Segurança em Redes de Computadores
Computer Network Security
(SRC)

(MIETI 4º Ano/S2 - 6707N5)

Henrique Santos (hsantos@dsi.uminho.pt)

Dpt. Sistemas de Informação

Ext. 510302

Sumary

- InfoSec Fundamentals
  - Simple Model for InfoSec (ISO 27k)
  - Attacks, Threats and Vulnerabilities in computer networks
  - InfoSec Policies
- Applied cryptography
- Access Control
- Security in TCP/IP based networks
- InfoSec Technologies
  - Biometrics
  - IPSec
  - SSL/TLS
  - Firewalls
  - Intrusion Detection Systems
  - VPN
  - …
- Introduction to forensic analysis

Teaching Objectives

- Develop essential knowledge on various information security technologies as well as the technical skills required for its correct implementation, which together are critical to enabling a conscious and effective involvement in designing and implementing an Information Security Management process; and
- Alert to issues (technical, personal, organizational, educational, etc.) related to the topic of Information Security in the current context of "Cyberspace"

Learning Outcomes

- Recognize the importance of a culture of security with respect to the use of computer systems and networks
- Identify the technical aspects of computer systems and networks that expose them more to security risks
- Recognize the main threats and the typical way the attacks are carried out
- Analyze vulnerabilities in networked systems
- Plan security strategies for networked computers
- Implement continuous management and control processes, defined in the context of a security policy for networked computers
- Use security analysis and auditing tools for computer and networks

Assessment Strategy

- Homework & Exercises (70%~80%)
- Final “cyber exercise” or essay (10%~25%)
- Participation in class initiatives (5%~10%)

- Late delivery concerning homework and other evaluation material is accepted with a penalty of 5%/hour!
- Attendance control in theoretical lessons is applied, but there are no absence limit. In the TPs **is mandatory** the presence of the 2/3 classes
- The UC monitoring will be done by Moodle platform

Assessment Strategy

- Homework & Exercises

Risk Analysis (2 weeks)

- Application of a RA simple method to a particular situation

Access Control (2 weeks)

- Use a formal model to specify an Access Control policy in a particular environment

Basic PKI deployment & Management (2 weeks)

- Use ADSS or OpenSSL to deploy a typical (simple) PKI

Network Traffic analysis (2 weeks)

- Use network security tools to understand network vulnerabilities and perform traffic analysis

Network Security – Firewall & IDS (2 weeks)

- Use open source tools to implement fundamental network security functions (traffic filters and intrusion detection)

Computer Security & Pen Testing (3 weeks)

- Experimenting attack tools and assess vulnerability's exploits impact

Final Pen Test Exercise

Bibliography

- Pfleeger, Charles P., Pfleeger, Shari L., “Security in Computing”, Fourth Edition, Prentice Hall PTR, 2007.
- C. Douligeris and D. N. Serpanos, “Network Security: Current Status and Future Directions” Wiley-IEEE Press, 2007. http://www.ebook3000.com/Network-Security--Current-Status-and-Future-Directions_22046.html
- Stallings, W., “Cryptography and Network Security: Principles and Practice”,5th., Prentice Hall Press, 2010.
- Bishop, M., “Introduction to Computer Security”. Prentice Hall PTR, 2004.
- Kaufman, C., Perlman, R., and Speciner, M., “Network Security: Private Communication in a Public World”. Second ed., Prentice Hall PTR, 2002.
- Bosworth, S., and Kabay, M. E., “Computer Security Handbook” 4th ed.: John Wiley & Sons, Inc., 2002.
- Anderson, R. J. ,“Security Engineering: A Guide to Building Dependable Distributed Systems”, 2nd Ed., Wiley Publishing, 2008. (http://www.cl.cam.ac.uk/~rja14/book.html)
- Santos, H. D., “A norma das normas em Segurança da Informação”, Publicação da Associação Portuguesa para a Qualidade, XXXV, 1 (Primavera, 2006), 11-19.
- Zúquete, A., “Segurança em Redes Informáticas”, 3ª ed., FCA – Editora Informática, 2010.

- CERT Coordination Center, http://www.cert.org/
- NIST Computer Security Division 893 and CSRC Home Page, http://csrc.nist.gov/
- Resources for Security Risk Analysis, Security Policies, ISO 17799 (or BS7799) and Security Audit, http://www.securityauditor.net/
- The Computer Security Institute, http://www.gocsi.com/
- ...

Initial Reflection

> “*The world is never going to be perfect, either on- or offline; so let’s not set impossibly high standards for online.*”
>
> — Esther Dyson

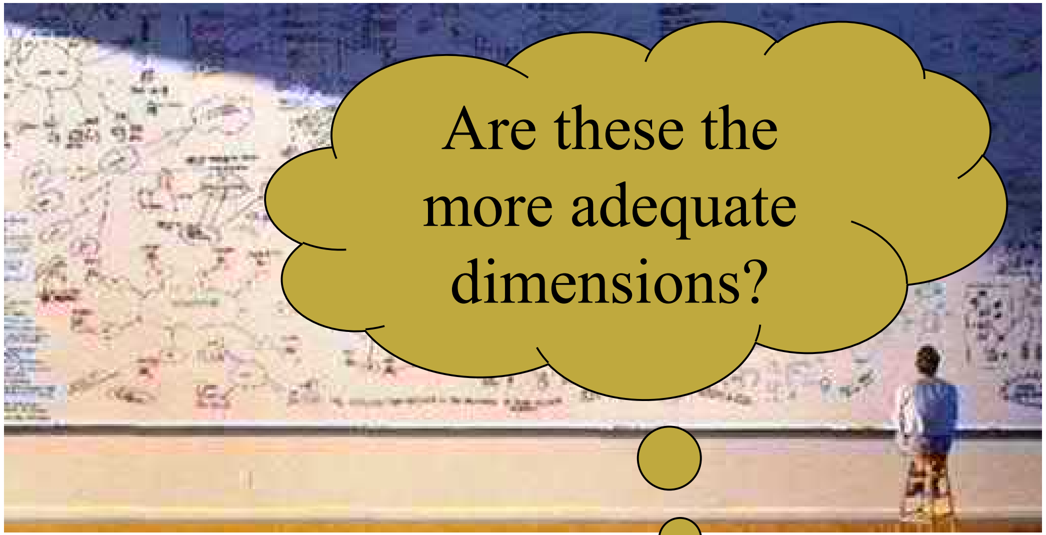
The Most Dangerous Town on the Internet - Where Cybercrime Goes to Hide

Contextualization

- Evolution of information technology (≈50 years)
  - Few computer centers isolated
  - Time-sharing
  - Data networks (Distributed Systems)
  - Personal computers
  - Ubiquitous computing, mobility and the technology convergence
- The first “worm”
  - In 1975, the scientific fiction classic from John Brunner, *The Shockwave Rider*, provided the first computer program that replicates itself and propagates itself

Contextualization

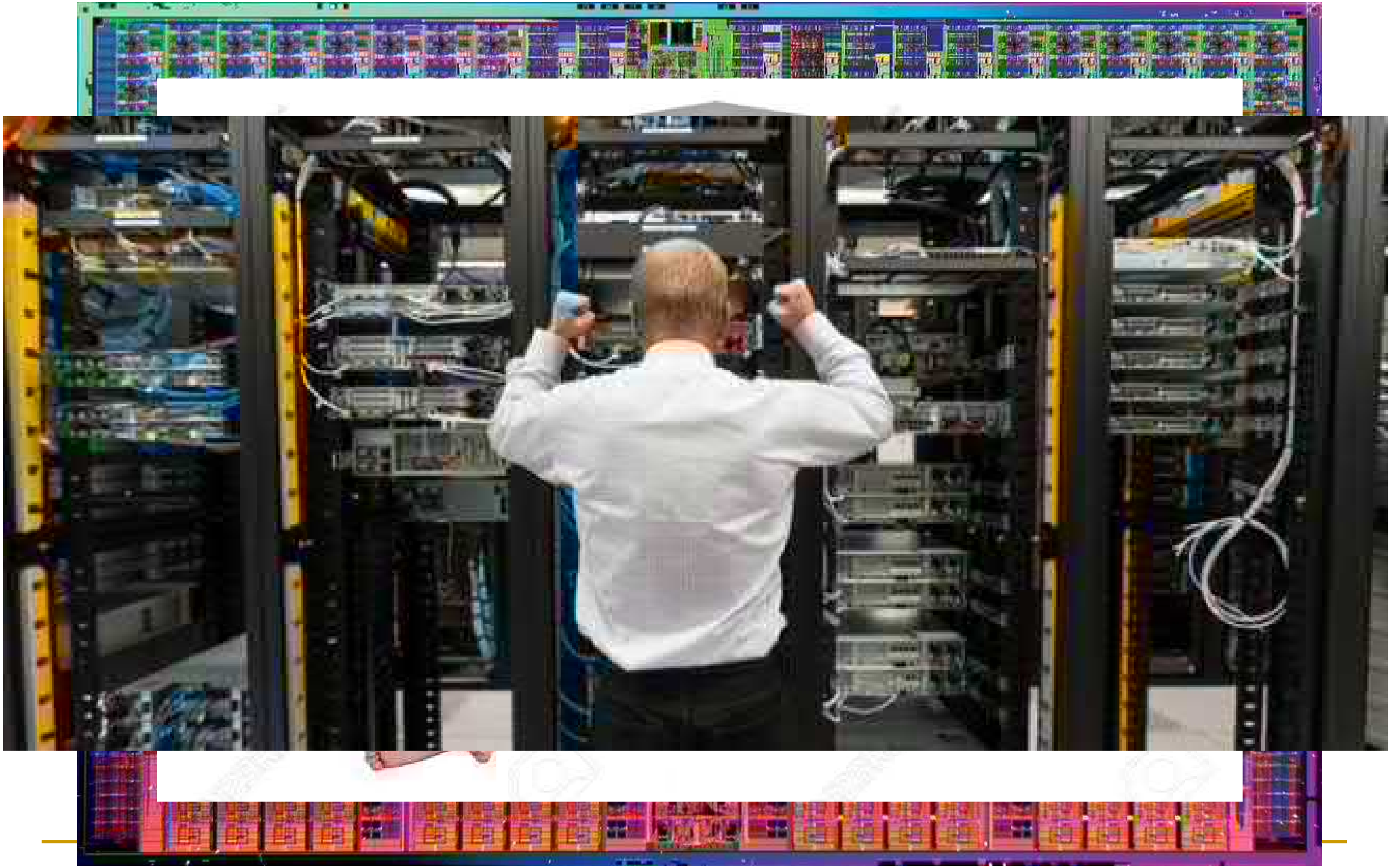
- **Complexity:**
  - Non rigorous engineering process
  - Legacy systems
  - Component integration (COTS)
  - Diversity and flexibility
  - Short life cycle
  - …



Are these the more adequate dimensions?

- **Risks**:
  - Availability
  - Confidentiality
  - Integrity

Technological complexity



Tecnologias disruptivas

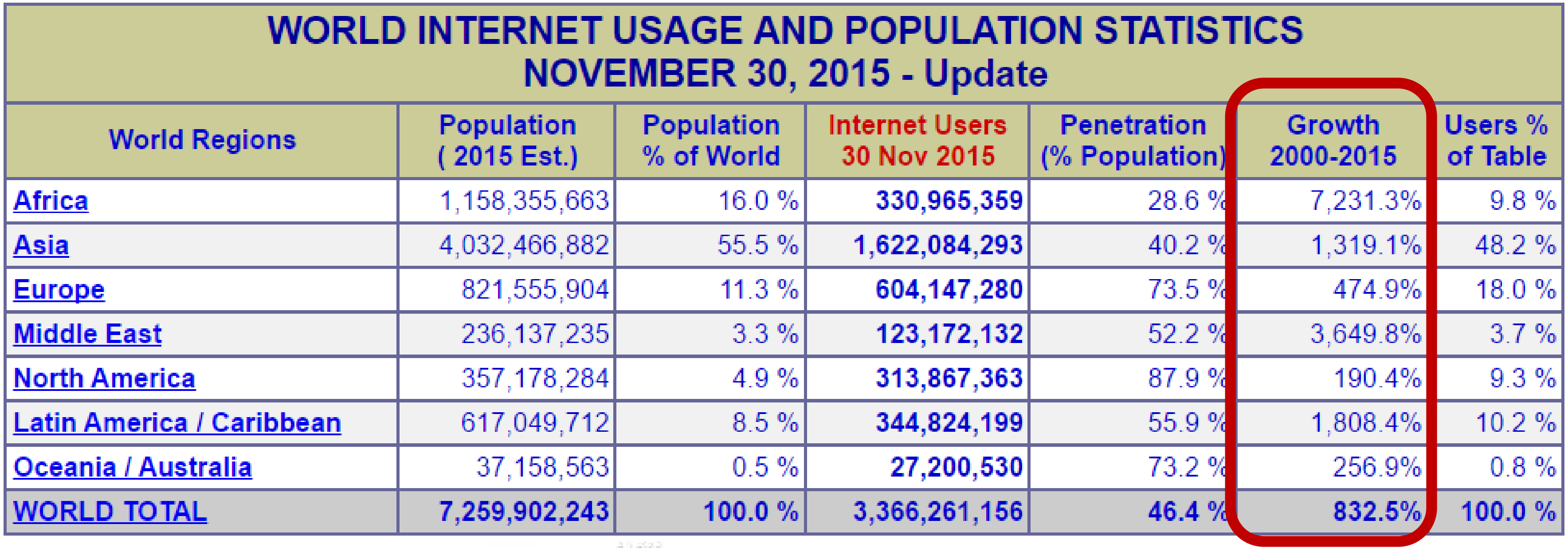
Cloud Computing

Azure Services Platform
salesforce.com
Microsoft
3tera
Sun
YAHOO! DEVELOPER NETWORK
force.com
Google
IBM
Google
vmware
EMC
amazon webservices
intel
MOSSO
NETSUITE
Joyent Accelerators
OpenID

