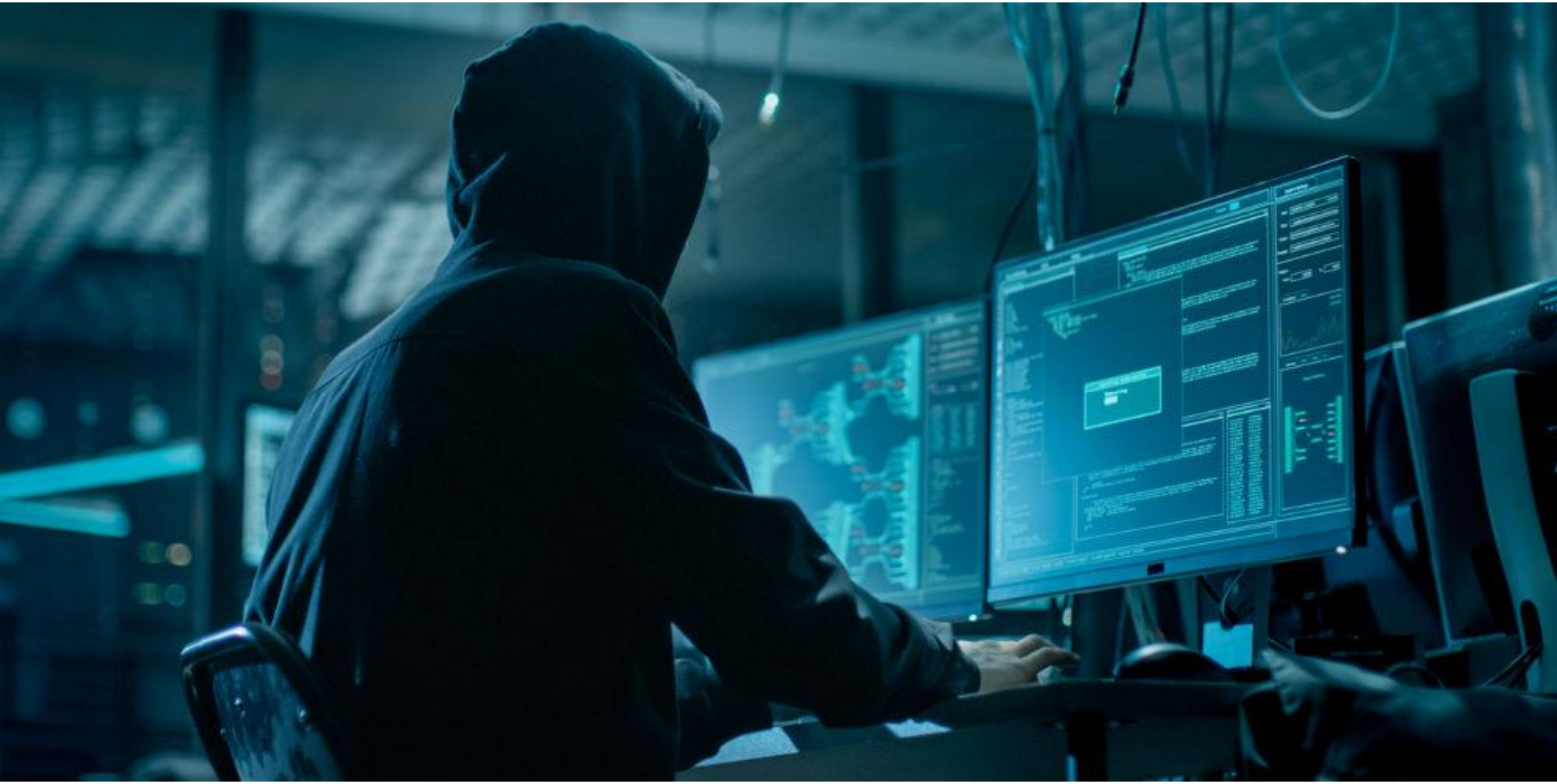
Introduction

INFORMATICS AND ORGANIZATIONAL SECURITY

Security



Security

Subject focused in the predictability of systems, processes, environments…

Across all aspects of the life cycle:

- Planning
- Development
- Execution
- Processes
- People
- Clients and Supply Chain
- Mechanisms
- Standards and Laws
- Intellectual Property

Security: Planning

Design of a solution complying with some requirements under a normative context

Without flaws

- All operation states are the ones predicted
- There are no additional states escaping the expected logic
  - Even if forced transitions are used

Under the scope of a normative context

- Specific for each activity or sector
- Ex: ISO 27001, ISO 27007, ISO 37001

Security: Development

Implement a solution complying with the design, without other operation modes

Without bugs which compromise the correct execution

- No crashes
- Without invalid or unexpected results
- With the correct execution times
- With adequate resource consumption
- With adequate access control to resources
- Without information leaks

Software:

- Requires careful implementation
- Requires tests to obtain an implementation with the expected… and only the expected behavior

Source: https://www.verificient.com/

Security: Execution

Code executes as it was written, with all predicted processes

Environment is controlled, cannot be manipulated or observed

Without the existence of anomalous behavior, introduced by environmental aspects

- Such as: storage speed, RAM amount, trusted communications

Security: people

Staff behavior cannot have a negative impact to the solution

Norms are in place to regulate what actions are expected

Staff is trained to distinguish correct from incorrect behavior

Staff has the correct incentives to behave adequately

When staff is compromised, or deviate, actions have limited impact

Security: Analysis and Auditing

What is the actual behavior of the solution?

