مواضيع في الامن السيبراني لمنظومات المعلومات الكبيرة: التهديدات والمضادات

جامعة تكنولوجيا المعلومات

أعداد د. لؤي ادور جورج

ايلول 2019

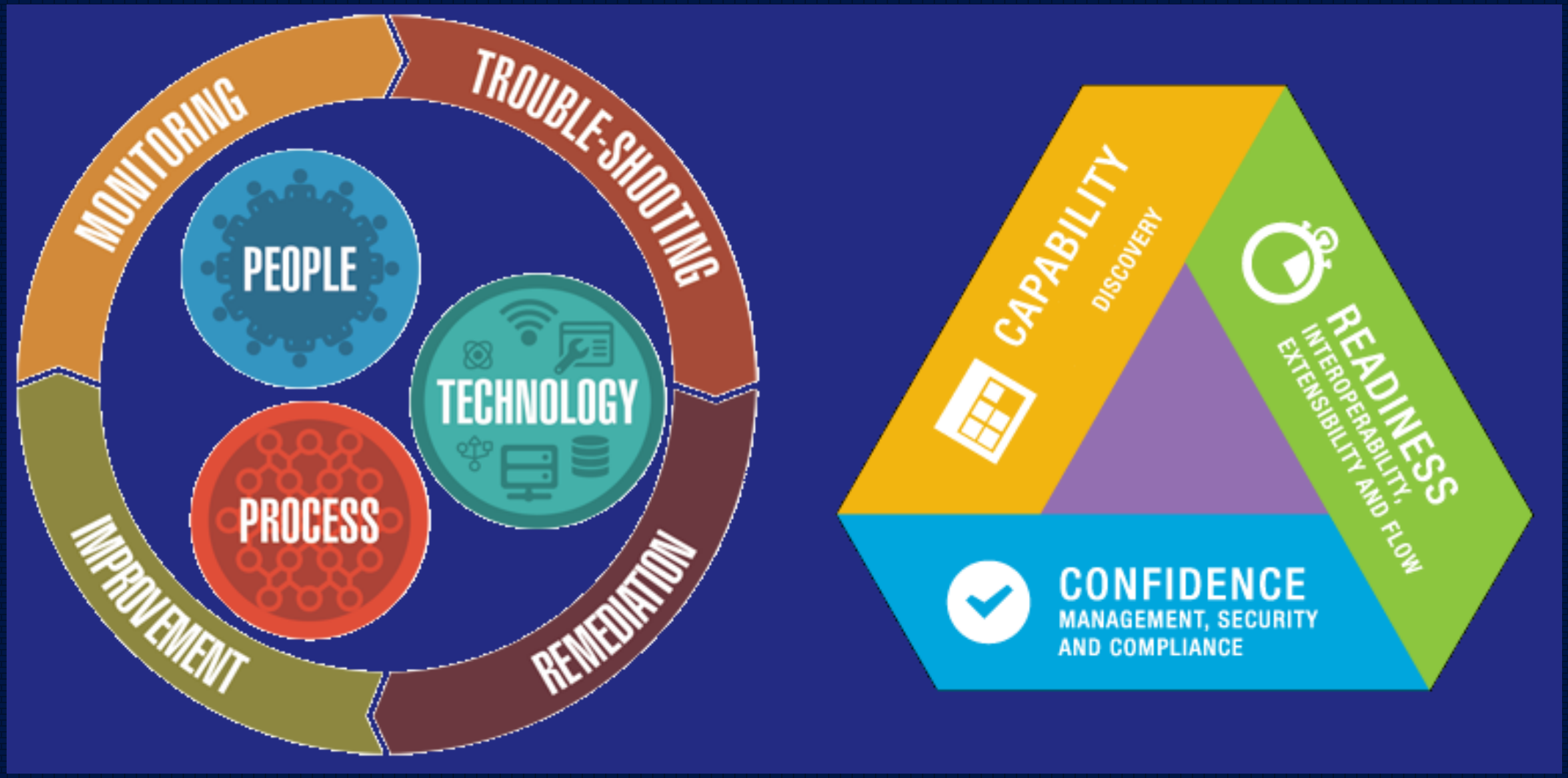
Why Security

To protect and preserve information assets.

In information technology (IT), security is the defense process for digital information and IT assets against "internal" and "external", "malicious and accidental" threats.

The Main Elements of Security System

1. Monitoring (Different Technologies).
2. Detection of threats (Smart, Automated Systems, Smart (intelligent), Various Methodologies).
3. Response or Reaction (Smart, Automated, Growing, Adaptive, Auditable, Using Various Methodologies).