Disruptive technologies

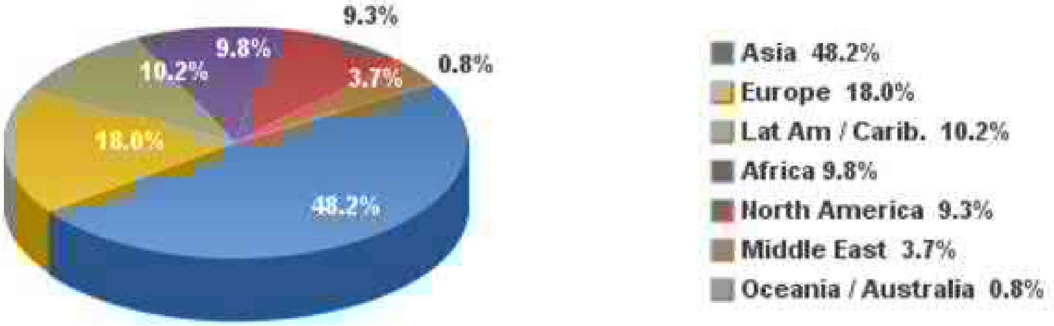
Complexity in social networks

- Internet statistics



WORLD INTERNET USAGE AND POPULATION STATISTICS
NOVEMBER 30, 2015 - Update

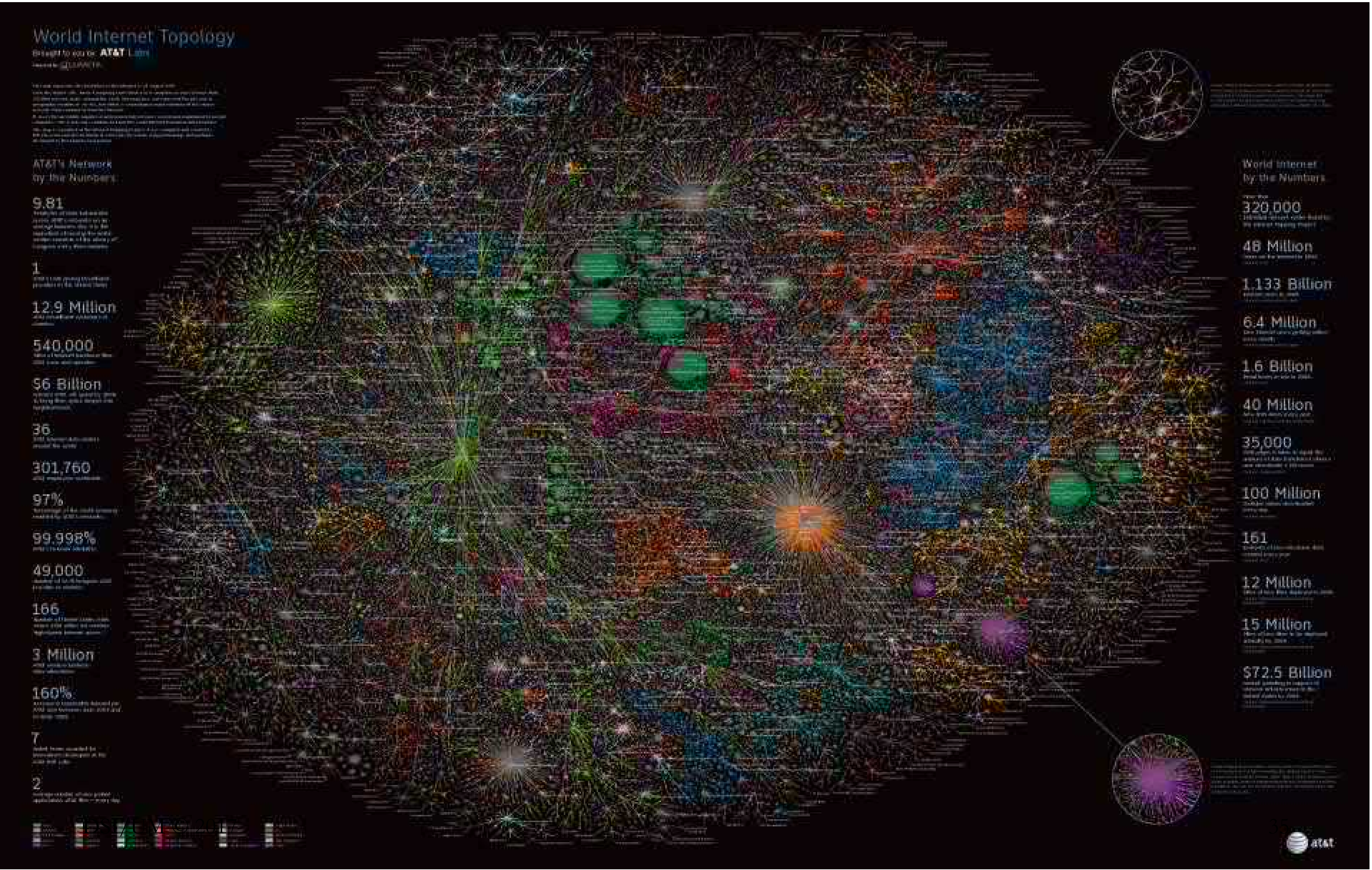
World Regions	Population (2015 Est.)	Population % of World	Internet Users 30 Nov 2015	Penetration (% Population)	Growth 2000-2015	Users % of Table
Africa	1,158,355,663	16.0 %	**330,965,359**	28.6 %	7,231.3%	9.8 %
Asia	4,032,466,882	55.5 %	**1,622,084,293**	40.2 %	1,319.1%	48.2 %
Europe	821,555,904	11.3 %	**604,147,280**	73.5 %	474.9%	18.0 %
Middle East	236,137,235	3.3 %	**123,172,132**	52.2 %	3,649.8%	3.7 %
North America	357,178,284	4.9 %	**313,867,363**	87.9 %	190.4%	9.3 %
Latin America / Caribbean	617,049,712	8.5 %	**344,824,199**	55.9 %	1,808.4%	10.2 %
Oceania / Australia	37,158,563	0.5 %	**27,200,530**	73.2 %	256.9%	0.8 %
WORLD TOTAL	**7,259,902,243**	**100.0 %**	**3,366,261,156**	**46.4 %**	**832.5%**	**100.0 %**



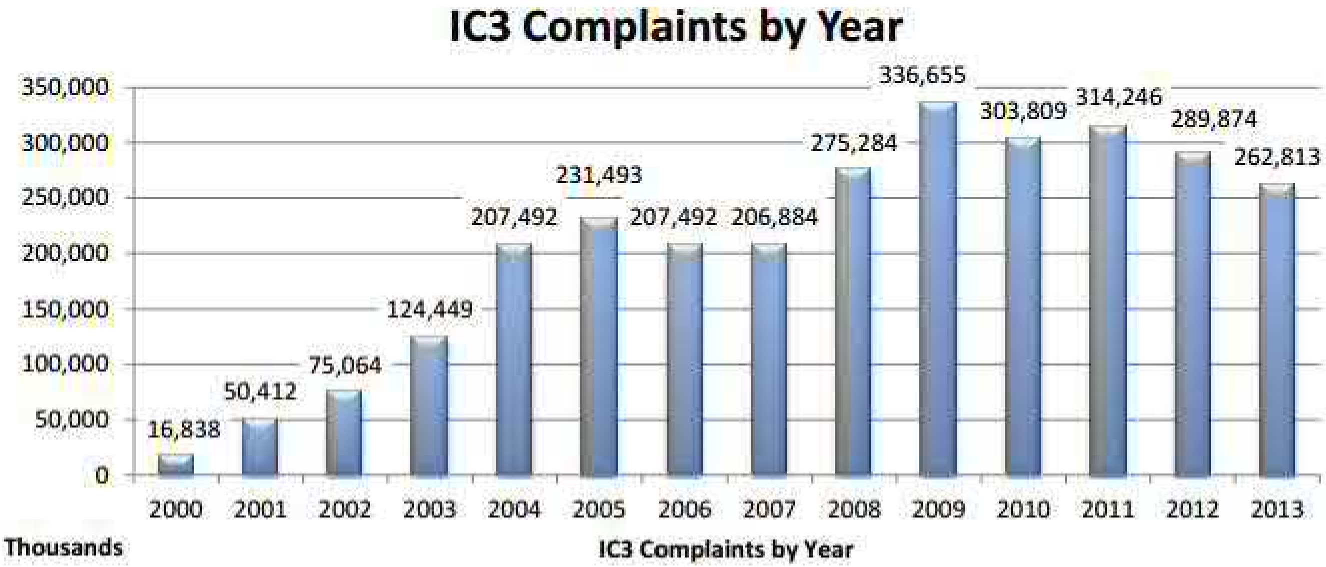
http://www.internetworldstats.com/stats.htm

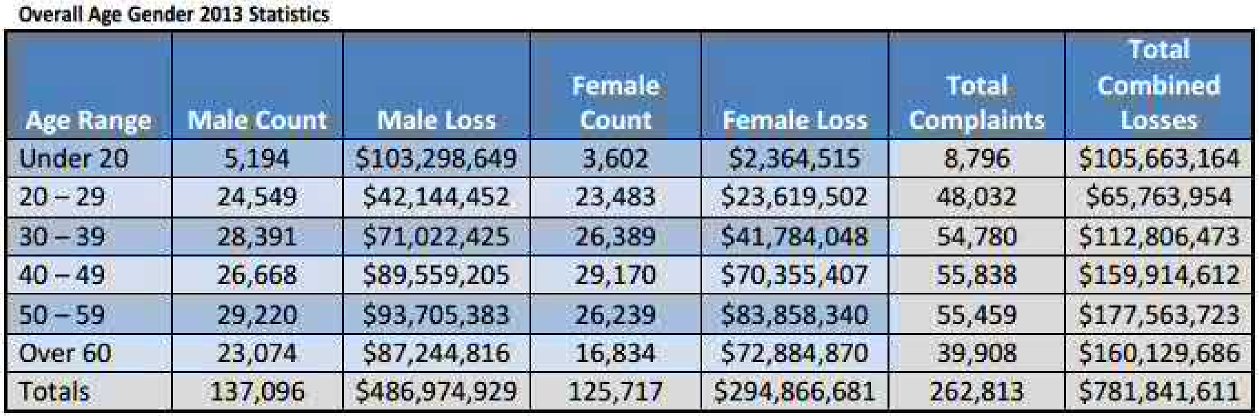
Ciber *backbone* – AT&T (2007)

http://javiergs.com/?p=983



Security incidents evolution

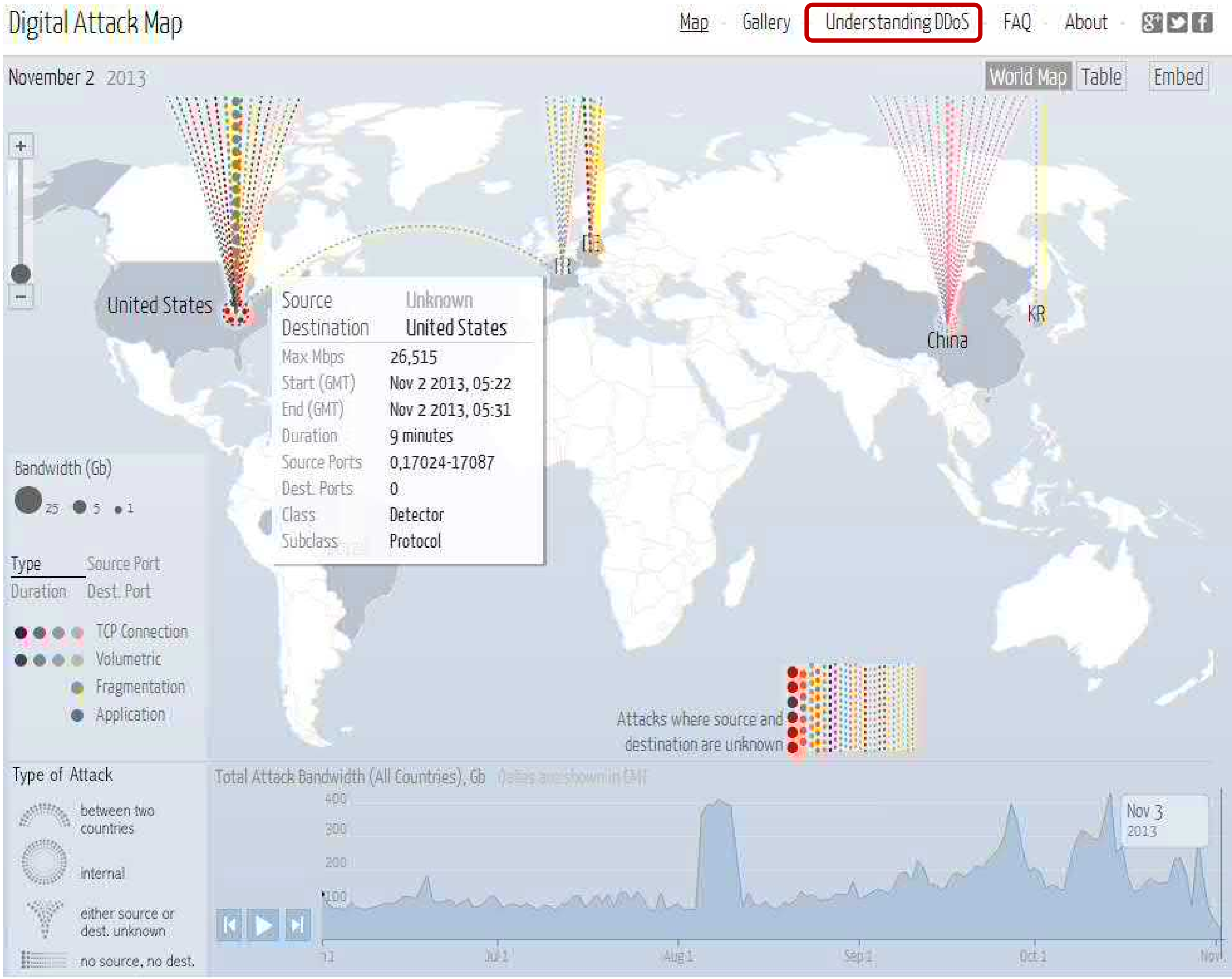




Overall Age Gender 2013 Statistics

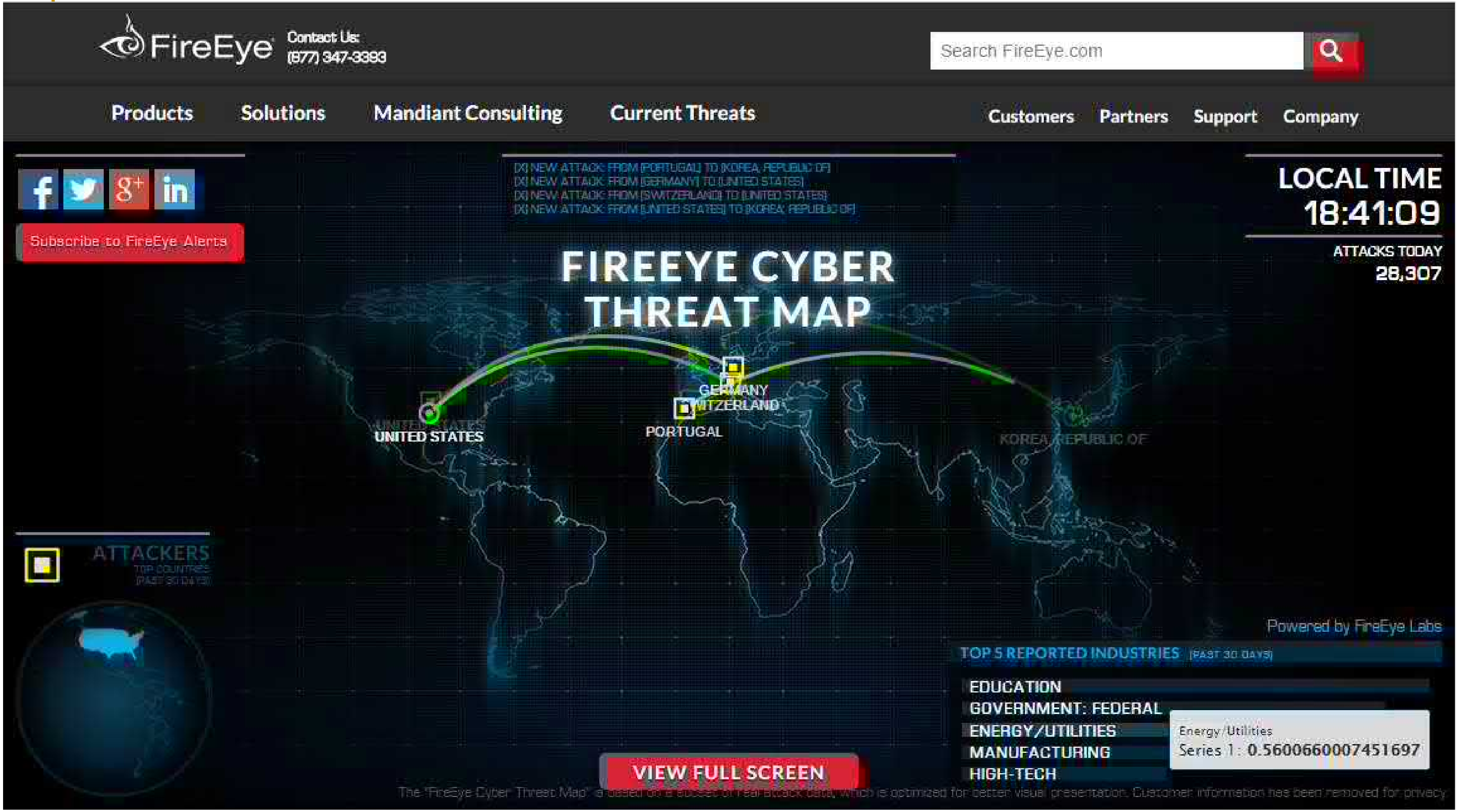
Age Range	Male Count	Male Loss	Female Count	Female Loss	Total Complaints	Total Combined Losses
Under 20	5,194	$103,298,649	3,602	$2,364,515	8,796	$105,663,164
20 – 29	24,549	$42,144,452	23,483	$23,619,502	48,032	$65,763,954
30 – 39	28,391	$71,022,425	26,389	$41,784,048	54,780	$112,806,473
40 – 49	26,668	$89,559,205	29,170	$70,355,407	55,838	$159,914,612
50 – 59	29,220	$93,705,383	26,239	$83,858,340	55,459	$177,563,723
Over 60	23,074	$87,244,816	16,834	$72,884,870	39,908	$160,129,686
Totals	137,096	$486,974,929	125,717	$294,866,681	262,813	$781,841,611

Fonte: FBI, 2013 Internet Crime Report



Source	Unknown
Destination	United States
Max Mbps	26,515
Start (GMT)	Nov 2 2013, 05:22
End (GMT)	Nov 2 2013, 05:31
Duration	9 minutes
Source Ports	0,17024-17087
Dest. Ports	0
Class	Detector
Subclass	Protocol

Cyber Attack Alerts



[X] NEW ATTACK: FROM [PORTUGAL] TO [KOREA, REPUBLIC OF]
[X] NEW ATTACK: FROM [GERMANY] TO [UNITED STATES]
[X] NEW ATTACK: FROM [SWITZERLAND] TO [UNITED STATES]
[X] NEW ATTACK: FROM [UNITED STATES] TO [KOREA, REPUBLIC OF]

FIREEYE CYBER THREAT MAP

LOCAL TIME
18:41:09

ATTACKS TODAY
28,307

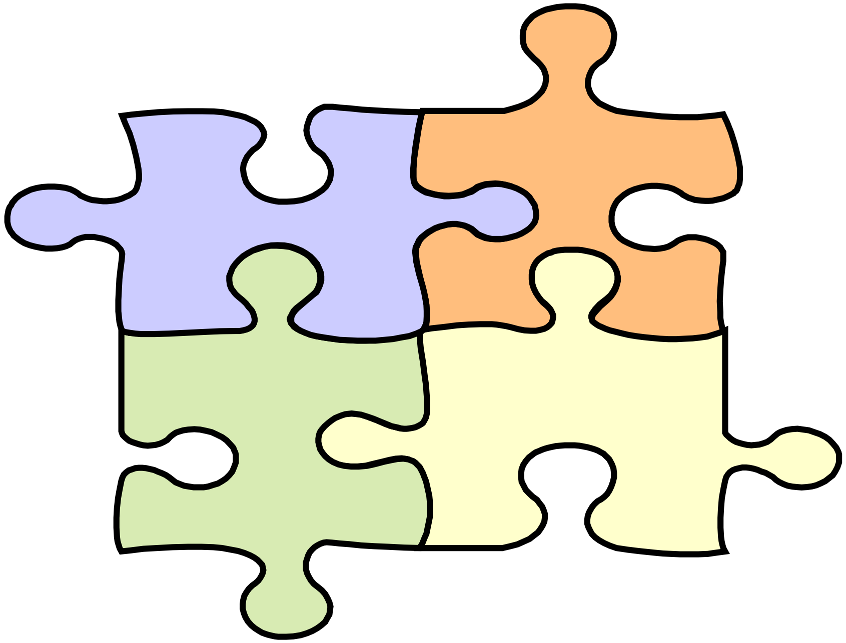
TOP 5 REPORTED INDUSTRIES (PAST 30 DAYS)

- EDUCATION
- GOVERNMENT: FEDERAL
- ENERGY/UTILITIES
- MANUFACTURING
- HIGH-TECH

Energy/Utilities
Series 1 : 0.5600660007451697

The "FireEye Cyber Threat Map" is based on a subset of real attack data, which is optimized for better visual presentation. Customer information has been removed for privacy

What security/safety measures (controls) are available, which should be used and **when** and **how** to implement them?



