDS : HYPE CYCLE SECURITY



INFORMATION SECURITY TRENDS : PROGRAM MATURITY



INFORMATION SECURITY TRENDS : 12 POSITIVE TRENDS FROM E&Y

Integrating Information Security with the Organization

Trend 1: Information risk management is becoming integrated into overall risk management.

Trend 2: Information security is now more integrated in companies' cultures.

Trend 3: The information security function is now more integrated in outsourcing discussions.

Extending the Impact of Compliance

Trend 4: The impact of compliance continues to grow.

Trend 5: Compliance is promoting teaming between information security and other functional business groups.

Trend 6: Compliance is improving information security.

Managing the Risks of Third Party Relationships

Trend 7: Companies are managing their suppliers' vendor-related risks.

Trend 8: Suppliers are managing their own vendor-related risks.

Focusing on Privacy and Personal Data Protection

Trend 9: There is an increasing focus on proactive privacy and personal data protection.

Trend 10: Privacy and personal data protection practices are becoming increasingly formalized.

Designing and Building Information Security

Trend 11: Information security is becoming more proactive in meeting business objectives and business continuity planning.

Trend 12: Information security is increasingly adopting recognized standards.

DO'S

Use strong passwords and change them regularly: a minimum of 8 characters, uppercase & lowercase letters, numbers and special characters.

Be aware of social engineering attacks: validate the requester's identity; verify the legitimacy of the request and provide as little information as possible.

Exercise responsible behavior: report any incident to your company local helpdesk and keep informed by regularly visiting the company Security intranet.

Use e-mail systems carefully. Be careful when opening e-mail from unknown senders: do not open attached files, do not forward, do not open web links.

Apply the « clear desk policy »: do not leave information unattended on desks, printers, meeting rooms, etc. Lock your PC by using the password controlled screen saver and reboot it regularly.

Use mobile devices securely: use an anti-theft security cable and an encrypted hard drive. Beware of shoulder surfers and never leave mobile equipment unattended.

Classify electronic files and hardcopy documents (NC non classified, C1 internal usage only, C2 restricted distribution, C3 secret).

DON'TS

Don't share your account or your password without proper authorization or **use someone else's personal account** (application or system).

Don't bypass security control systems (web-mail access, tunneling, WiFi, etc.).

Don't view, download, forward or store illegal files or data (pornography, pedophilia, racism, xenophobia, cracked files or software, etc.).

Don't publish your company e-mail address for personal purposes (forums, etc.) or use your company name as a reference when expressing your own political, religious or other personal views on such forums, bulletin boards etc.

Don't share copyrighted multi-media files (mp3, divx, etc.) or **overload network traffic with voluminous files.**

Don't install hardware or software without a license and proper authorization.

Don't attempt to remove classified data (C1, C2, C3) **from your company premises** (e-mail, CD/DVD, USB key, PDAs, Portable devices etc.).