Identify deviations from the expected atributes

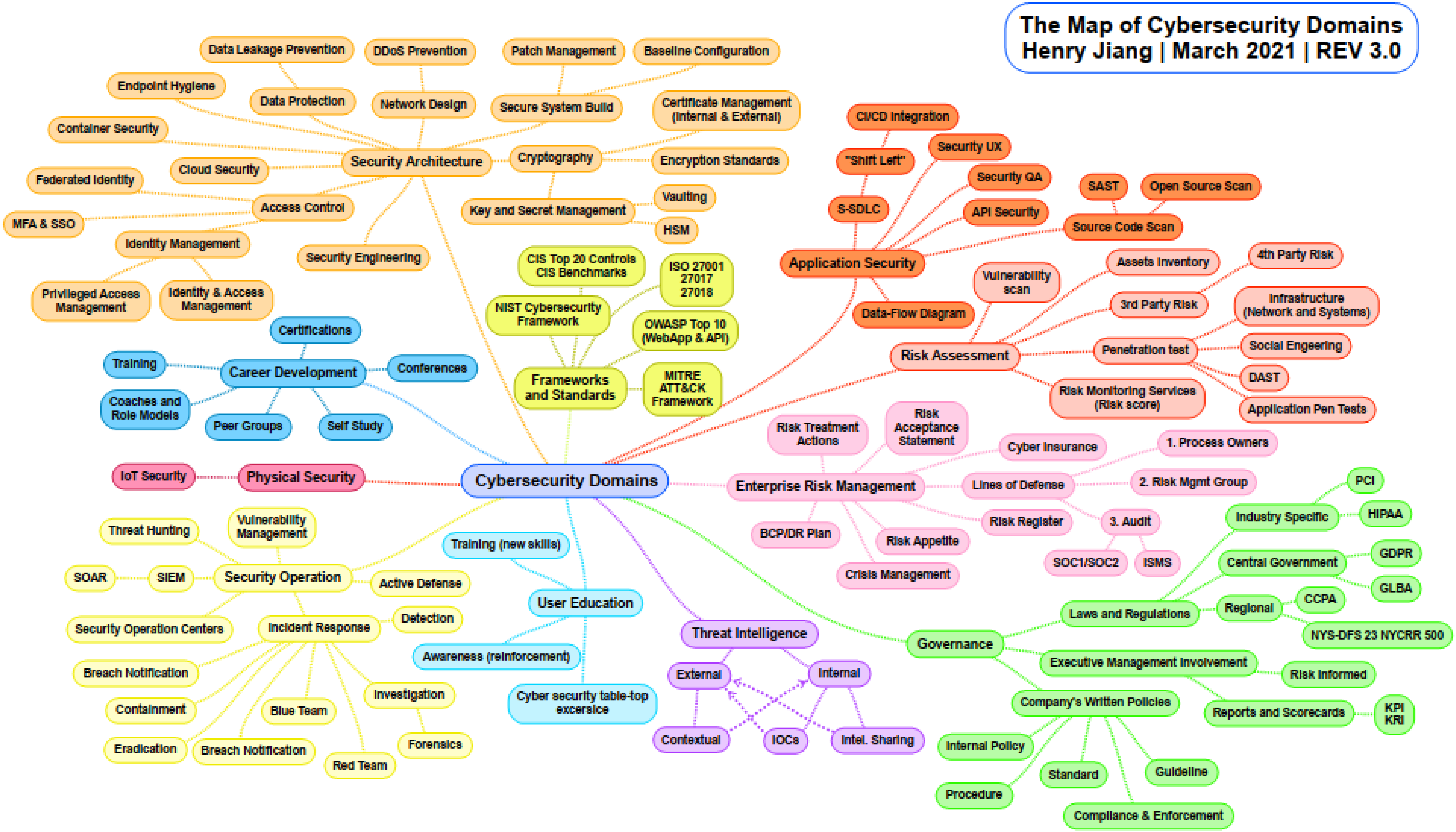
- Faults, Errors, behavior

Identify the risk for the solution to be modified

- Exposition to possible attackers
- Incentives one may have to modify it
- Identify potential actos (Threats)

Identify the impact of the deviations

- Total loss of data? Denial of Service? Increase Operation Cost?