InfoSec fundamental concepts

- **Security** is a “measure” of **dependability** (quality of a system that allows us to trust, in a justified way, in its service) against **faults** affecting integrity, confidentiality and availability (!?)
- Security is not safety…
  but security contributes to safety

InfoSec fundamental concepts

- Terms and definitions (ISO/IEC 27000)
  - Resource
    - Any good or asset that **has value** to the organization
  - Information Security Event
    - Occurrence in a system, service or network, of an **identifiable state** which shows:
      - A possible **violation of security policy**;
      - A **failure of a defense**; or
      - A previously unknown situation with security relevance
  - Security Incident
    - Occurrence of one or more unexpected or unwanted security events, which have a **significant probability of compromising the operation of the organization** and threaten the information security.

(Bosworth, 2002)

InfoSec fundamental concepts

- Terms and definitions (ISO/IEC 27000)
  - Controls
    - ‘*means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature. Control is also used as a synonym for safeguard or countermeasure*’
  - Risk
    - ‘*Effect of uncertainty on objectives*’
      …‘*An effect is a deviation from the expected — positive or negative*’
      … ‘*Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood*’
      …

(ISO 27000, 2012)

InfoSec fundamental concepts

- **Security objectives** – preservation of certain information properties (or attributes) :
  - C **Confidentiality**
    - Restricted access to legitimate users
  - I **Integrity**
    - Content is not modified unexpectedly
  - A **Availability**
    - Accessible when needed
  - Authenticity
    - Unambiguous identification of the **responsible**
  - Utility
    - It serves the **purpose** for which it was created
  - Possession
    - Sole control by the **holder**

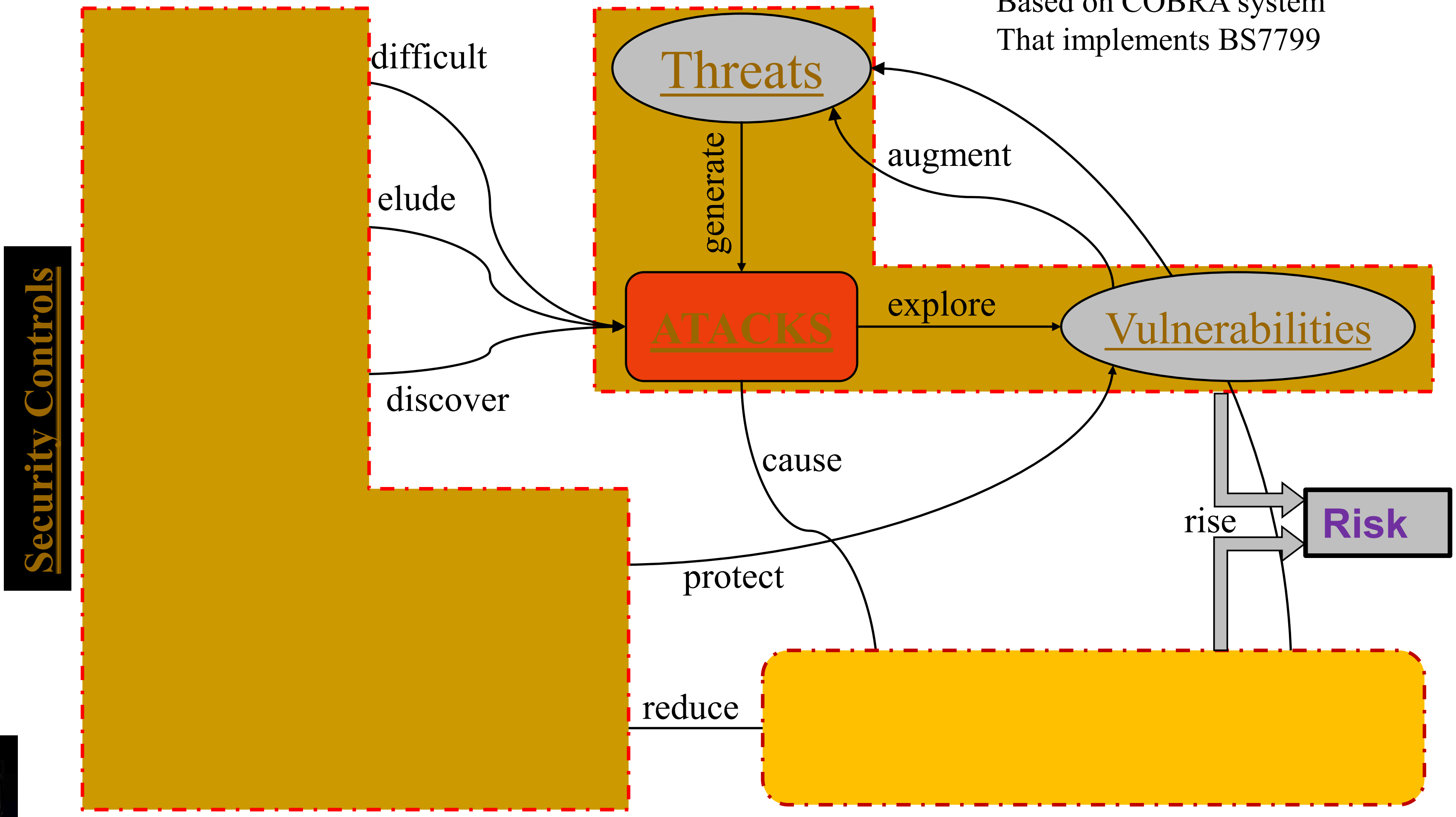
Integrity

Availability?!

Availability

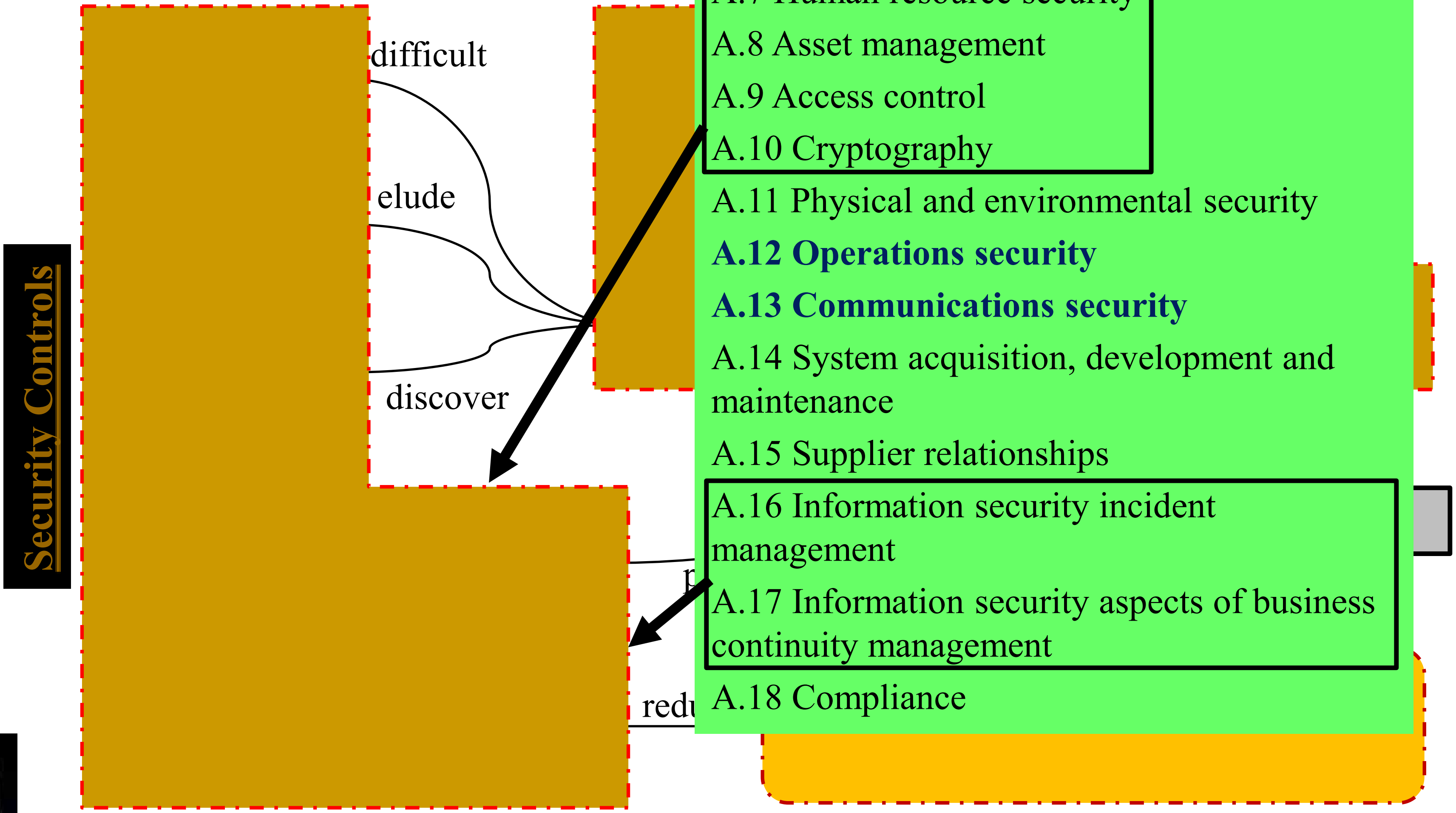
Confidentiality?!

InfoSec Model



Based on COBRA system
That implements BS7799

InfoSec Model



A.5 Information security policies

A.6 Organization of information security

A.7 Human resource security

A.8 Asset management

A.9 Access control

A.10 Cryptography

A.11 Physical and environmental security

A.12 Operations security

A.13 Communications security

A.14 System acquisition, development and maintenance

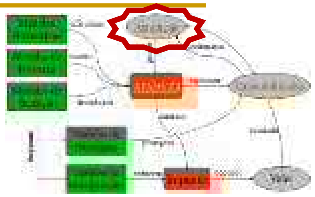
A.15 Supplier relationships

A.16 Information security incident management

A.17 Information security aspects of business continuity management

A.18 Compliance

Threat Landscape



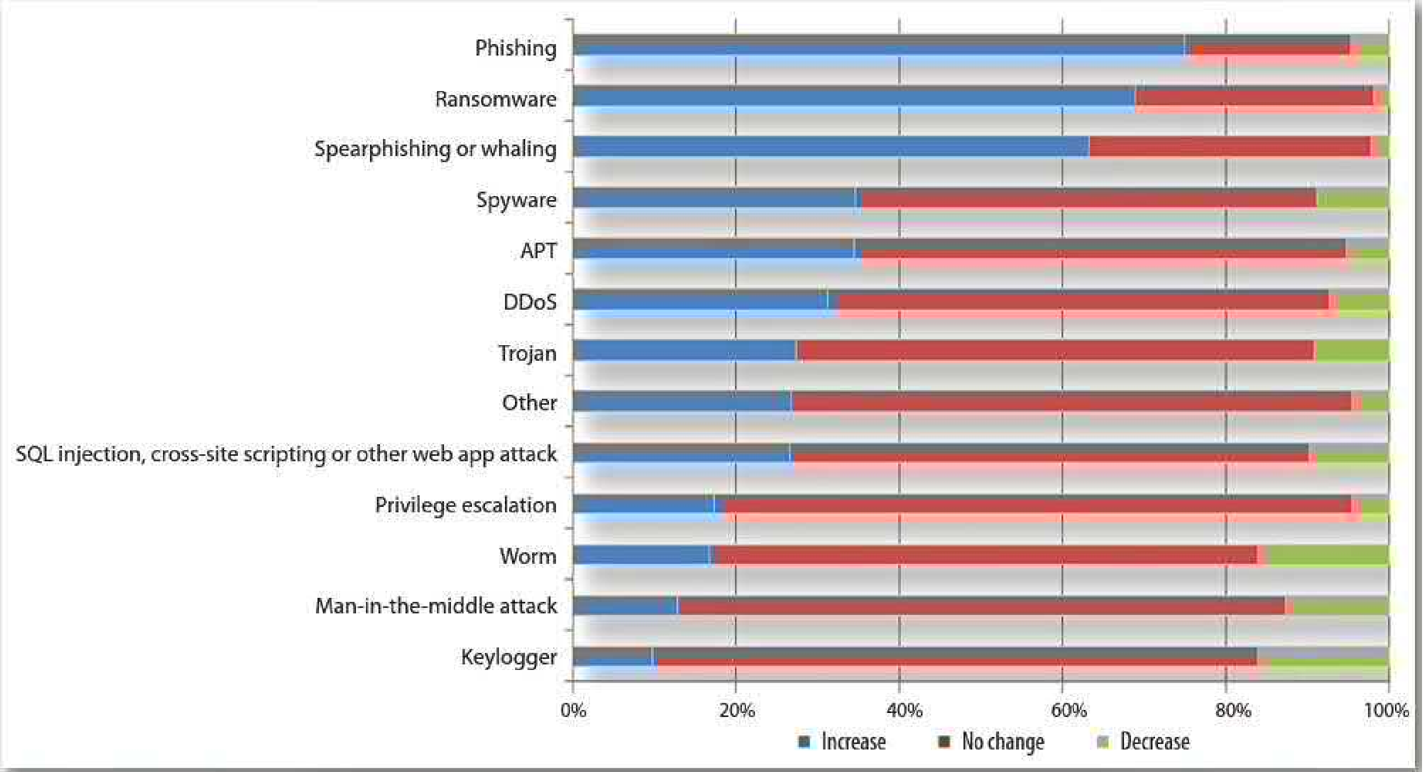
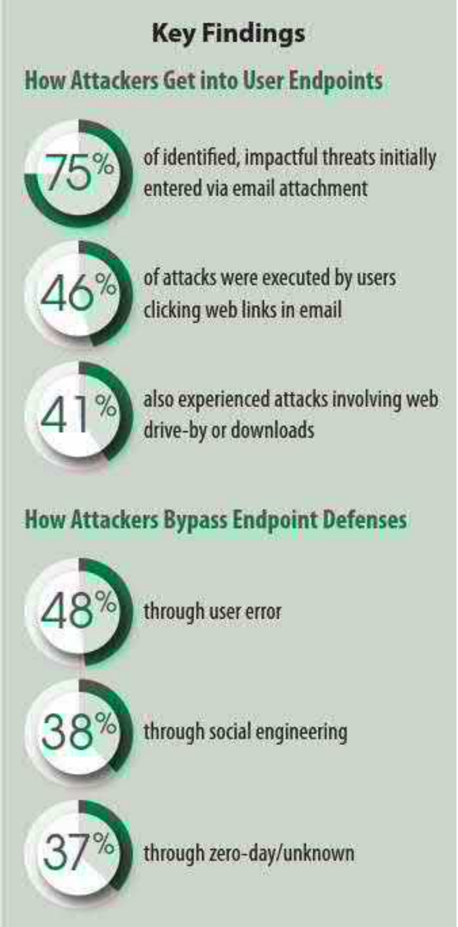