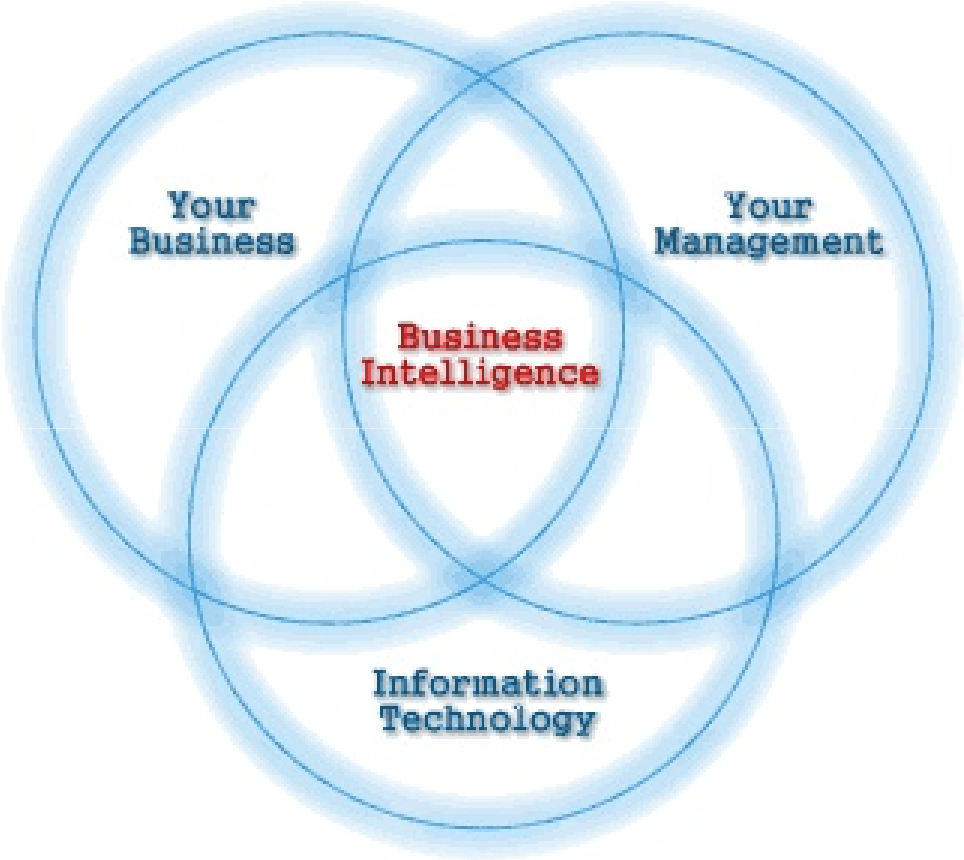
INFORMATION SECURITY

Conclusion

INFORMATION SECURITY: SIX POINTS TO UNLOCK THE VALUE OF SECURITY

- Assess and manage risk in terms of disruption and value to the business
- View compliance as a catalyst for business improvement and innovation
- Embed security in the business
- Automate security administration and management
- Leverage people and processes as well as technology to proactively manage threats and vulnerabilities

BUSINESS INTELLIGENCE: A QUICK OVERVIEW…



THE POWER OF INFORMATION …

ERIKA = TOTAL

PRESTIGE = ?

Anticipation vs. reaction

- Information needs to be controlled :
  - White : press, internet, seminars … 80%
  - Grey : client documentation, consultants … 15%
  - Black : n/a