MONITORING
TROUBLE-SHOOTING
REMEDIATION
IMPROVEMENT
PEOPLE
PROCESS
TECHNOLOGY
CAPABILITY
DISCOVERY
READINESS
INTEROPERABILITY,
EXTENSIBILITY AND FLOW
CONFIDENCE
MANAGEMENT, SECURITY
AND COMPLIANCE

There is no Secure System for Ever... in other words "there is no eternity in security... No Security model can stay for long time".

- Always there is need for enhancement, support
- re-enforcement the security system.
- There is need for security staff (specialists in IT security).

What is the difference between Cyber Security and Information Systems Security?

- Basically the difference is the date the phrase was written. What used to be called "Computer Security" became "Information Systems Security" and is now called Cyber Security.
- Of course the change of fashionable names does cover the advances in techniques over time. If someone studied Computer Security at a post-masters degree level in the late 1980s then almost everything they learned is still true.

Factors threaten any life time of any security system

1. Time,
2. Technology,
3. People,
4. Knowledge,
5. Access Control (no. of visits or stay close to system),
6. Discipline & Roles (regulations, ethics).

Information Assets

An information asset is a body of information that has financial value to an organization. Generally speaking, this means that it improves future revenues or reduces future costs. Some of the following information examples are given below:

1. Strategy: Strategies, plans, goals and objectives that have been developed to improve an organizations future.
2. Products & Services: Information that is directly sold to customers as a product or service such as a book or research tool.
3. Intellectual Property: Valuable copyrights, trademarks, patents and other information that is granted legal protections such as trade dress. This includes software that you have developed.

Information Assets (continue)

4. Trade Secrets: Techniques, methods, processes, procedures, formulas and designs that contribute to your competitive advantage.
5. Projects Information: about inflight projects such as requirements, plans and designs. Historical project information may also have limited value as a reference.
6. Training Materials: Media and content that you use to train your employees and partners.
7. Marketing Media: Marketing media such as an advertising poster or video that is used to generate demand or brand awareness.
8. Sales Collaterals: Information tools that are useful for selling such as a sales presentation.

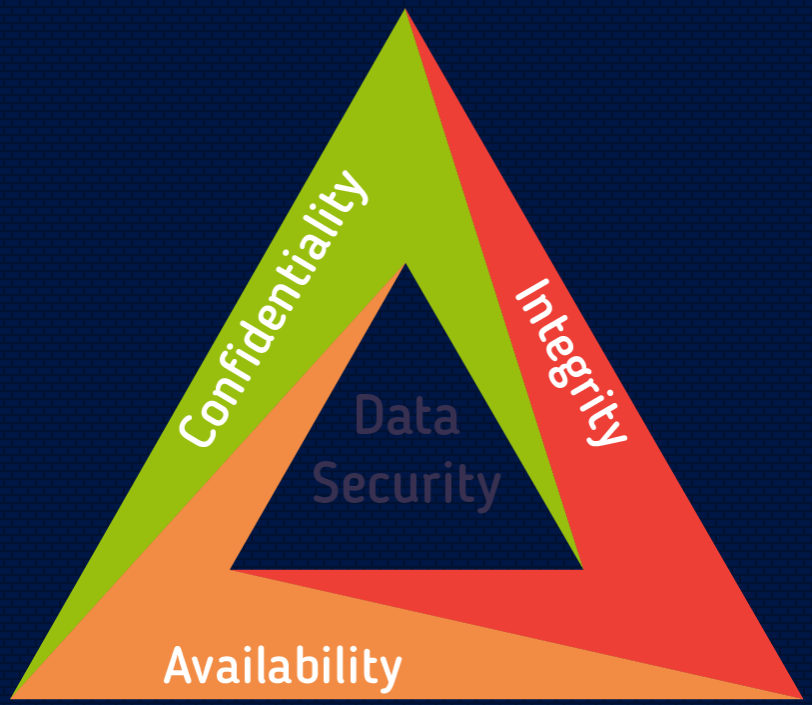
Information Assets (continue)