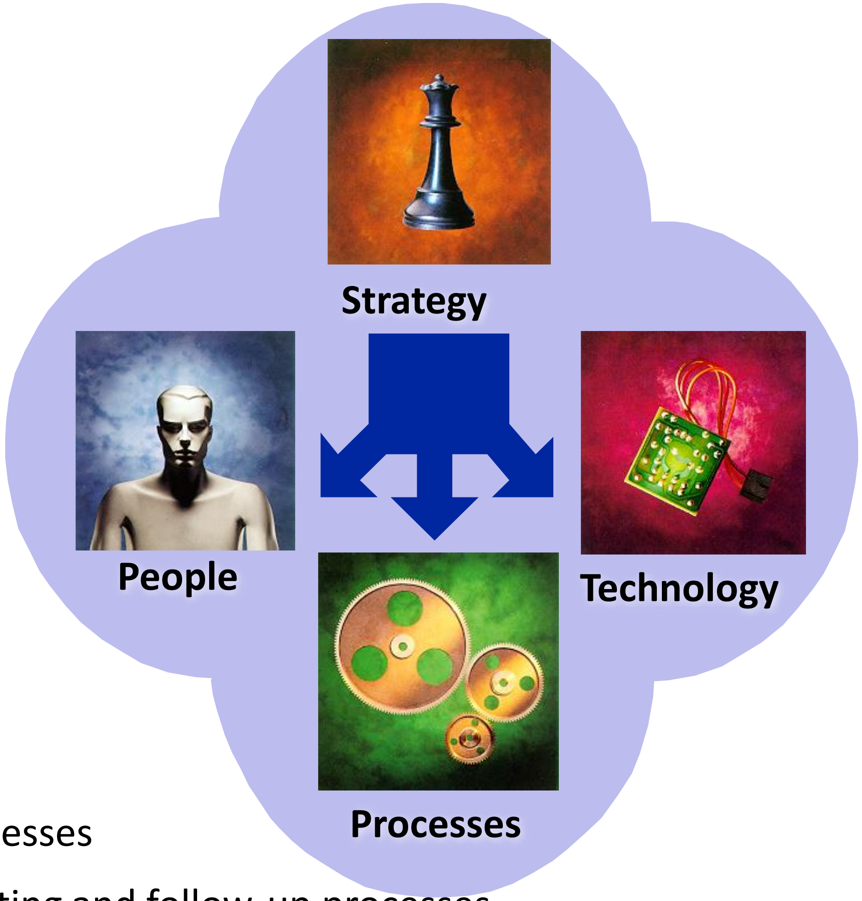


The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.0

- Cybersecurity Domains
  - Security Architecture
    - Data Leakage Prevention
    - DDoS Prevention
    - Patch Management
    - Baseline Configuration
    - Endpoint Hygiene
    - Data Protection
    - Network Design
    - Secure System Build
    - Certificate Management (Internal & External)
    - Container Security
    - Cloud Security
    - Cryptography
      - Encryption Standards
      - Key and Secret Management
        - Vaulting
        - HSM
    - Access Control
      - Federated Identity
      - MFA & SSO
      - Identity Management
        - Privileged Access Management
        - Identity & Access Management
    - Security Engineering
  - Career Development
    - Certifications
    - Training
    - Conferences
    - Coaches and Role Models
    - Peer Groups
    - Self Study
  - Frameworks and Standards
    - CIS Top 20 Controls CIS Benchmarks
    - ISO 27001 27017 27018
    - NIST Cybersecurity Framework
    - OWASP Top 10 (WebApp & API)
    - MITRE ATT&CK Framework
  - Application Security
    - CI/CD Integration
    - Security UX
    - "Shift Left"
    - Security QA
    - S-SDLC
    - API Security
    - Source Code Scan
      - SAST
      - Open Source Scan
    - Data-Flow Diagram
  - Risk Assessment
    - Vulnerability scan
    - Assets Inventory
    - 3rd Party Risk
      - 4th Party Risk
    - Penetration test
      - Infrastructure (Network and Systems)
      - Social Engageing
      - DAST
      - Application Pen Tests
    - Risk Monitoring Services (Risk score)
  - Physical Security
    - IoT Security
  - Enterprise Risk Management
    - Risk Treatment Actions
    - Risk Acceptance Statement
    - Cyber Insurance
    - Lines of Defense
      - 1. Process Owners
      - 2. Risk Mgmt Group
      - 3. Audit
        - SOC1/SOC2
        - ISMS
    - Risk Register
    - BCP/DR Plan
    - Risk Appetite
    - Crisis Management
  - Security Operation
    - Threat Hunting
    - Vulnerability Management
    - SIEM
      - SOAR
    - Active Defense
    - Security Operation Centers
    - Incident Response
      - Detection
      - Breach Notification
      - Containment
      - Eradication
      - Breach Notification
      - Blue Team
      - Red Team
      - Investigation
      - Forensics
  - User Education
    - Training (new skills)
    - Awareness (reinforcement)
    - Cyber security table-top excersice
  - Threat Intelligence
    - External
    - Internal
    - Contextual
    - IOCs
    - Intel. Sharing
  - Governance
    - Laws and Regulations
      - Industry Specific
        - PCI
        - HIPAA
      - Central Government
        - GDPR
        - GLBA
      - Regional
        - CCPA
        - NYS-DFS 23 NYCRR 500
    - Executive Management Involvement
      - Risk Informed
    - Reports and Scorecards
      - KPI KRI
    - Company's Written Policies
      - Internal Policy
      - Standard
      - Guideline
      - Procedure
      - Compliance & Enforcement

Dimensions to consider

- Selection
- Training
- Awareness
- Organization of security



- Vulnerability scanning
- Firewalls
- Authentication
- Access Control
- Cryptography
- Digital Signatures
- Certification authorities
- Certification hierarchies
- etc...