Figure 5. Phishing, Ransomware, Spearphishing Most on the Rise



Key Findings

How Attackers Get into User Endpoints

75% of identified, impactful threats initially entered via email attachment

46% of attacks were executed by users clicking web links in email

41% also experienced attacks involving web drive-by or downloads

How Attackers Bypass Endpoint Defenses

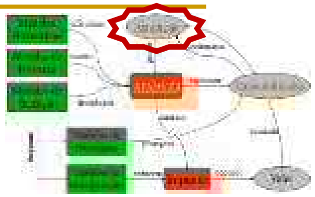
48% through user error

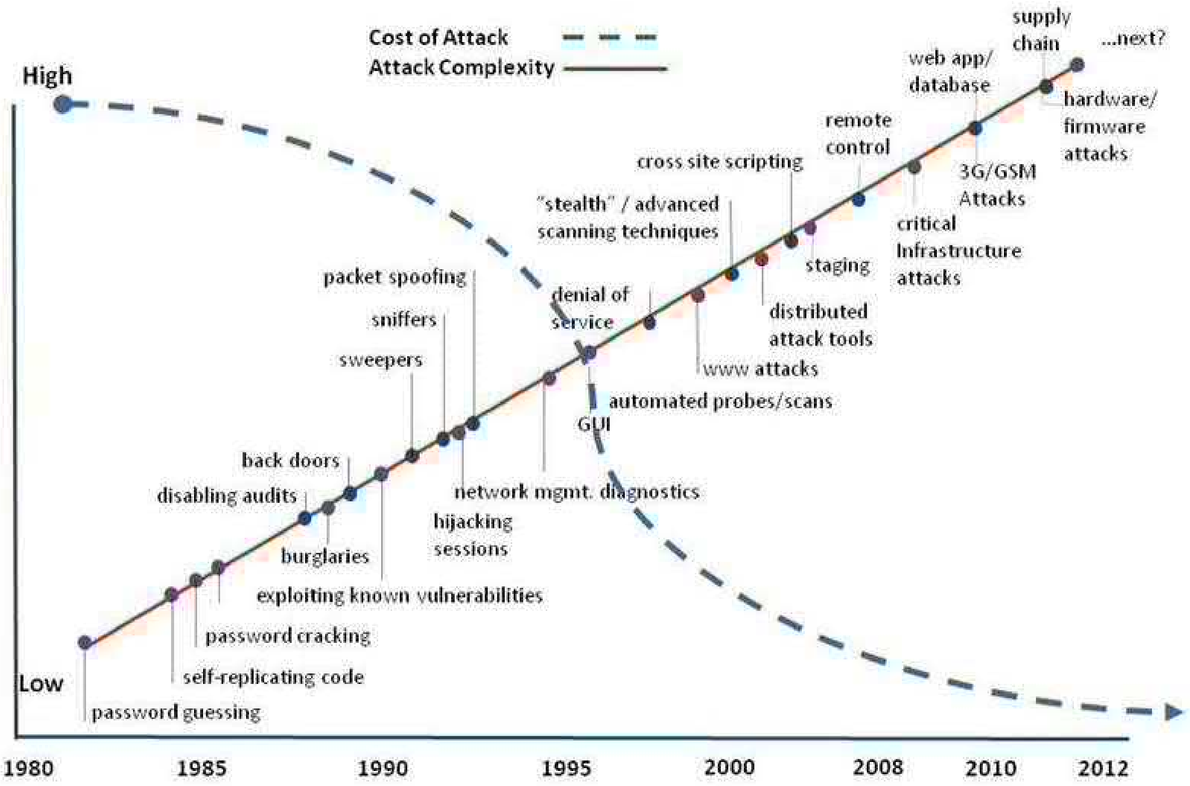
38% through social engineering

37% through zero-day/unknown

Exploits at the Endpoint: SANS 2016 Threat Landscape Survey

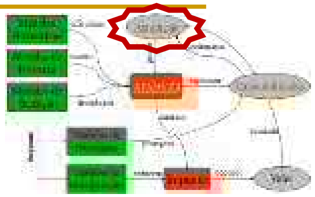
Threat Landscape





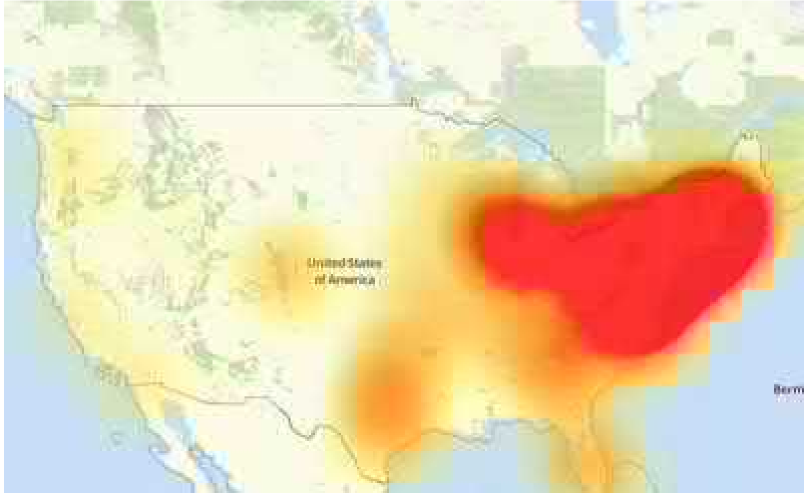
Fonte: *infosecurityinc.net/...-/Consult-Cyber-1Cyber-Threats-Diminishing-Attack-Costs-Increasing-Complexity4.jpg*

Threat Landscape



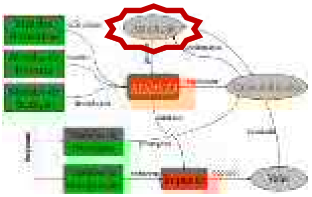
Denial-of-service attacks are shutting down major websites across the internet

- Starting at **11:10 UTC on October 21th-Friday 2016** we began monitoring and mitigating a DDoS attack against our Dyn Managed DNS infrastructure. Some customers may experience increased DNS query latency and delayed zone propagation during this time. Updates will be posted as information becomes available.
- …
- **The Department of Homeland Security is reportedly investigating the incidents**.
- Several other websites were shut down as an apparent result of the attack. Among those appeared to be Reddit, Airbnb, Tumblr, Amazon, and The New York Times, although the final list of those affected seems to be much longer.
- …
- Update October 21st, 9:49AM ET: In another update, Dyn says the issues have been resolved.
- Update October 21st, 1:02PM ET: Dyn now writes it is once again under attack.
- Update October 21st, 4:28PM ET: Dyn reportedly hit by a third DDoS attack.



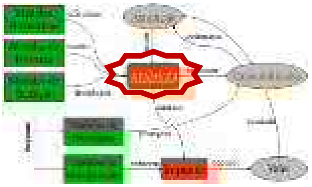
SOURCE: Dyn

Threats

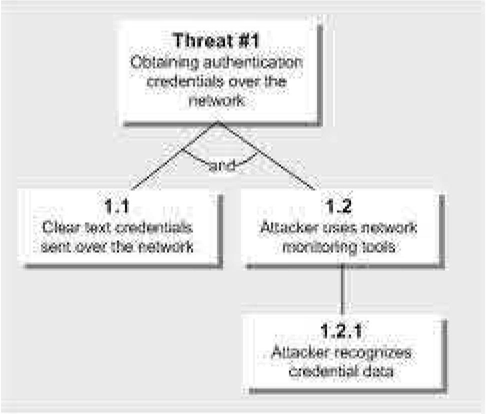


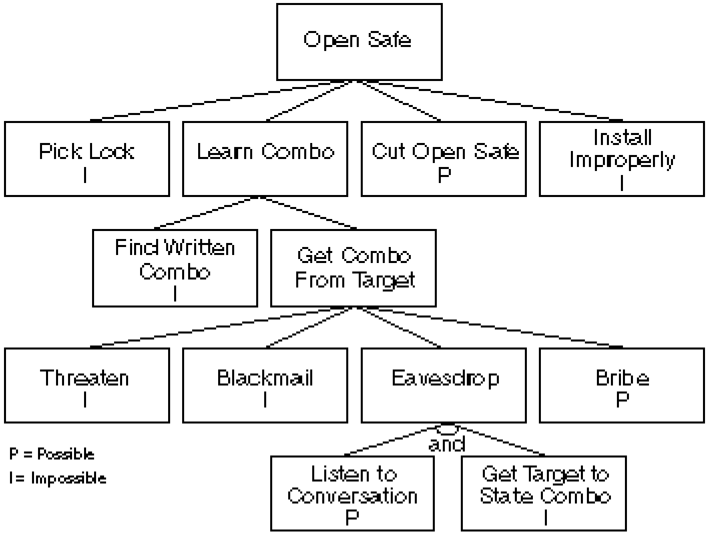
- What threats impend on (critical) resources?
  - Availability (and Utility) – **Interruption**
    - Destruction, damage, or contamination
    - Refusal or delay in access
    - Dislocation or obscuration
  - Integrity (and Authenticity) – **Modification / Fabrication**
    - Insert or production of false data
    - Replacement, removal, separation or reorganization
    - Representation or encoding
    - Repudiation
  - Confidentiality (and Possession) – **Interception**
    - Illicit copy, observation, monitoring, or inference
    - Unwanted transfer of control or custody
    - Disclosure (in particular by legitimate users, by negligence or fraud)

Attacks



- An attack (or attacker) appears when there is:
  - ***Method***: knowledge, skills and tools to exploit vulnerabilities
  - ***Opportunity***: time and conditions to access
  - ***Motive***: a reason to carry out the attack
- A well known analysis model: Tree Modeling Moore, AP (2001)
  Tool: AttackTree++


Threat #1
Obtaining authentication credentials over the network
and
1.1
Clear text credentials sent over the network
1.2
Attacker uses network monitoring tools
1.2.1
Attacker recognizes credential data



Open Safe

Pick Lock I

Learn Combo

Cut Open Safe P

Install Improperly I

Find Written Combo I

Get Combo From Target

Threaten I

Blackmail I

Eavesdrop

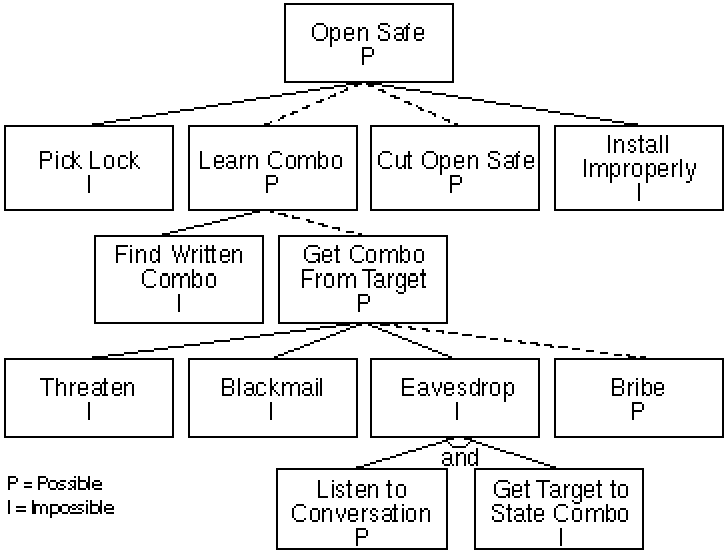
Bribe P

and

Listen to Conversation P

Get Target to State Combo I

P = Possible
I = Impossible



Open Safe P

Pick Lock I

Learn Combo P

Cut Open Safe P

Install Improperly I

Find Written Combo I

Get Combo From Target P

Threaten I

Blackmail I

Eavesdrop I

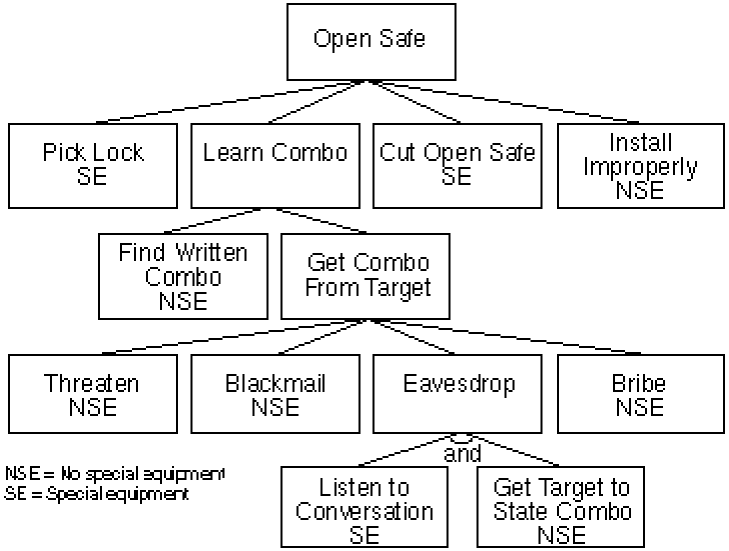
Bribe P

and

Listen to Conversation P

Get Target to State Combo I

P = Possible
I = Impossible



Open Safe

Pick Lock SE

Learn Combo

Cut Open Safe SE

Install Improperly NSE

Find Written Combo NSE

Get Combo From Target

Threaten NSE

Blackmail NSE

Eavesdrop

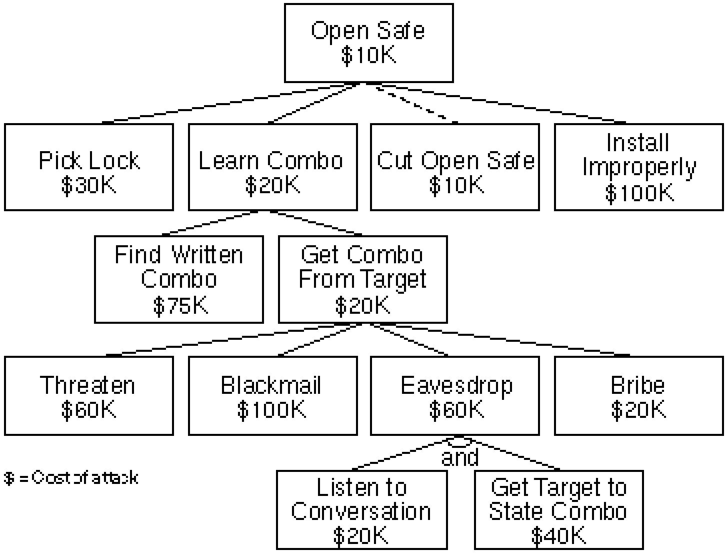
Bribe NSE

and

Listen to Conversation SE

Get Target to State Combo NSE

NSE = No special equipment
SE = Special equipment



Open Safe $10K

Pick Lock $30K

Learn Combo $20K

Cut Open Safe $10K

Install Improperly $100K

Find Written Combo $75K

Get Combo From Target $20K

Threaten $60K

Blackmail $100K

Eavesdrop $60K

Bribe $20K

and

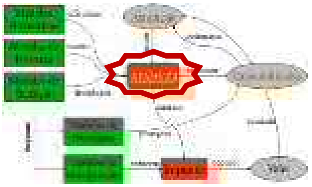
Listen to Conversation $20K

Get Target to State Combo $40K

$ = Cost of attack

https://www.schneier.com/paper-attacktrees-ddj-ft.html

Well known attacks



- Denial of Service (DoS/DDoS)
- Spam
- Mail Bombing
- Pharming

External (very difficult to avoid)

- Social Engineering
- Hoaxes and Phishing

External (targeted to users)

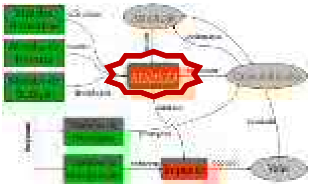
- Malicious code (virus; Trojans; worms; ram…)
- Back Doors

Internal or external (affect machines)

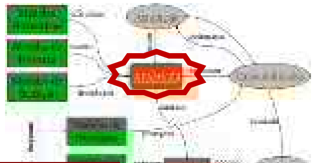
- Password Crack
- Man-in-the-Middle (or Hijacking)
- Spoofing
- Sniffers

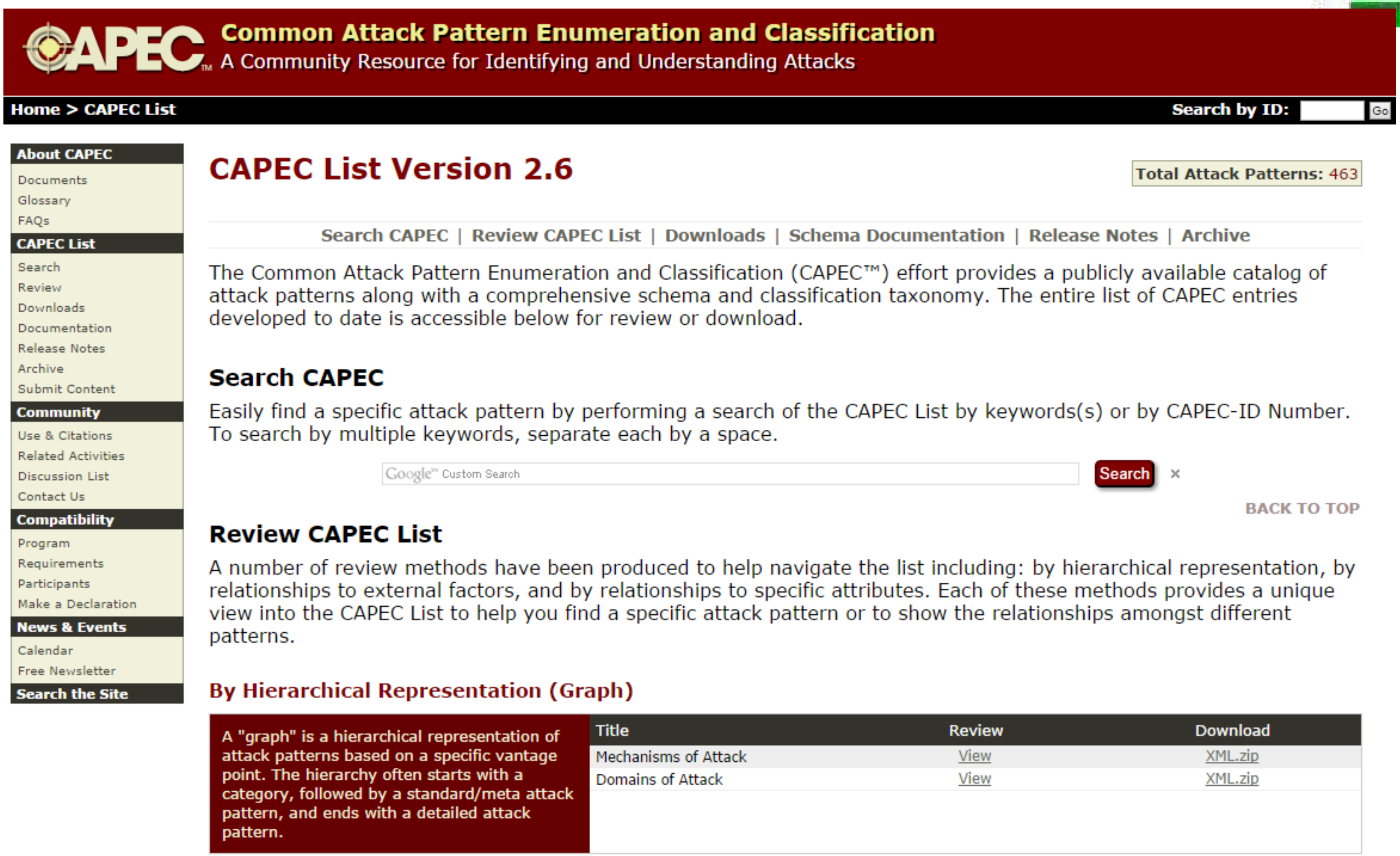
Internal (require access to LAN)

Well known attacks



- Harder to recognize attacks:
  - Human error
  - Failures in the and the analysis and design of Information Systems
  - Violation of safe places by "trustable people"
  - Intrusions
  - Natural disasters
- Some important efforts to "normalize" the description of attacks:
  - http://capec.mitre.org/data/index.html





Common Attack Pattern Enumeration and Classification

A Community Resource for Identifying and Understanding Attacks

CAPEC List Version 2.6

Total Attack Patterns: 463

Search CAPEC | Review CAPEC List | Downloads | Schema Documentation | Release Notes | Archive

The Common Attack Pattern Enumeration and Classification (CAPEC™) effort provides a publicly available catalog of attack patterns along with a comprehensive schema and classification taxonomy. The entire list of CAPEC entries developed to date is accessible below for review or download.