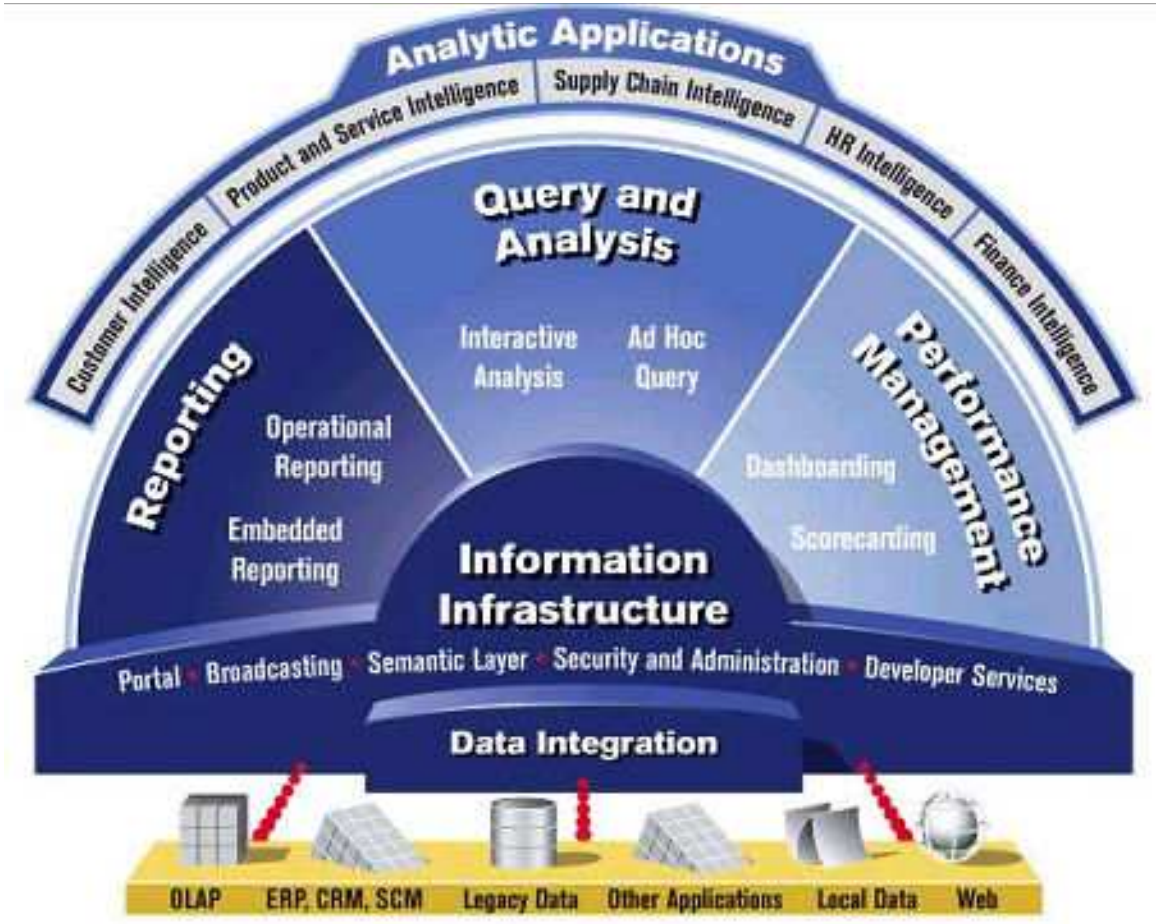
BUSINESS / COMPETITIVE INTELLIGENCE (INTELLIGENCE ÉCONOMIQUE)

- **"… is the art of threats and opportunities detection while coordinating the collection, the sorting, the memorization, the analysis and the diffusion of any useful or strategic information" for the organization (Bernard Besson)**

- **Therefore the targets are**
  - To anticipate against threats and vulnerabilities
  - To identify growth opportunities for the organization

- **Competitive Intelligence is an ethical and legal business practice**

BUSINESS INTELLIGENCE AT A GLANCE



CONCLUSION

- **FACT : The Information is key in the decision process**

- **REALITY :**
  - The management of the information is not yet organized

- **NEED :**
  - The information needs to be managed : collection, analysis, dispatching …
  - The information needs to circulate : bottom / up – top / down
  - The information needs to be protected : Information Security, Communication …
  - … at every level of the organization, by everyone …

FUTUR FICTION

2020

- 20 billion devices connected to the internet
- Every piece of hardware uniquely identifiable, but organised crime clones them anyway
- Duplicate identities commonplace, but ignored
- Physical location and multiple biometric verification required for high value transactions
- EBay enters financial services markets with more than 1 billion active traders – banks start to fail
- Google merges with NewsCorp and buys CNN and BBC

© Steve Prentice
Gartner

2025

- EBay buys NYSE and LSE to control global trading
- Privacy no longer exists, Global Identity database now stores more than 2 billion people, but is compromised
- Deteriorating environmental conditions make most of Northern Hemisphere hazardous to elderly and young
- Nanotech and biosensors used to check foodstuffs
- Remote medical sensing now mandatory for insurance
- Merger of virtual gaming worlds creates 8th largest economy on the planet with more than 80 million citizens

2030

- EBay becomes the global trust broker, exceeding the influence of governments and regulators
- Silicon computing reaching the limits
- First organic and molecular compute matrices added to the global compute grid
- More than 100 billion devices connected to the net
- Business is redefined by P2P trading and exchanges
- The Information Age enters the final stages

© Steve Prentice
Gartner

QUOTE

“There are three roads to ruin : Women, Gambling and Technology.
Women are the most pleasurable, gambling is the quickest, but technology is the most certain !”

President Pompidou