- Security policies
- Security administration processes
- Continued evolution of auditing and follow-up processes

Perspectives

Security has multiple intertwined perspectives

Defensive: focus on maintaining predictability

Offensive: focus on exploiting predictability

- With malicious/criminal intent
- With the purpose of validating the solution (Red Teams)

Other:

- Reverse Engineering: Recovery of design from built products
- Forensics: extract information and reconstruct previous events
- Disaster Recovery: minimize the impact of attacks
- Auditing: validate the solution complies with some set of requirements

Information Security

CIA: Confidentiality, Integrity, Availability

Confidentiality: Information can only be accessed by a restricted set of subjects

Integrity: Information is not modified

- Can be extended to behavior of devices and services (outside infosec)

Availability: Information is available

- Can be extended to service/systems

Information Security - Users

Privacy: Information dissemination from an individual is restricted

- Focus on information from users
- Addresses dissemination, storage and manipulation

Personification: Act under the identity of another subject

- Explore an identity without authorization (Identity Theft)
- Related with individuals, services or systems

Core Concepts

1. **Domains**
2. **Policies**
3. **Mechanisms**
4. **Controls**

Security Domains

A set of entities sharing similar security attributes

Allow managing security in a aggregated manner

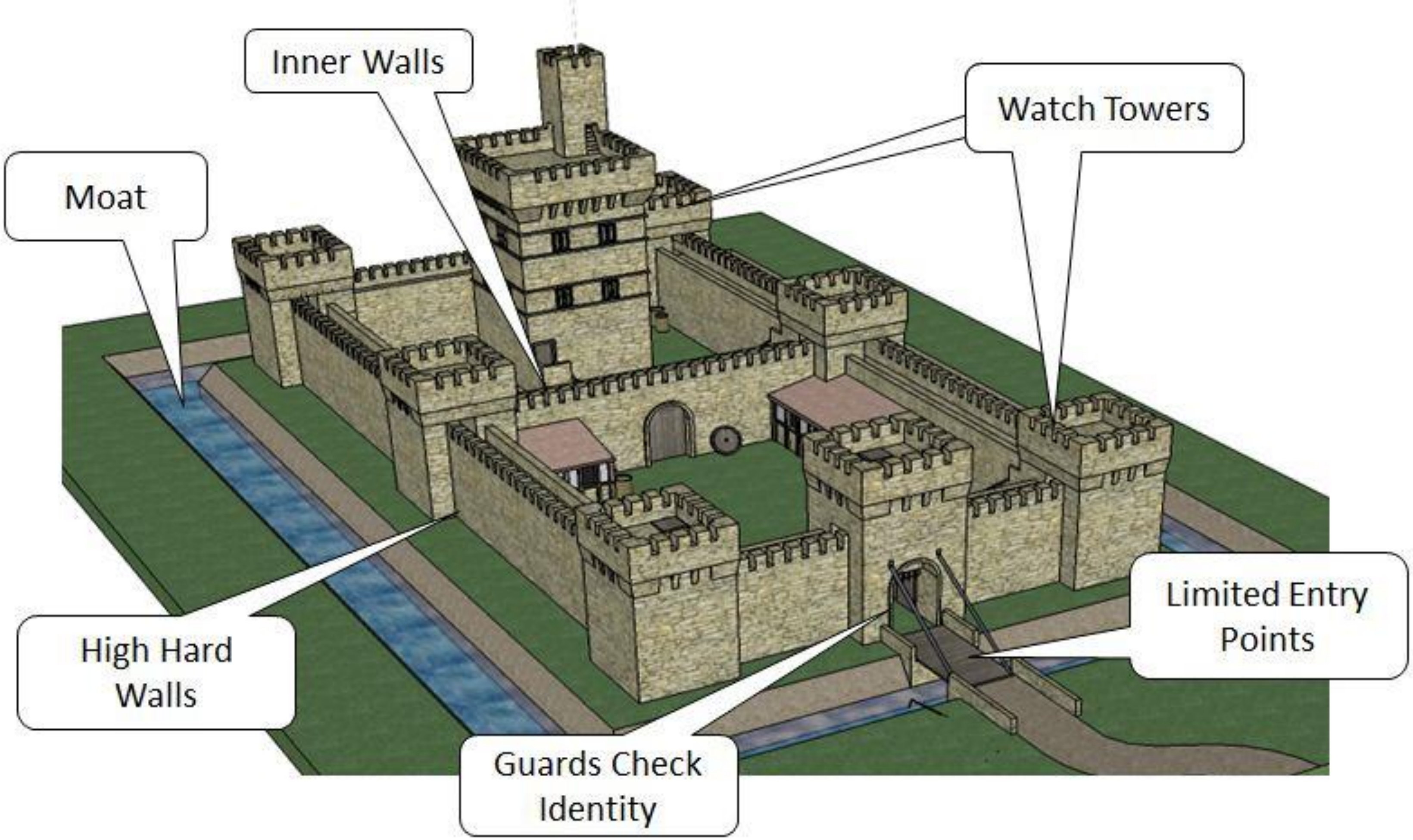
- Management will set the attributes of the domain
- Entities are added do the domain and will get the "group" attributes