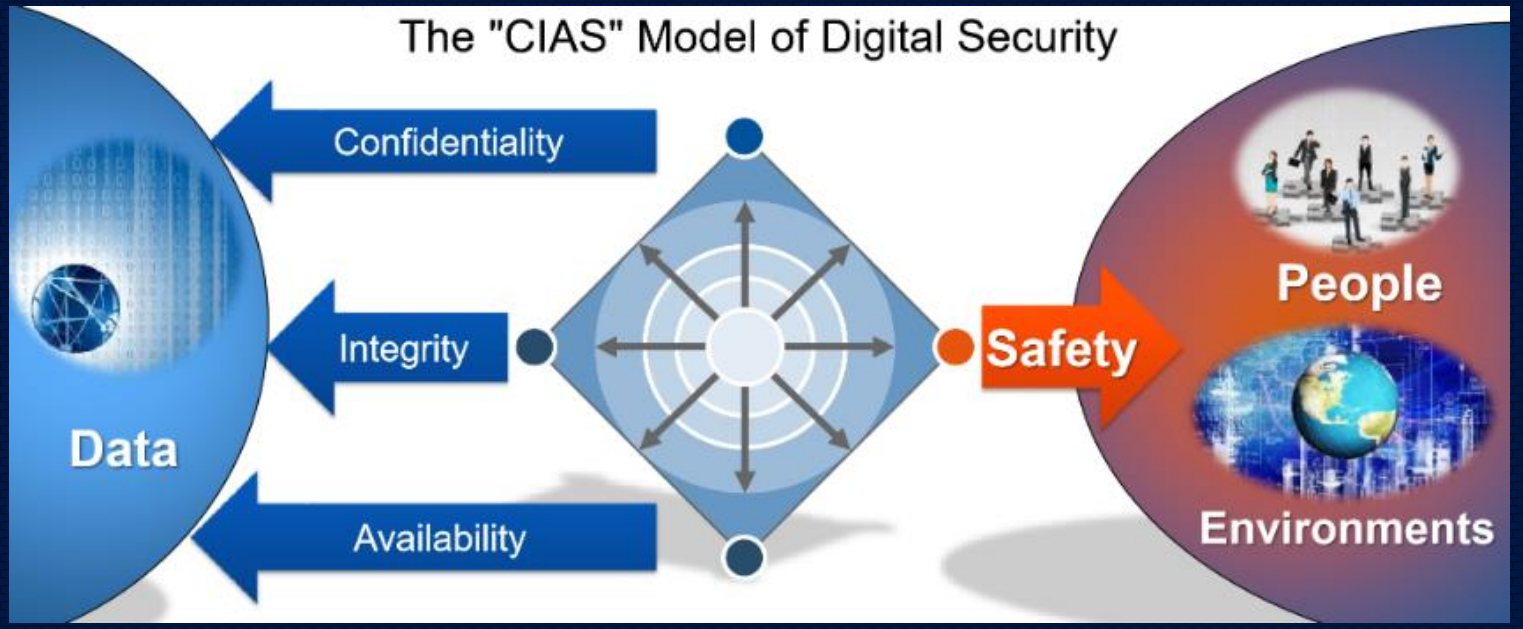
9. Customer Lists: Data about customers and prospective customers.
10. Operations Documentation, software and data that are used to complete processes and procedures. For example, product specifications that are required to operate a production line.
11. Decision Support: Information tools and data that are used to improve decisions.
12. Financial information such as accounting data and financial reports.
13. Organizational Culture: Information such as stories and visual symbols that contribute to organizational culture. For example, a set of principles adopted by a customer service team.

Information Assets (continue)

14. Legal & Compliance: Documents and data that are retained for legal and compliance reasons such as employee performance reviews.
15. Research & Development: Information about current and historical innovation initiatives. For example, market research for a new product design.

The CIA Triad: the Key Concept of Information Security





CIA Triad

Critical Information Characteristics:

1. Confidentiality
2. Integrity
3. Availability.

Security Measures:

1. Educational and training.
2. Policy and practice,
3. Technology.

Information States:

1. Transmission.
2. Storage.
3. Availability.

Confidentiality

- Certain data or information in any corporation needs to be secure from prying eyes.
- Confidentiality provides a degree of assurance that data has not been compromised, made available or disclosed to unauthorized individuals, processes, or other entities. In essence, it assures that data can only be read or understood between trusted parties.
- Confidentiality can be breached bypassed by someone shoulder surfing, sniffing or network monitoring, stealing passwords, or social engineering.

Confidentiality (continue)

Threats to confidentiality include the following:

A. Hackers/crackers;
B. Masqueraders/spoofing;
C. Unauthorized user activity;
D. Unprotected downloaded files;
E. Network sniffing;
F. Trojan horses;
G. Social engineering;

Integrity

Integrity in the formal security model includes the issue of protecting against unauthorized modification or destruction of information. Good integrity includes the assurance that data leaving point A and arriving at point B arrives without modification. Good integrity assures that point A and point B are indeed who they claim to be.

There are three basic principles that are used to establish integrity in the enterprise:

A. Need-to-Know Access: Users should be granted access only to those files and absolutely need to fulfill their duties. This status is the least privileged.