Search CAPEC

Easily find a specific attack pattern by performing a search of the CAPEC List by keywords(s) or by CAPEC-ID Number. To search by multiple keywords, separate each by a space.

Review CAPEC List

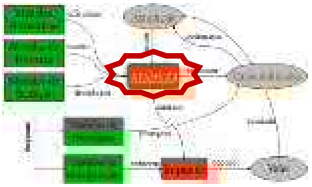
A number of review methods have been produced to help navigate the list including: by hierarchical representation, by relationships to external factors, and by relationships to specific attributes. Each of these methods provides a unique view into the CAPEC List to help you find a specific attack pattern or to show the relationships amongst different patterns.

By Hierarchical Representation (Graph)

A "graph" is a hierarchical representation of attack patterns based on a specific vantage point. The hierarchy often starts with a category, followed by a standard/meta attack pattern, and ends with a detailed attack pattern.

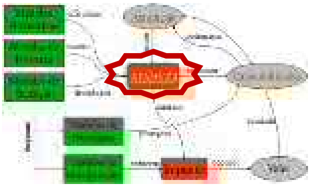
Title	Review	Download
Mechanisms of Attack	View	XML.zip
Domains of Attack	View	XML.zip

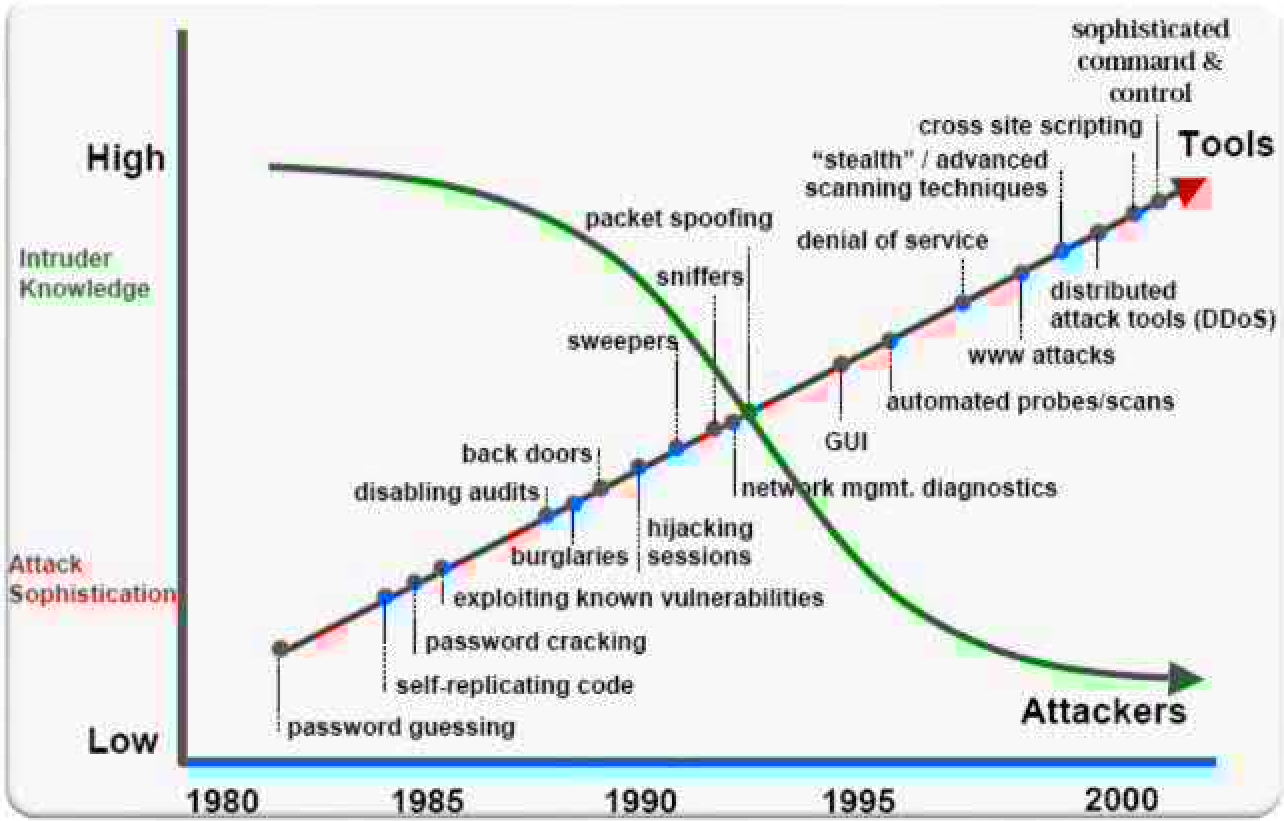
Attackers



- Concerning Information Systems, who are the attackers?
  - Amateur: driven by curiosity and the prospect of social role
  - *Crackers* and *Hackers*: often students, with high technical expertise; typically they want to take over computers, for mere pleasure or for any economic advantage; often organized in Internet communities
  - Criminals: there is some evidence that organized crime and international groups have been increasing its involvement in computer crime (the profit opportunities are increasing)
  - Terrorists: increasingly evident and at various levels
    - Targeting ISs as critical infra-structures
    - Using SIs as a mean of propaganda
    - Using SIs as a mean of attack

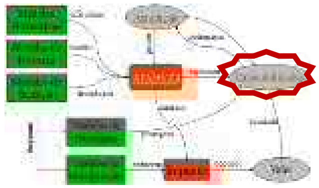
Attacks and attackers





Fonte: H.F. Lipson, CERT Coordination Center, CMU/DEI-2002-SR-009

Vulnerabilities



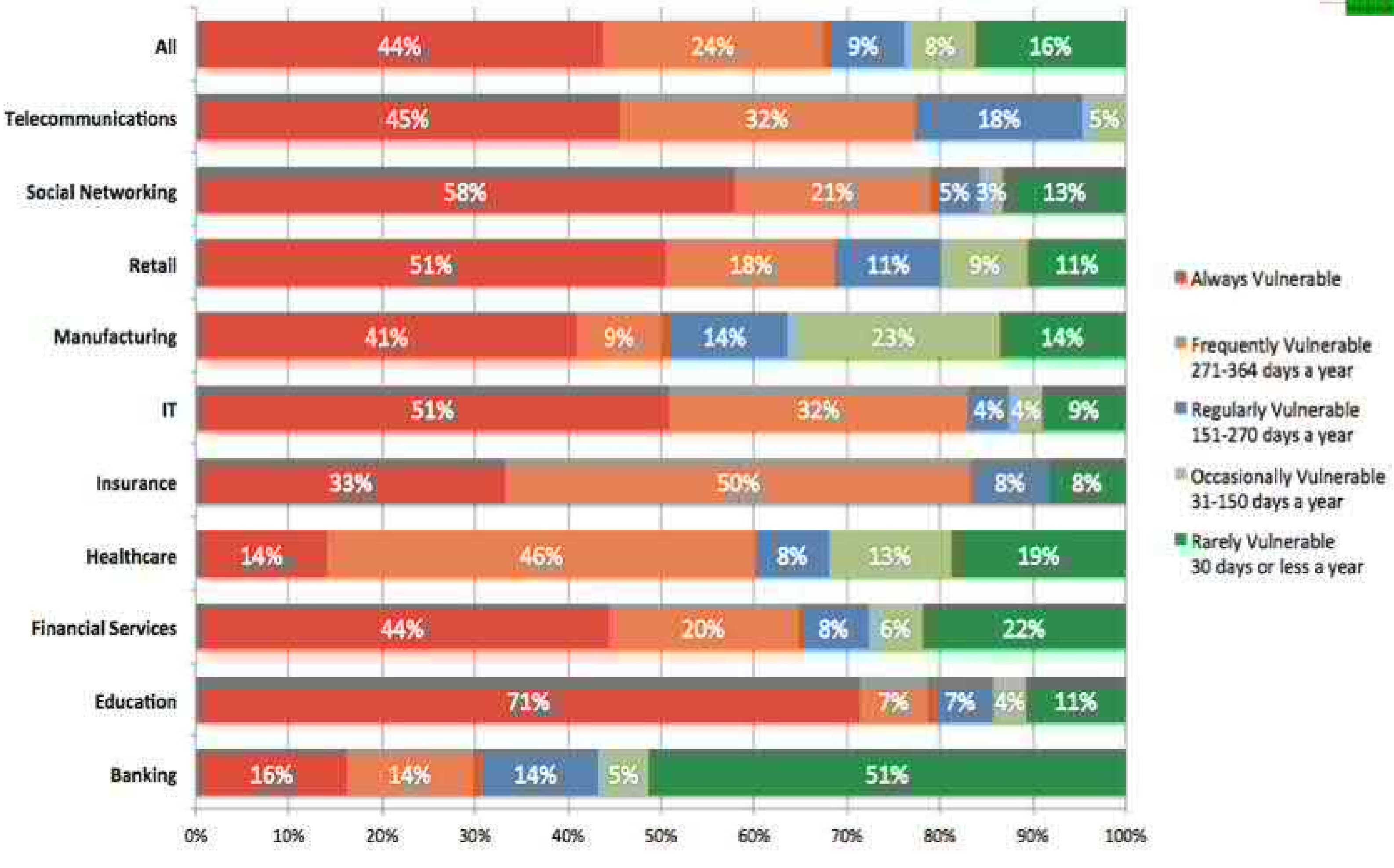
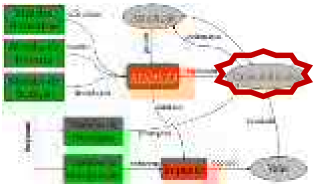


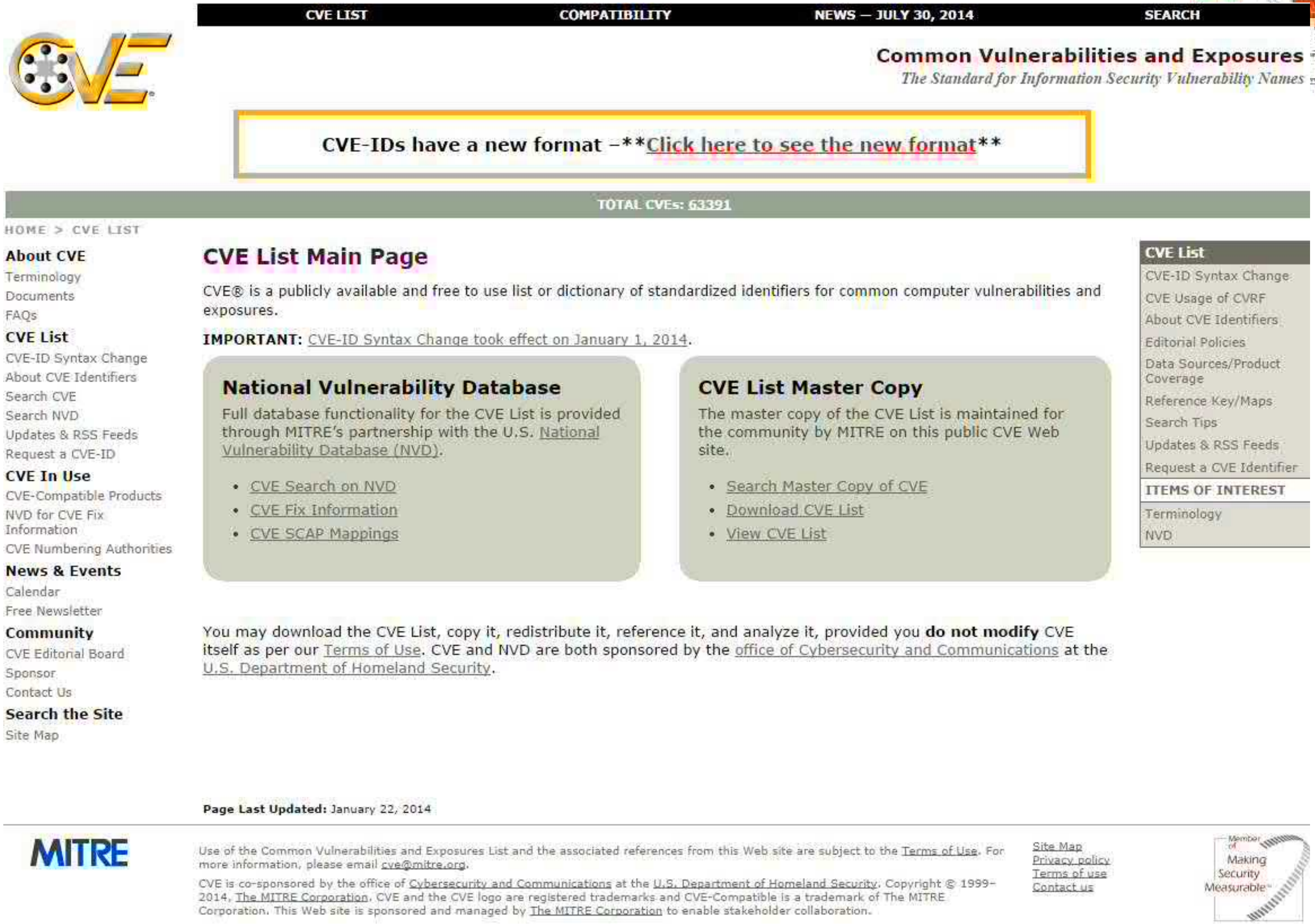
Figure 2. Window of Exposure by Industry (2010)

Source: http://jeremiahgrossman.blogspot.pt/2011/03/11th-whitehat-website-security.html

Vulnerabilities



- Vulnerabilities origin
  - An IS is generally made of hardware (execute simple instructions and transactions), software (create operations as logical sequences of instructions and transactions) and data (information)
  - Computer Systems
    - Complexity, degree of autonomy, miniaturization and dematerialization, ubiquity, interconnect, are factors that contribute to increased vulnerability
    - Vulnerabilities detection/management support
      - Tools like NESSUS, SAINT, Grabber,…
      - Resources like CVS, NIST, SANS



Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

CVE-IDs have a new format –**Click here to see the new format**

TOTAL CVEs: 63391

CVE List Main Page

CVE® is a publicly available and free to use list or dictionary of standardized identifiers for common computer vulnerabilities and exposures.

IMPORTANT: CVE-ID Syntax Change took effect on January 1, 2014.

National Vulnerability Database

Full database functionality for the CVE List is provided through MITRE's partnership with the U.S. National Vulnerability Database (NVD).

- CVE Search on NVD
- CVE Fix Information
- CVE SCAP Mappings

CVE List Master Copy

The master copy of the CVE List is maintained for the community by MITRE on this public CVE Web site.

- Search Master Copy of CVE
- Download CVE List
- View CVE List

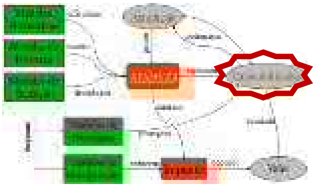
You may download the CVE List, copy it, redistribute it, reference it, and analyze it, provided you **do not modify** CVE itself as per our Terms of Use. CVE and NVD are both sponsored by the office of Cybersecurity and Communications at the U.S. Department of Homeland Security.

Page Last Updated: January 22, 2014

Use of the Common Vulnerabilities and Exposures List and the associated references from this Web site are subject to the Terms of Use. For more information, please email cve@mitre.org.