Behavior and interactions are homogenous inside the domain

Domains can be organized in a flat of hierarchical manner

Interactions between domains are usually controlled

Security Domains



Security Policies

Set of guidelines related to security, that rule over a domain

Organization will contain multiple policies

- Applicable to each specific domain
- They may overlap and have different scopes/abstraction levels

The multiple policies must be coherent

Examples

- Users can only access web services
- Subjects must be authenticated in order to enter the domain
- Walls must be made of concrete
- Communications must be encrypted

Security Policies

Define the power of each subject

- Least privilege principle: each subject should only have the privileges required for the fulfillment of his duties.

Define security procedures

- Who does what in which circumstances

Define the minimum security requirements of a domain

- Security levels, Security Groups
- Required authorization
  - And the related minimum authentication requirements (Strong/weak, single/multifactor, remote/face-to-face)

Security Policies

Define defense strategies and fight back tactics

- Defensive architecture
- Monitoring of critical activities or attack signs
- Reaction against attacks or other abnormal scenarios

Define what are legal and illegal activities

- Forbid list model: Some activities are denied, the rest are allowed
- Permit list model: Some activities are allowed, the rest is forbidden

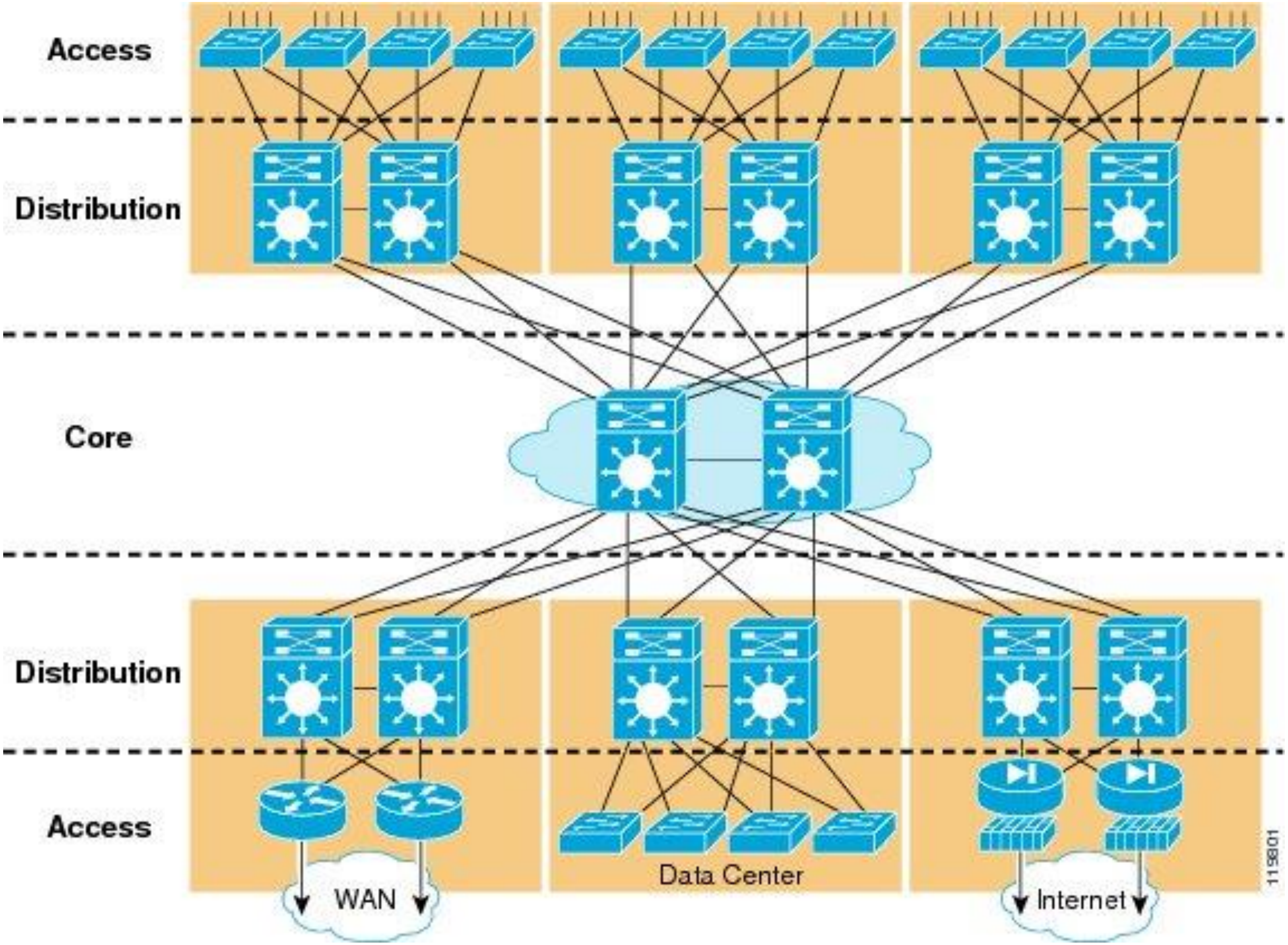
Security mechanisms

Mechanisms implement policies

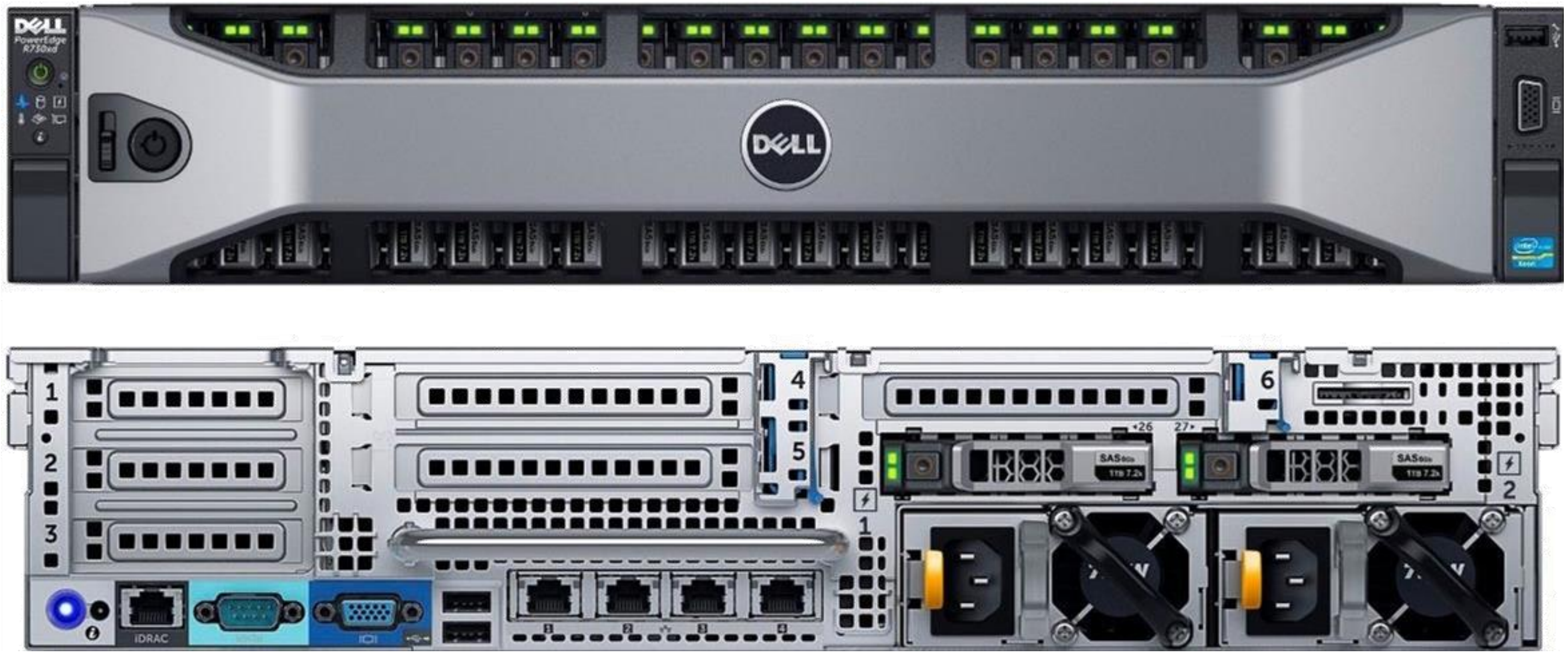
- Policies define, at a higher level, what needs to be done or exist
- Mechanisms are used to deploy policies