Integrity (continue)

B. Separation of Duties: Use this principle to ensure that no single person has control of a transaction from beginning to end. Make sure that two or more people should be responsible for an entire transaction.

C. Rotation of Duties: Job responsibilities should be periodically changed so that users will find collaboration more difficult to exercise complete control of a transaction or subvert one for fraudulent purposes.

Availability

It is the attribute that ensures the reliable and timely access of resources to authorized individuals. Network engineers have three principles regarding users needs ingrained into them from management:

A. They need the network to work,

B. They need to be able to access their resources,

C. They need to be able to access their resources.

Availability (continue)

- Network engineers can provide sufficient bandwidth from users to their resources; they can provide Quality of Service (QoS) guarantees to ensure high priority traffic reaches the destination first, they can provide high-availability and redundancy in the network;
- but they cannot ensure that the system from which data is being requested is operational and able to reply to requests. Availability addresses all those questions, and as you can see, covers a large portion of the network in general.

Availability (continue)

There are two facets of availability that are normally discussed:

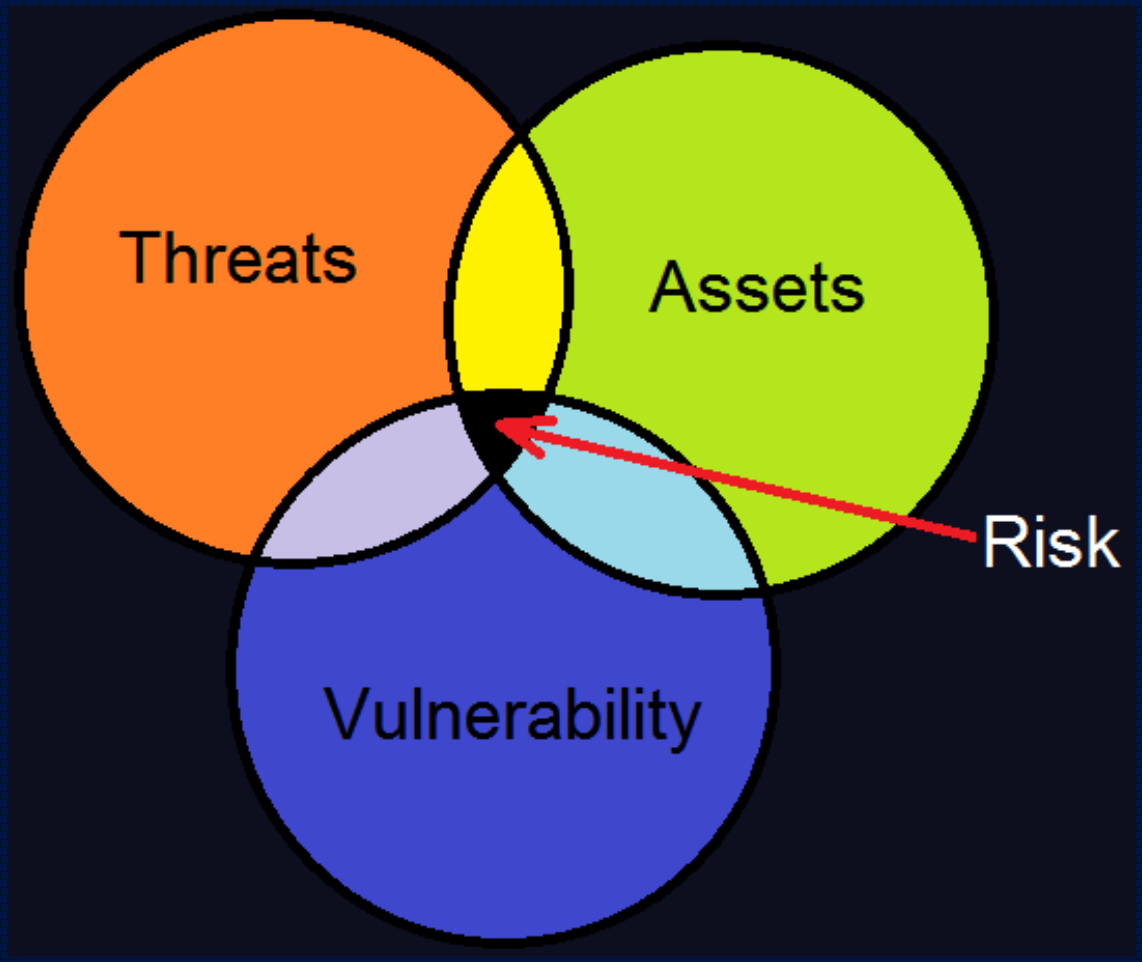
A. Denial-of-Service (DoS): Actions by users or attackers that tie up computing resources in such a way that renders the system unusable or unable to reply to authorized users.