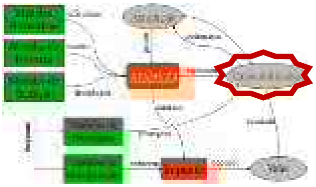
CVE is co-sponsored by the office of Cybersecurity and Communications at the U.S. Department of Homeland Security. Copyright © 1999–2014, The MITRE Corporation. CVE and the CVE logo are registered trademarks and CVE-Compatible is a trademark of The MITRE Corporation. This Web site is sponsored and managed by The MITRE Corporation to enable stakeholder collaboration.

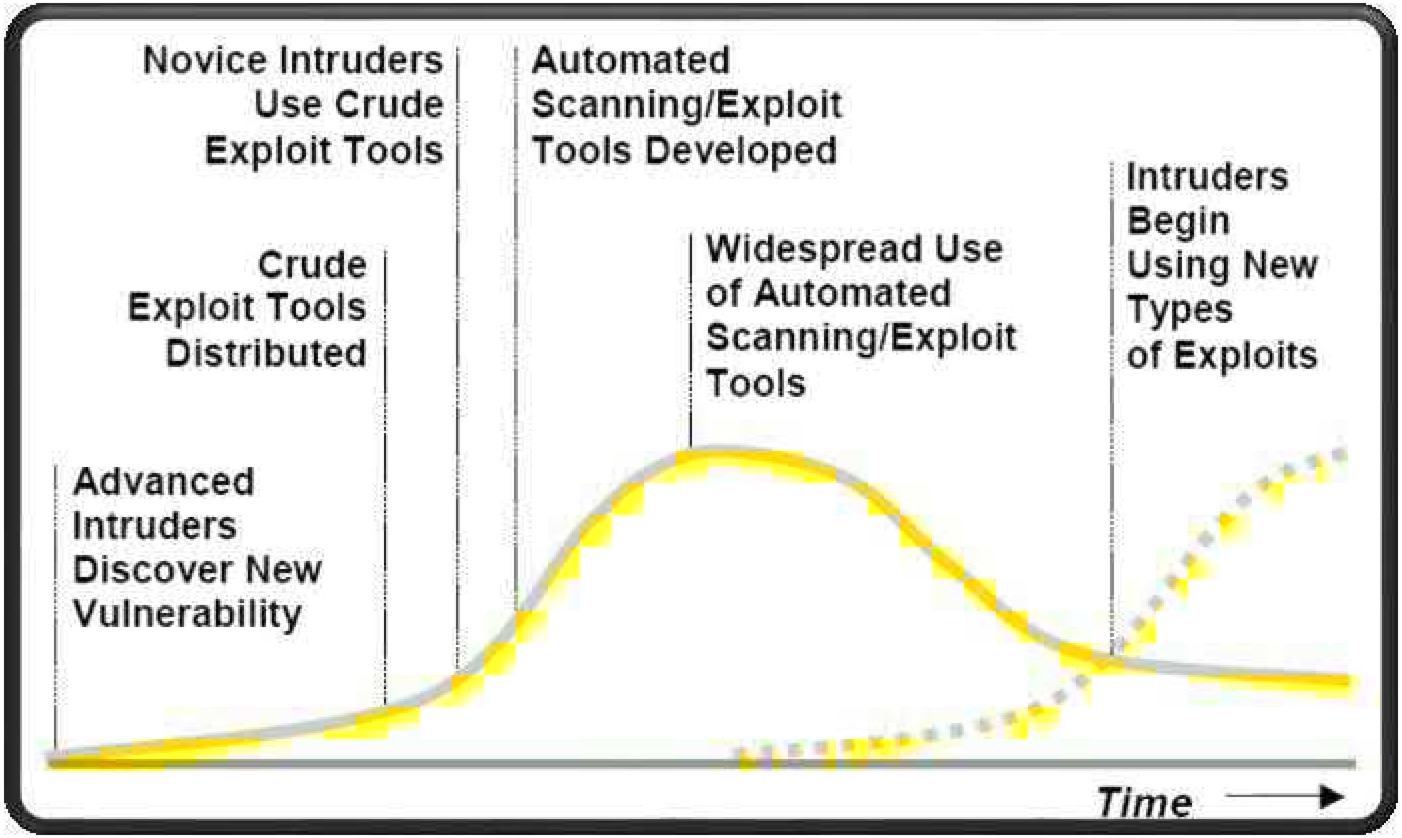
Vulnerabilities



- Vulnerabilities origin (cont)
  - Inadequate user behaviors
- Vulnerabilities recognition can derive from reflection on what can go wrong
  - Interruptible
  - Modifiable
  - “Manufacturable”
  - “Interceptable”
  - Incomplete (incomplete or misunderstood specifications)
  - …

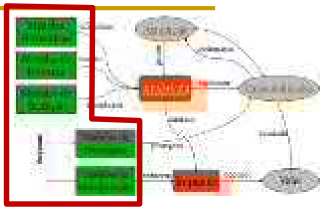
Cycle of vulnerabilities exploitation




Novice Intruders Use Crude Exploit Tools
Automated Scanning/Exploit Tools Developed
Intruders Begin Using New Types of Exploits
Crude Exploit Tools Distributed
Widespread Use of Automated Scanning/Exploit Tools
Advanced Intruders Discover New Vulnerability
Time

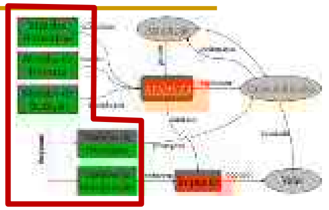
Fonte: H.F. Lipson, CERT Coordination Center, CMU/DEI-2002-SR-009

Security Controls



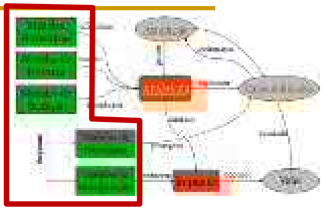
- Security properties driven classification
  - CIA oriented
    - User and organization policies
    - Access Control
      - Users; Networks; Applications; Physical
    - Antivirus and antimalware
    - Intrusion Detection Systems (IDS)
  - CI oriented
    - Cryptography, Digital Signatures; Digital Certificates
  - IA oriented
    - Backups
  - A oriented
    - Disaster Recovery
    - Redundancy (data and services)
  - I oriented
    - Integrity verifiers

Security Controls



- **Policies**, **procedures**, **guides**, good practices, **hardware and software devices** or even organizational initiatives aiming to manage risk …
- Organizational oriented
  - **Resources** are main targets; objectives: **what to assure**
- Security "mechanisms"
  - Technologies or actions to implement security policies
  - Standards define mainly security mechanisms:
    - http://www.27000.org/index.htm
    - http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-12.pdf
    - http://www.itu.int/rec/T-REC-X.800-199103-I/en

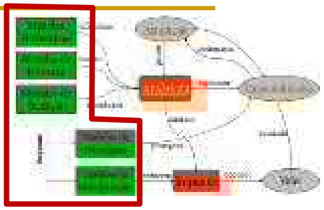
Security Controls



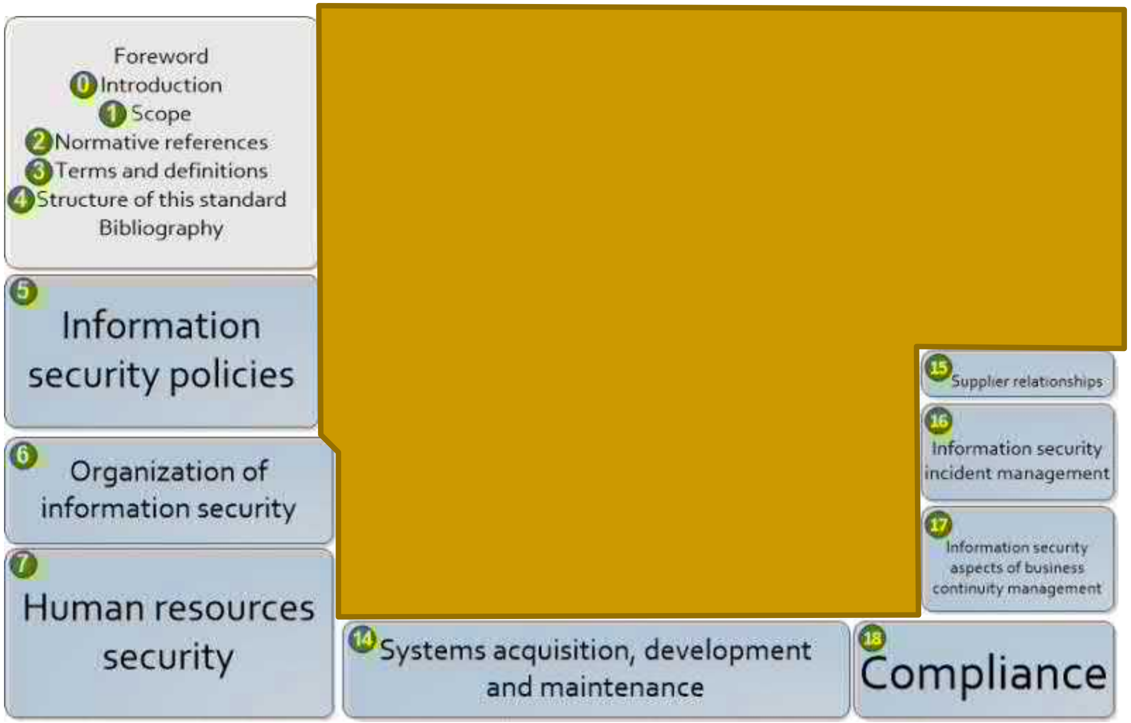
- Policies or procedures in use:
  - Password management politics – 74%
  - Inappropriate use politics – 71%
  - Education and awareness politics – 67%
  - Internet access monitoring – 65%
  - Corporate security politics – 62%
  - Risk Management practices – ≈ 55%
  - ...
  - Employing ex-hackers – 14%

Source: 2005 E-Crime Watch Survey – CSO magazine

Security Controls



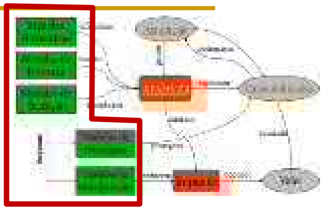
- ISO/IEC **27002:2013** (Code of Practice for InfoSec Management)
  - 14 classes (clauses) – sections 5 to 18
  - 35 control objectives
  - 114 security controls
  - About one half are technological
  - About one half are organizational or managerial



Foreword
0 Introduction
1 Scope
2 Normative references
3 Terms and definitions
4 Structure of this standard
Bibliography
5 Information security policies
6 Organization of information security
7 Human resources security
14 Systems acquisition, development and maintenance
15 Supplier relationships
16 Information security incident management
17 Information security aspects of business continuity management
18 Compliance

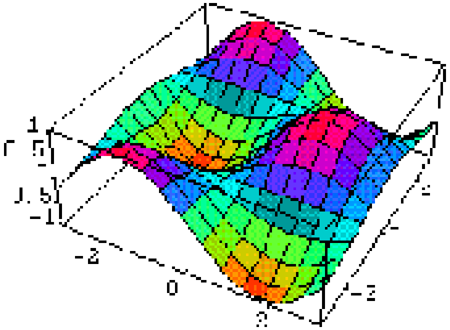
http://www.iso27001security.com/html/27002.html

Security Controls



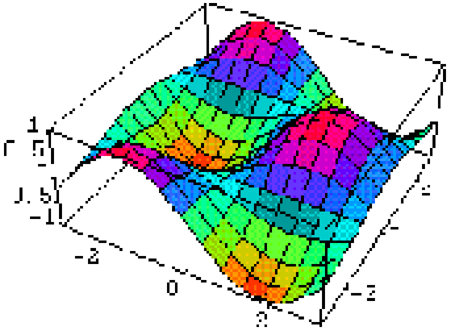
- Most used security technologies :
  - Antivirus – 97%
  - Antispam – 95%
  - *Firewalls* – 94%
  - Virtual Private Network (VPN) – 85%
  - Antispyware/adware – 80%
  - Cipher (data in transit) – 71% (↑)
  - Intrusion Detection (IDS) – 69%
  - Vulnerability scanners and patch – 65%
  - Web/URL filtering – 61%
  - Application level Firewalls – 53% (↑)
  - ...
  - PKI – 36%
  - Smartcards and other OTP devices – 36%
  - Integrated NAC solutions – 34% (↑)
  - Virtualization specific tools – 29%
  - Wireless tools – 27% (↓)
  - Biometrics – 23%

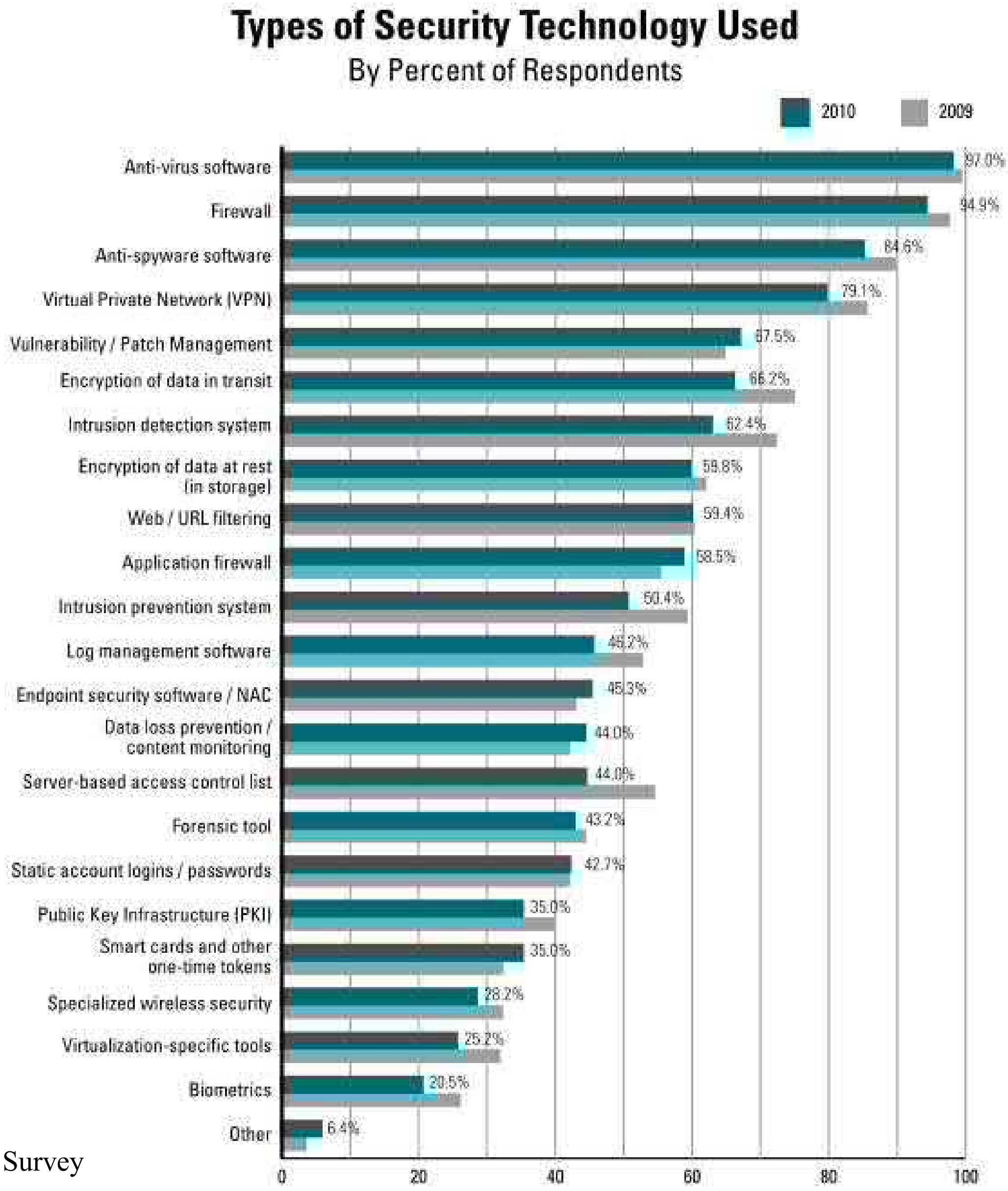
Eficiência?!

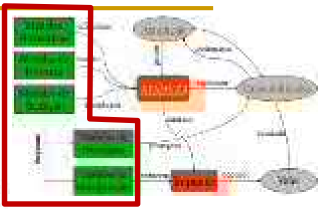


Source: CSI Computer Crime & Security Survey, 2008

Efficiency?!

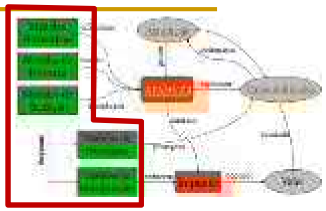






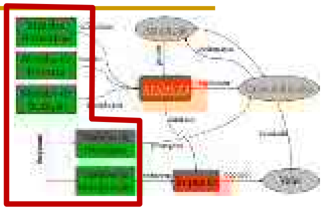
2010/2011 CSI Computer Crime and Security Survey

Controls' efficiency



- A *metagoal*
  - Awareness of the need to use - the establishment of a "safety culture"
  - Guarantee of service
  - Overlap effect of different controls
  - Periodic review
- **Principle of efficiency**: to ensure that controls produce results, they must be appropriate and used properly
- **Principle of adequate protection**: resources must be protected to a degree consistent with its **value**

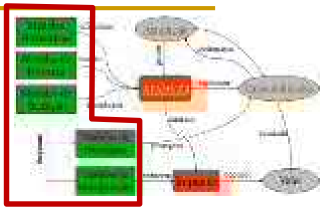
Controls' efficiency



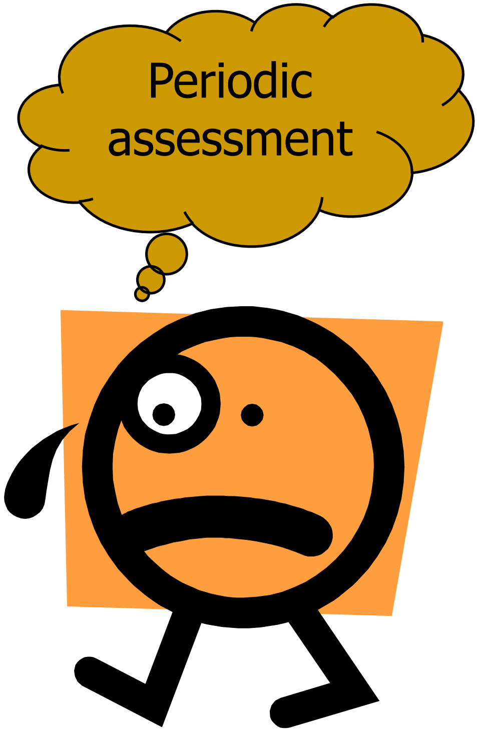
- Techniques used to evaluate efficiency
  - ❑ Internal auditing (82%)
  - ❑ Penetration test (66%)
  - ❑ Automatic tools (66%)
  - ❑ External auditing (62%)
  - ❑ Monitoring software:
    - e-mails (61%)
    - Web activity (58%)

What exactly is being measured?

Controls’ effectiveness

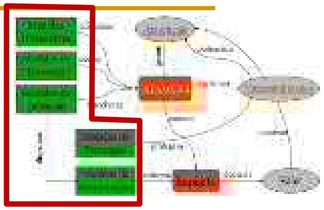


- More effective technologies:
  - ❑ *Firewalls* – 68%
  - ❑ Anti-Vírus – 66%
  - ❑ Cipher – 58%
  - ❑ Two-phase authentication – 56%
  - ❑ Intrusion Detection (IDS) – 50%
  - ❑ Physical Security – 49%
  - ❑ Network traffic monitoring – 46%
  - ❑ Spyware/Adware – 43%
  - ❑ ...
  - ❑ Manual patches – 26%



Source: 2005 E-Crime Watch Survey – CSO magazine

About metrics



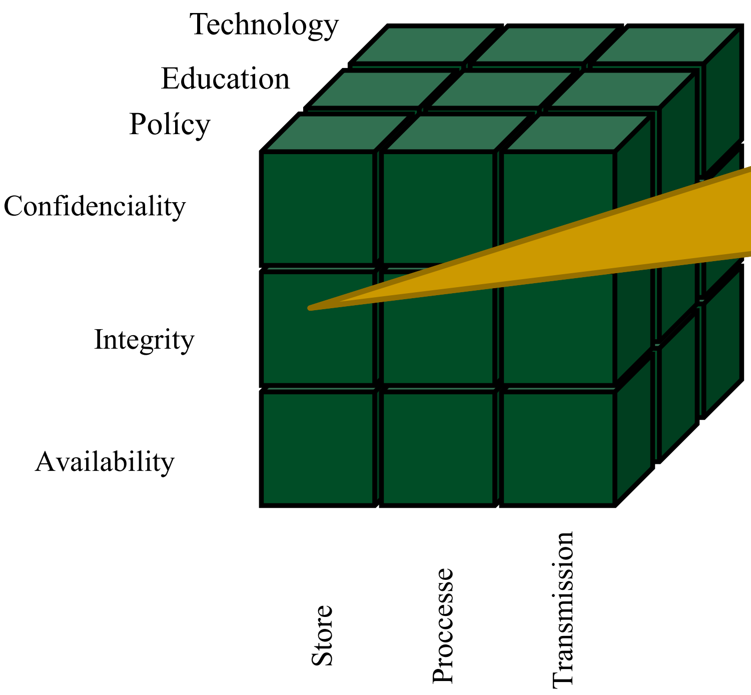
- NIST SP800-55 (*Security Metrics Guide for Information Technology Systems*) defines three metric types:
  - Implementation metrics
  - Efficacy/Efficiency metrics
  - Impact metrics

…

- A lot of (very hard) work to do ☹

InfoSec Model

CNSS Model (*McCumber Cube*) - *Committee on National Security Systems,* a NSA group (NSTISSI-4011)



Involves the need for technology to protect the integrity of the stored data:

Exemples: HIDS, integrity checker software

InfoSec Model

- The previous approaches are centered on effects, but there are other possible perspectives (e.g., centered on environmental factors):

  "*The absence of threats that can affect our expectations about information systems equivalently protected in equivalent environments*."

(Canal, 2005)

About Models

“All Models Are Wrong But Some Are Useful”

Author: George Box

Regulatory Compliance

- Internacional
  - ISO/IEC 17799 / 27000
- USA
  - Federal Information Security Management Act (FISMA)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - NIST – Computer Division SP-800 family
  - Sarbanes–Oxley Act; Gramm–Leach–Bliley Act; COBIT
- Australia and the UK also have their own normalization bodies
- National
  - LPD (Law for Data Protection – “Lei 67/98”) which transcribe the EU Directive 95/46/CE
  - SEGNAC 1 and 4 published by GNS (QG of Centro Nacional de Cibersegurança)

27000 Standards’

InfoSec is a Management Process!

ISO/IEC 27000 overview & vocabulary	
ISO/IEC 27001 formal ISMS specificatio	
ISO/IEC 27002 infosec controls guidelin	
ISO/IEC 27003 implementation guidanc	
ISO/IEC 27004 infosec metrics	
ISO/IEC 27005 infosec risk management	ISO/IEC 27033 network security
ISO/IEC 27006 ISMS certification guide	ISO/IEC 27034 application security
ISO/IEC 27007 MS auditing guide	ISO/IEC 27035 incident management
ISO/IEC TR 27008 technical auditing	ISO/IEC 27037 digital evidence
ISO/IEC 27010 for inter-org comms	ISO 27799 ISO27k for healthcare industry
ISO/IEC 27011 ISO27k for telecomms	

http://www.iso27001security.com/

Regulatory Compliance

- Many regulations provide some kind of "***baseline security control***"
  - Ex: Payment Card Industry Data Security Standard (PCI DSS); NSA; Cisco;…
- But…
  - To what extent this set of controls is aligned with reality?
  - Once in compliance means compliance forever?

Security evaluation

- Example: *Common Criteria* (ISO/IEC 15408)

Level of Assessment	Characteristic
EAL7	Formal methodology for both project and test
EAL6	Semi-formal methodology for both project and test
EAL5	Methodologically projected, supported by a semi-formal test
EAL4	Methodologically designed, tested, verified and reviewed
EAL3	Methodologically tested and verified
EAL2	Structural test (module interconnection)
EAL1	Functional test

Qualitative

- Now we have a model. What’s next?
- We still need to understand better the security technology available and how to use it correctly…
- Long and hard way…

▶

“Management is the process of achieving objectives using a given set of resources”

in Whitman, Management of Information Security, p9

So…

Information Security is a business management activity

What to do next? (1)

- Study and understand the technological controls (hardware and software)
  - Computers, Operating Systems, applications, and networks
- Study and understand the controls related with the utilization and the environment - Security Administration
  - Security management; privacy, law and ethics
  - Psychology of risk
- Study and understand the controls based on cryptography

What to do next? (2)

- Proposed Guidelines for an ISMS (Information Security Management System)
  - BS 7799 and derivate (ISO/IEC 17799, ISO/IEC 27000, …)
  - Generally Accepted System/Information Security Principles (GASSP, GAISP after v3.0)
  - System Security Engineering CMM (SSE-CMM)
  - TCSEC/Orange Book
  - ITSEC (Common Criteria or ISO/IEC 15408)
  - GMITS
  - CobiT
  - IT Baseline Protection Manual
  - ITIL
  - …

InfoSec Management

- Performance evaluation is fundamental within InfoSec. A good metric for the InfoSec function should seek to answer questions as:
  - What is the efficiency of my security process?
  - Am I more secure than I was 1 year ago?
  - **What is my level of security compared to my peers?**
  - The level of investment (in InfoSec) is appropriate?
  - What are my options for managing the risk?

InfoSec Management

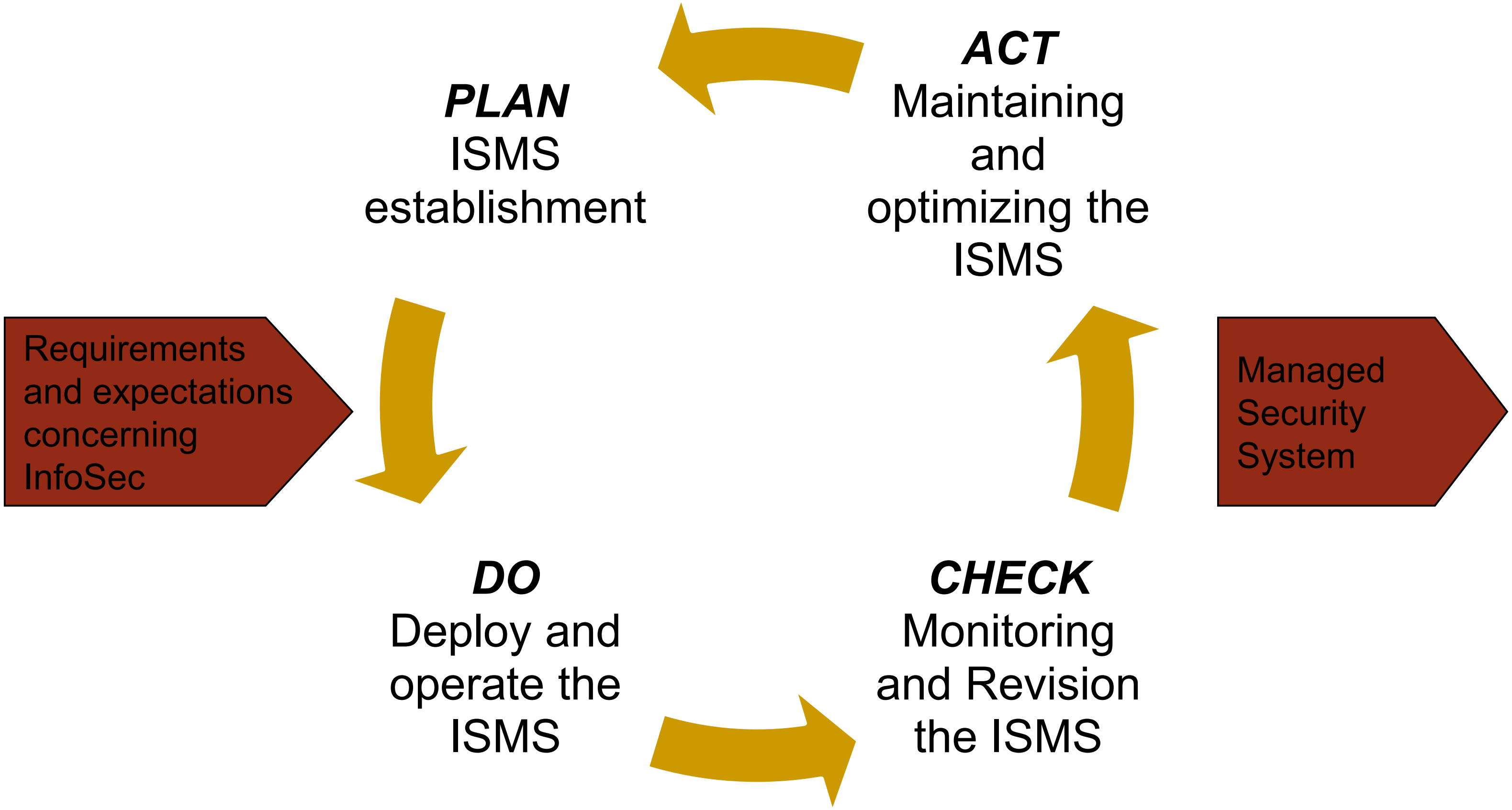
- General criteria for good metrics
  - **Scope**: the part of the system to be measured must be clearly identified
  - **Repeatable**: if the measurement is repeated by the same agent, the result shall be the same
  - **Repeatable**: If the measurement is made by another agent, the result should be the same
  - **Relevant**: to the decision making process
  - **Effective**: measurement should be obtained with an acceptable cost

Exercise

- Define an appropriate metric for the security control selected in your last exercise.
  - Does it provide any kind of logs?
  - Does it interact with other systems?
  - What do you really expect from it?
  - What others think about it?

InfoSec Management

- Based on the PDCA process model (ISO/IEC 27000/1 – establishment and management of an ISMS)



PLAN
ISMS establishment
ACT
Maintaining and optimizing the ISMS
Requirements and expectations concerning InfoSec
Managed Security System
_DO_
Deploy and operate the ISMS
CHECK
Monitoring and Revision the ISMS

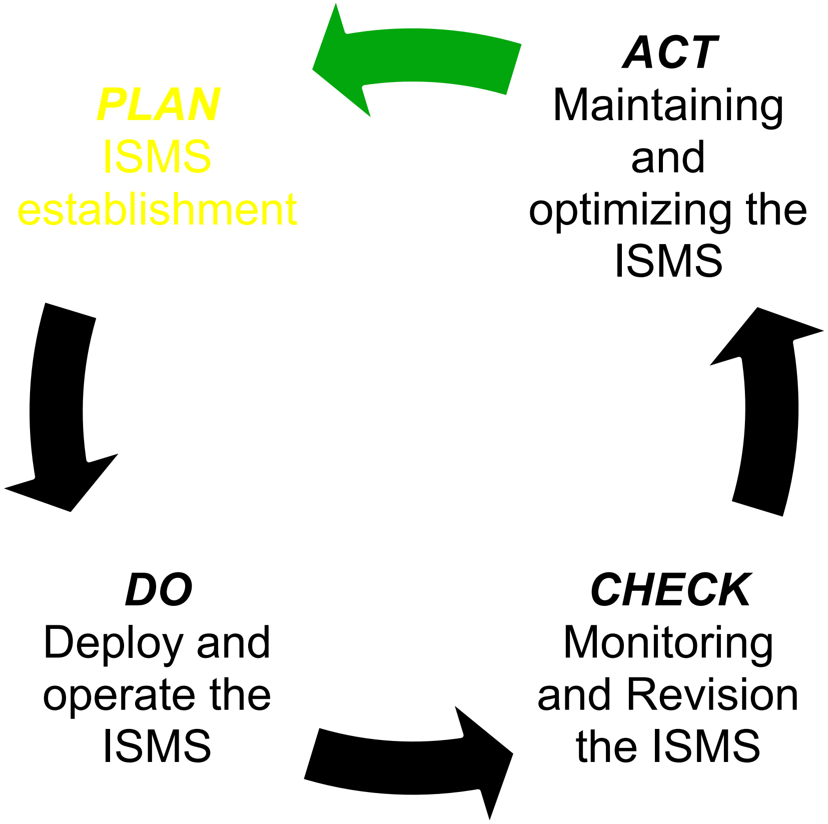
InfoSec Management

- PDCA – Plan; Do; Check; Act
  - **Plan**: Set out objectives, policies, targets and relevant measures to control risk (Threats and Risk Analysis)
  - **Do**: Design and implementation of controls
  - **Check**: Verification and evaluation against security policy
  - **Act**: Make the necessary corrections

[Cavalli, 2004 #50]

InfoSec Management

- Risk management
  - Analysis, valuation of risk and risk mitigation
  - Vulnerabilities, threats and impact of attacks
- ISO/IEC 13335 (part 3 and 4) and 27005
- Security controls
  - Security Policy
  - Security properties
- ISO/IEC 17799, 27001 and 27002



PLAN
ISMS establishment

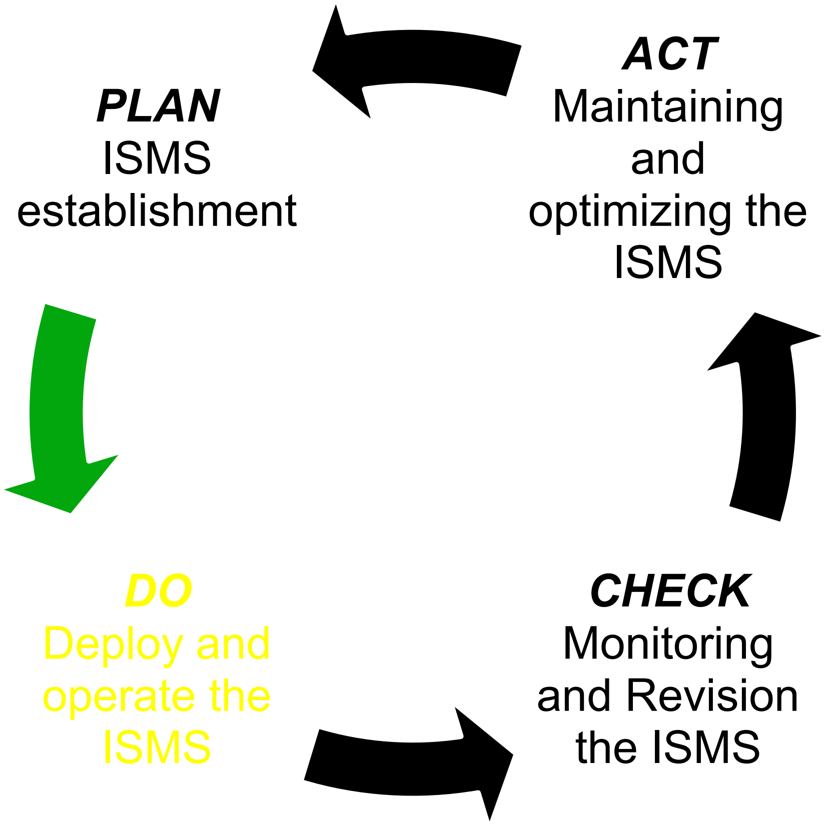
ACT
Maintaining and optimizing the ISMS

DO
Deploy and operate the ISMS

CHECK
Monitoring and Revision the ISMS

InfoSec Management

- Implementation of security controls
  - “Security Engineering”, risk control and confidence
  - Continuity, repeatability, efficiency and reliability
- ISO/IEC 21827 – will be replaced by 27003(?)