B. Loss of Capabilities: When natural disasters (fire, flood, earthquake) or human action (bombs, strikes, malicious code) create loss of data processing capabilities.

Vulnerability vs Threat vs Risk

- An asset (A) is what we're trying to protect.
- A threat (T) is what we're trying to protect against.
- A vulnerability (V) is a weakness or gap in our protection efforts.
- Risk (R) is the intersection of assets, threats, and vulnerabilities.

A + T + V = R



Information security vulnerabilities are weaknesses that expose an organization to risk. Understanding your vulnerabilities is the first step to managing risk.

The List of Vulnerabilities

The Big List of Vulnerabilities

1. Employees

A. Social interaction;

B. Customer interaction;

C. Discussing work in public locations;

D. Taking data out of the office (paper, mobile phones, laptops);

E. Emailing documents and data;

F. Mailing and faxing documents;

G. Installing unauthorized software and apps;

H. Removing or disabling security tools;

I. Letting unauthorized persons into the office.

The Big List of Vulnerabilities

1. Employees (continue)

J. Opening spam emails;
K. Connecting personal devices to company networks;
L. Writing down passwords and sensitive data;
M. Losing security devices such as id cards;
N. Lack of information security awareness;
O. Keying data.

2. Former Employees

A. Former employees working for competitors;
B. Former employees retaining company data;
C. Former employees discussing company matters.

The Big List of Vulnerabilities

3. Technology

A. Social networking;
B. File sharing;
C. Rapid technological changes;
D. Legacy systems;
D. Storing data on mobile devices such as mobile phones;
F. Internet browsers.

4. Hardware

A. Susceptibility to dust, heat and humidity;
B. Hardware design flaws;
C. Out of date hardware;
D. Misconfiguration of hardware.

The Big List of Vulnerabilities

5. Software
    A. Insufficient testing;
    B. Lack of audit trail;
    C. Software bugs and design faults;
    D. Unchecked user input;
    E. Software that fails to consider human factors;
    F. Software complexity (bloatware);
    G. Software as a service (relinquishing control of data);
    H. Software vendors that go out of business or change ownership.

The Big List of Vulnerabilities

6. Network

A. Unprotected network communications;

B. Open physical connections, IPs and ports;

C. Insecure network architecture;

D. Unused user ids;

E. Excessive privileges;

F. Unnecessary jobs and scripts executing;

G. Wifi networks.

The Big List of Vulnerabilities

7. IT Management

A. Insufficient IT capacity;

B. Missed security patches;

C. Insufficient incident and problem management;

D. Configuration errors and missed security notices;

E. System operation errors;

F. Lack of regular audits;

G. Improper waste disposal;

H. Insufficient change management;

I. Business process flaws.

The Big List of Vulnerabilities

7. IT Management (Continue)

J. Inadequate business rules;

K. Inadequate business controls;

L. Processes that fail to consider human factors;

M. Overconfidence in security audits;

N. Lack of risk analysis;

O. Rapid business change;

P. Inadequate continuity planning;

Q. Lax recruiting processes.

The Big List of Vulnerabilities

8. Partners and Suppliers

A. Disruption of telecom services;

B. Disruption of utility services such as electric, gas, water;

C. Hardware failure;

D. Software failure;

E. Lost mail and courier packages;

F. Supply disruptions;

G. Sharing confidential data with partners and suppliers.

The Big List of Vulnerabilities

9. Customers

A. Customers access to secure areas;

B. Customer access to data (i.e., customer portal).

10. Offices and Data Centers

A. Sites that are prone to natural disasters such as earthquakes;

B. Locations that are politically unstable;

C. Locations subject to government spying;

D. Unreliable power sources;

E. High crime areas;

F. Multiple sites in the same geographical location.

The List of Threats

The Big List of Threats

1. Nature and Accidents

A. Earthquakes;

B. Landslides;

C. Volcanoes;

D. Fires;

E. Storms and floods;

F. Transportation accidents (car, aviation etc..);

G. Hazardous materials related events;

H. Solar flares.

The Big List of Threats

Current and Past Employees

A. Human error;

B. Sabotage;

C. Tampering;

D. Vandalism;

E. Theft;

F. Unions, strikes and labour actions;

G. Pandemics and disease;

H. Insider trading;

I. Fraud;

J. Liability for employee actions;

K. Scandals;

L. Corporate crime;

M. Discriminatory abuse;

N. Workplace bullying;

O. Sexual harassment;

P. Professional misconduct;

Q. Negligence;

R. Passive–aggressive behavior;

S. Workplace revenge;

T. Insurance fraud;

U. Lawsuits against employer.

The Big List of Threats

3. Competitors

A. Industrial espionage;

B. Intellectual property theft;

C. Copyright infringement;

D. Mudslinging;

E. Illegal infiltration;

F. Dirty tricks;

G. Patent infringement;

H. Competitive research;

I. Price surveillance.

The Big List of Threats

4. Litigants

A. Seeking confidential data as evidence.

5. The Press

A. Bad publicity;

B. Exposing trade secrets;

C. Exposing strategy and new products.

The Big List of Threats

6. Hackers

A. IP Spoofing;

B. Social engineering;

C. Man-in-the-middle spoofing;

D. DNS Poisoning;

E. Trojan;

F. Cracks;

G. Worms;

H. Viruses;

I. Eavesdropping;

J. Spam;

K. Phishing;

L. Spyware;

M. Malware;

N. Password Cracking;

O. Network sniffing;

P. Back door/trap door;

Q. Tunneling;

R. Website defacement;

S. TCP/IP hijacking;

T. Replay Attacks;

U. System tampering;

V. System penetration.

The Big List of Threats

7. Criminals

A. Kidnapping;

B. Bribery;

C. Extortion;

D. Fraud;

E. Theft;

F. Physical infrastructure attacks;

G. Information blackmail;

H. Assault;

I. Sale of stolen information;

J. Cyberstalking.

The Big List of Threats

8. Governments, Terrorists and Political Organizations

A. Acts of war (conventional);

B. Nuclear war;

C. Biological warfare;

D. Chemical warfare;

E. Computer warfare (including physical disruption of communication satellites etc..);

F. Espionage;

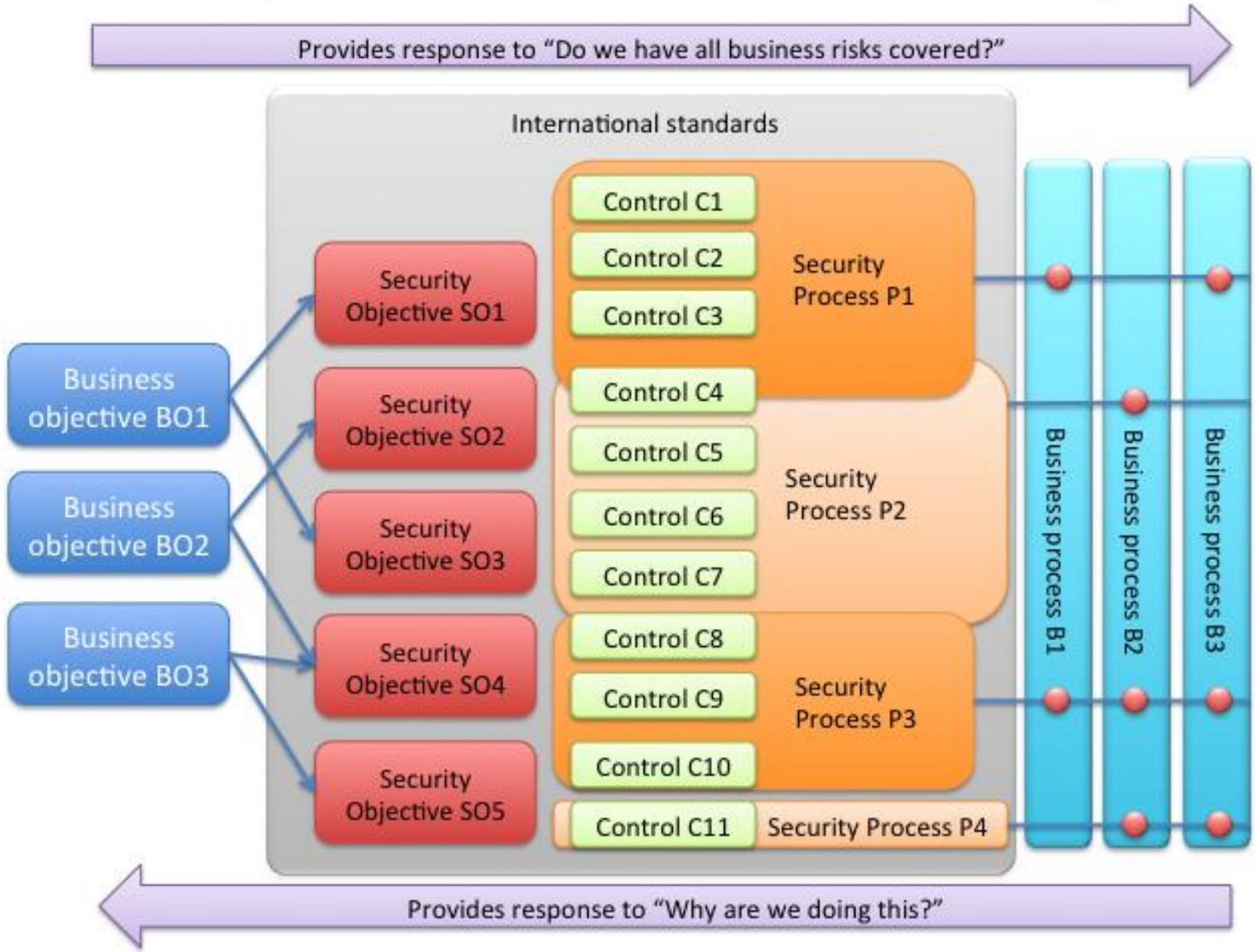
G. Terrorism;