PLAN
ISMS establishment

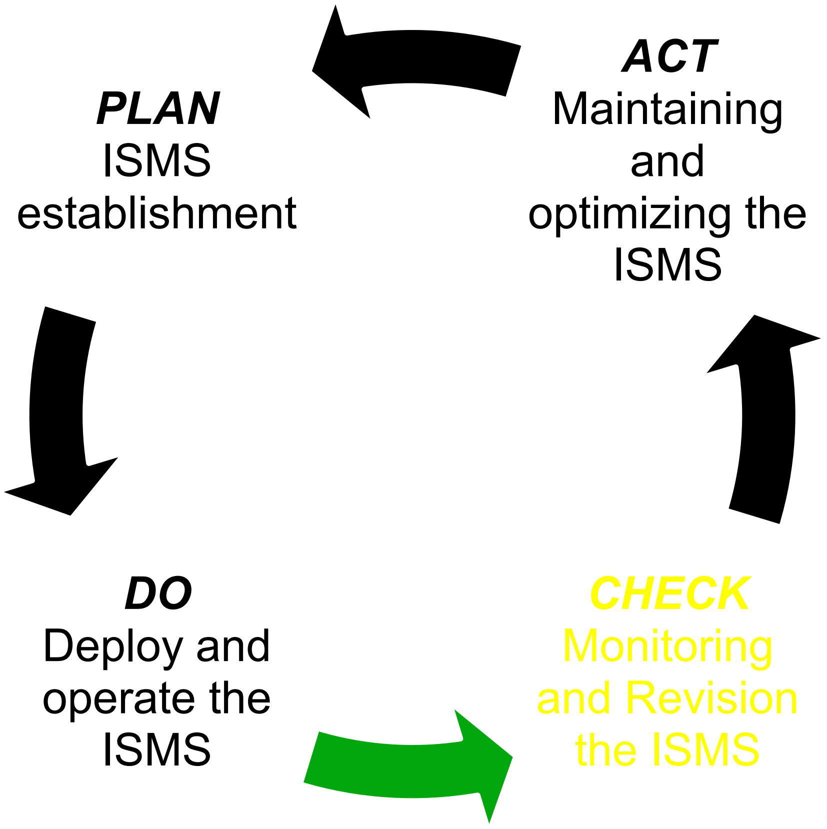
ACT
Maintaining and optimizing the ISMS

DO
Deploy and operate the ISMS

CHECK
Monitoring and Revision the ISMS

InfoSec Management

- Security assessment
  - Measurement of compliance with safety requirements (and functional, when necessary); determine the protection of privacy
  - Measuring the efficiency and correctness of repeatability, efficiency and reliability
- ISO/IEC 15408 – will be replaced by 27004(?) but…



PLAN
ISMS establishment

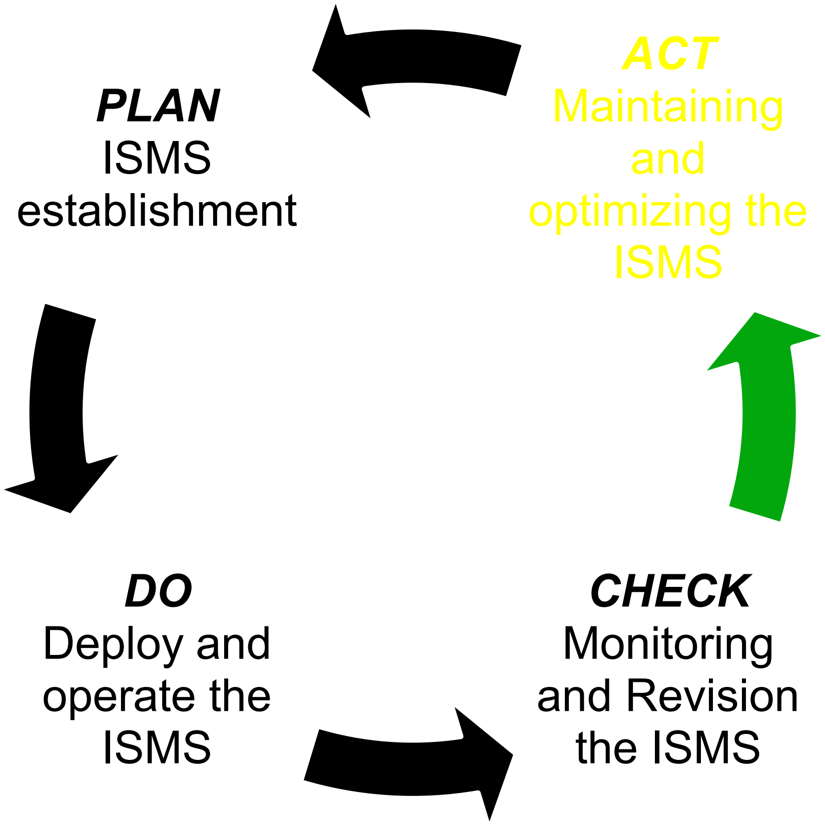
ACT
Maintaining and optimizing the ISMS

DO
Deploy and operate the ISMS

CHECK
Monitoring and Revision the ISMS

InfoSec Management

- Review the whole process and review the requirements and objectives
  - Documentation of the entire evolution process
  - Improvement mechanisms; internal and external communication
- ISO/IEC 27001
- **CERTIFICATION**



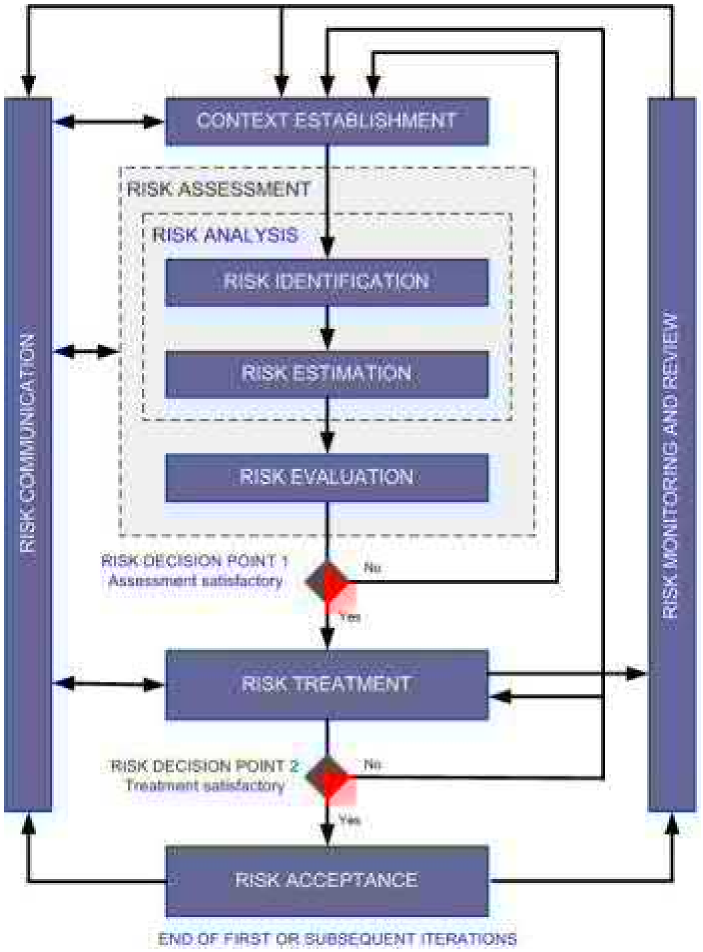
PLAN
ISMS establishment

DO
Deploy and operate the ISMS

CHECK
Monitoring and Revision the ISMS

ACT
Maintaining and optimizing the ISMS

Risk Management



ISO/IEC FDIS 27005:2008(E)

Risk Evaluation (quantitative)

- “A risk (r) consists of the expected likelihood of a hazardous event (p), and the expected damage (e) of it.” [DIN 31000]

$$\boxed{r = p \times e}$$

  - How to determine e for intangible objects?
  - What is the value of a phone number? Of course it depends on the use that is made of it!
  - The p value is usually determined by a Bayeseana function (each p depends on various conditions). How to determine events that occur very rarely?

Risk Evaluation (quantitative)

- For each pair attack/resource *r* is frequently decomposed in:
  - Single Loss Expectancy (**SLE**) – resource value plus percentage corresponding to value lost when attacked
  - Annualized Rate of Occurrence (**ARO**) – annualized probabilistic value of attack occurrence, derived from observation
- SLE x ARO = **ALE** (Annualized Loss Expectancy)
- This model promotes cost/benefit analysis

$$\mathbf{CBA = ALE_{(pre)} - ALE_{(post)} - ACS}$$

where ACS stands for (Annualized Cost of the Safeguard)

Risk Evaluation (quantitative)

- It requires a detailed analysis of the IS, identifying all the targeted assets. The following can help:
  - Aggregation of threats and resources (e.g., by the value of potential losses…)
  - Focus on loss causes
    - Cost of resource replacement
    - Costs due to liability
    - Cost of service interruption (loss of productivity, delay / reduction of turnover; costs of repair; penalties for delays; intangibles like public image…)

Risk Evaluation (quantitative)

- Example of Threats aggregation (ISs' perspective)

Integrity	♦ Authentication ♦ Session High jacking ♦ False data ♦ Non validated access methods ♦ Exploit of trust relationships ♦ Programming errors ♦ Privilege abuse ♦ Backdoors ♦ Social engineering
Confidenciality (privacy)	♦ Inadvertent disclosure ♦ Data theft ♦ Data aggregation
Availability	♦ Service disruption ♦ Inhibition of the audit function

Risk Evaluation (quantitative)

- There are risks that are fully assessed with the quantitative model:
  - 100 operators work in 2.000h/year terminal; rate of typing errors = 100/hour/operator
  - 20,000,000 typos / year (high incidence)
  - 99% are immediately detected at cost 0 (zero)
  - 20,000 will be corrected later, at a cost of $ 1 each
  - ALE = $20.000/year
  - Mitigation:
    - With the cost of $ 100/operator/year in education and training, undetected errors can be reduced by 30% ☹
    - But if you can reduce by 90%... ☺ ☺ ☺

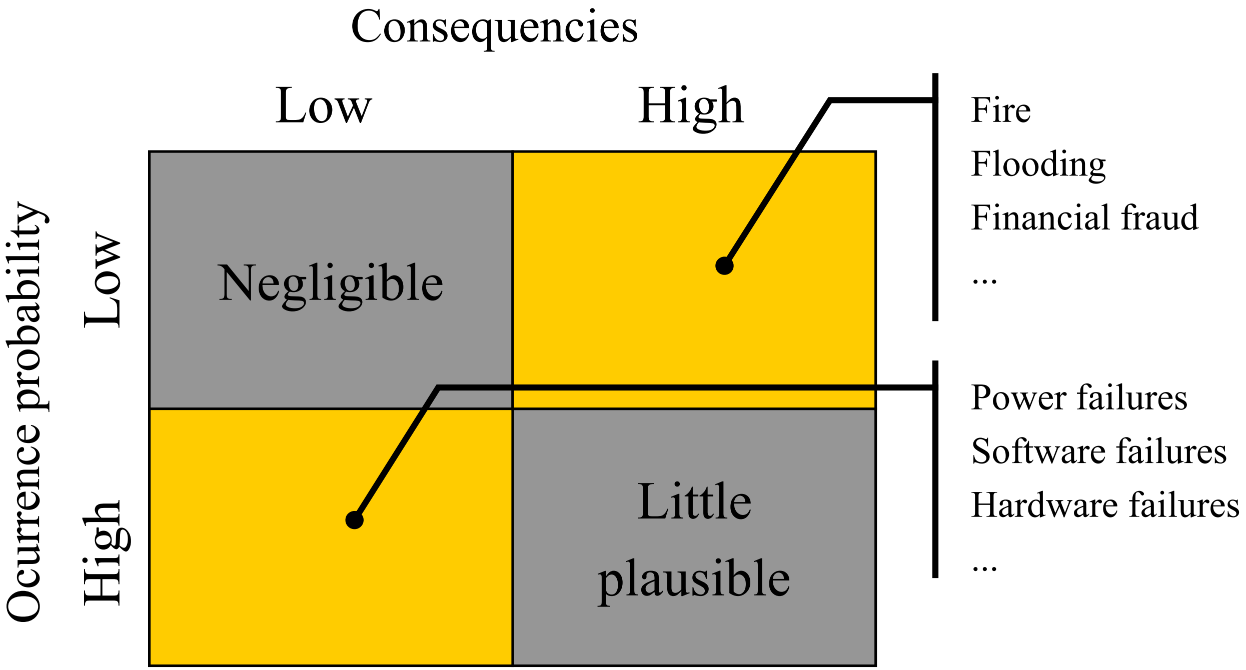
Risk Evaluation (quantitative)

- With rare events it can be observed a high variance in the calculation of loss
- Assume SLE=10k€ and ARO=0,5; ⇒ ALE=5k€ But using a Poisson distribution we can draw the following table (for $\lambda=1$ => 2 year period):

Number of occurrences	Probability	Loss
1	0.3679	10k€
2	0.1839	20k€
3	0.0613	30k€
4	0.0153	40k€
>4	0.0727	≥50k€

Risk Evaluation (qualitative)

- *Jacobson's Window* – a simple model



Consequencies

Low

High

Ocurrence probability

Low

High

Negligible

Little plausible

Fire

Flooding

Financial fraud

...

Power failures

Software failures

Hardware failures

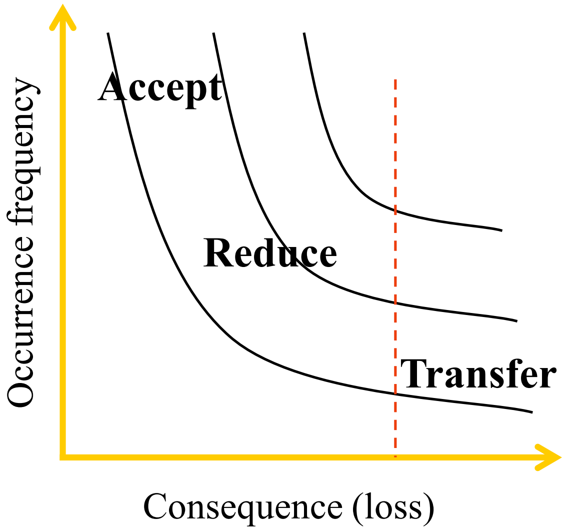
...

Risk treatment

- 4 reasons to adopt mitigation measures
  - The measure is required by law ☺
  - The cost/benefit relation is favorable
  - A risk of the class "Low-High" with a value of loss intolerable
    - Usually quantified by a value SOL (*Single Occurrence Loss*)
  - The cost of the safeguard is less than the reduction of the ALE (i.e., the ROI is positive)

Risk treatment

- Risk mitigation concerning class "Low-High"
  - Reduce the amount of loss
    - Transferring the risk (insurance)
    - Decreasing the exposure of the resource
    - Reduce vulnerabilities associated with the resource
    - Accept risk
  - Model help
    - Decision support



Bibliography

- Bosworth, S. and M. E. Kabay, “Computer Security Handbook, 4th ed.”, John Wiley & Sons, Inc., 2002
- Pfleeger, C. P. and S. L. Pfleeger, “Security in Computing – 4th ed.”, Prentice Hall Professional Technical Reference. 2007
- Dhillon, G. “Managing information system security”, London: Macmillan, 1997
- KPMG. “Building on solid foundations: an information security case study”, report.
- Schneier, B. “Security in the Real World: How to Evaluate Security Technology”, Computer Security Journal, Vol XV, Number 4, 1999
- Theoharidou, M., Gritazalis, D., "Common Body of Knowledge for Information Security," *IEEE Security and Privacy*, vol. 5, no. 2, pp. 64-67, March/April, 2007
- Yasinsac, A. (2001). Information Security Curricula in Computer Science Departments: Theory and Practice, Department of Computer Science, Florida State University.
- CERT Coordination Center, http://www.cert.org/
- NIST Computer Security Division 893 and CSRC Home Page, http://csrc.nist.gov/
- Resources for Security Risk Analysis, Security Policies, ISO 17799 (or BS7799) and Security Audit, http://www.securityauditor.net/
- The Computer Security Institute, http://www.gocsi.com/
- UKITSEC Certified Product List, http://www.itsec.gov.uk/products/
- ...