H. Cyberwarfare;

I. Electromagnetic weapons;

J. Wiretapping.

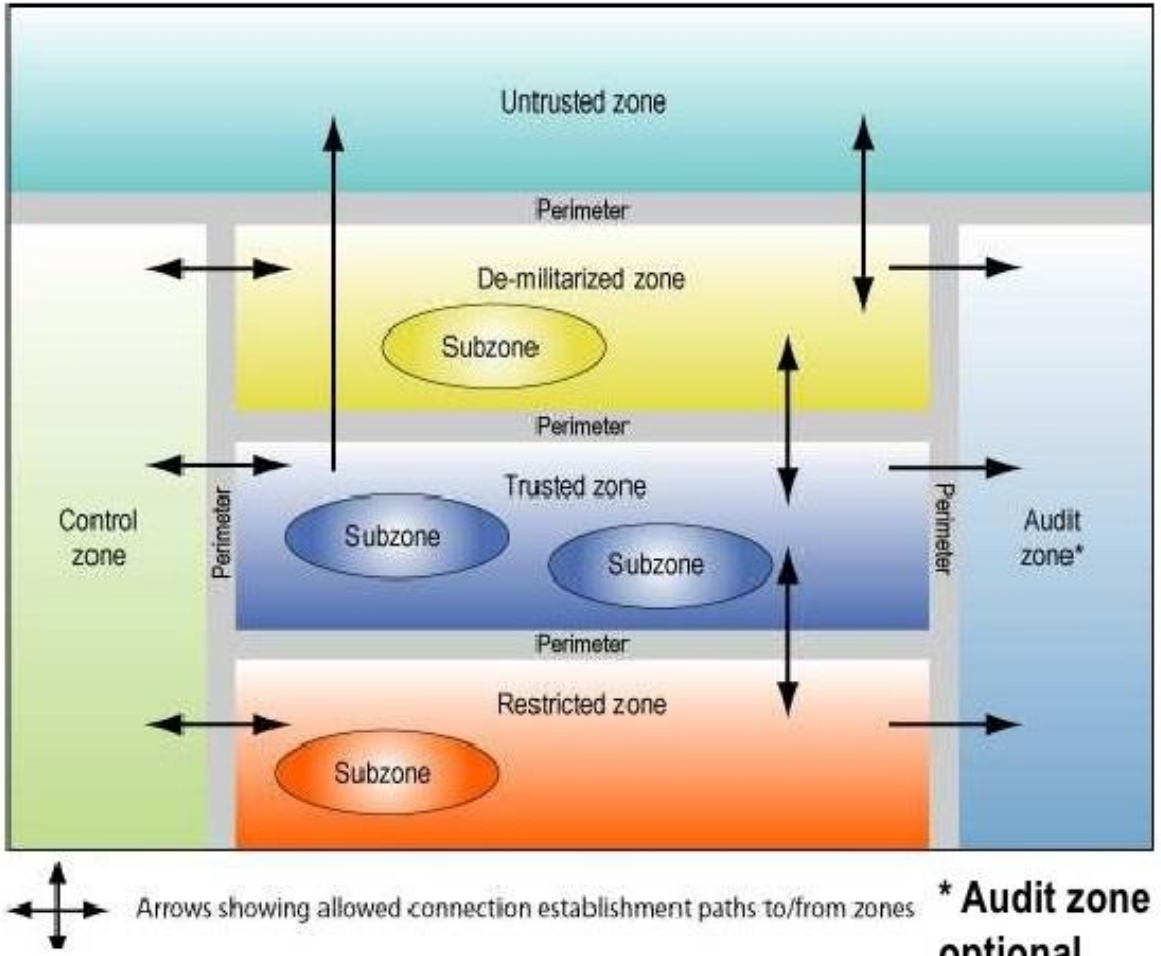
Relationship between business objectives and security processes



Security Zone Model

Zone definition: "A grouping of IT resources which may reside at multiple locations but have similar business communication and network protection requirements"

Typical organization has equivalent of some or all of these zones



Cloud Computing

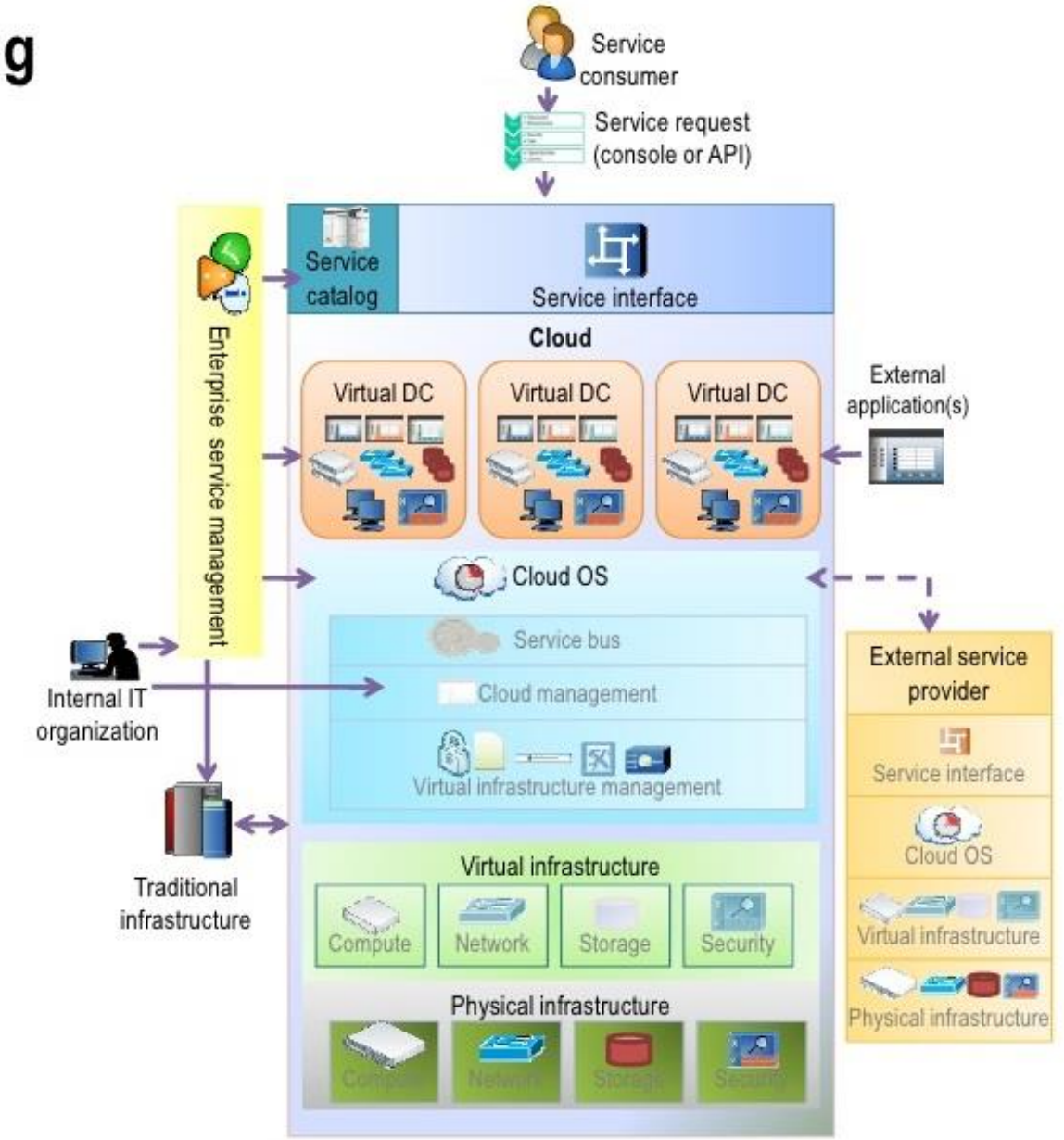
The set of disciplines, technologies, and business models used to deliver IT capabilities (software, platforms, hardware) as on-demand, scalable, elastic services

How can I make this...

Look more like this?

Cloud Computing Requires a New Security Architecture

- Virtual data centers
- Service oriented interfaces
- Next generation of operating systems and management tools



Thank you for Listening

Good Luck