Generic security mechanisms

- Confinement (Sandboxing)
- Authentication
- Access control
- Privileged Execution
- Filtering
- Logging
- Auditing
- Cryptographic algorithms
- Cryptographic protocols



Source: CISCO



Source: DELL

Security Controls

Controls are any aspect allowing to minimize risk (protect the CIA properties)

Controls include policies and mechanisms, but also:

- Norms
- Processes
- Laws
- Regulations

Controls are explicitly stated and can be auditable

- Act as control points of a solution

Types of Security Controls

	Prevention	Detection	Correction
Physical	- Fences - Gates - Locks	- CCTV	- Repair Locks - Repair Windows - Redeploy access cards
Technical	- Firewall - Authentication - Antivirus	- Intrusion Detection Systems - Alarms - Honeypots	- Vulnerability patching - Reboot Systems - Redeploy VMs - Remove Virus
Administrative	- Contractual clauses - Separation of Duties - Information Classification	- Review Access Matrixes - Audits	- Implement a business continuity plan - Implement an incident response plan

Security objectives (1/3)

Defense against catastrophic events

- Natural phenomena
- Abnormal temperature, lightning, thunder, flooding, radiation, …

Degradation of computer hardware

- bad sectors in disks
- failure of power supplies
- bit errors in RAM cells or SSD, etc.

Security objectives (2/3)

Defense against ordinary faults / failures

- Power outages
- Systems' internal failures
  - Linux Kernel panic, Windows blue screen, OS X panic
  - Deadlocks
  - Abnormal resource usage
- Software faults / Communication faults...

Security objectives (3/3)

Defense against non-authorized activities (adversaries)

- Initiated by someone “from outside” or “from inside”

Types of non-authorized activities:

- Information access
- Information alteration
- Resource usage
  - CPU, memory, print, network, etc.
- Denial of Service
- Vandalism
  - Interference with the normal system behavior without any benefit for the attacker

Practical Security

Realistic Prevention

Consider that perfect security is impossible

Focus on the most probable events

- May depend on physical location, legal framework, …

Consider cost and profit

- A great number of controls has a low cost
- However, there is no upper limit on the cost of a security strategy

Consider all domains and entities

- A single breach can be escalated to a more serious situation

Practical Security

Realistic Prevention

Consider Impact

- Under the light of CIA and other potential impact areas (e.g. brand)

Consider the cost and recover time

- Monetary cost, reputation, market access

Characterize attackers

- Define controls specific for those attackers
- There will always exist more resourceful attackers

Consider that the system will be compromised

- Have recovery plans

Security in computing systems: Complex problems

Computers can do much damage in a short time frame

- Computers manage huge amounts of information
- Process and communicate with very high speed

The number of <u>weaknesses is always growing</u>

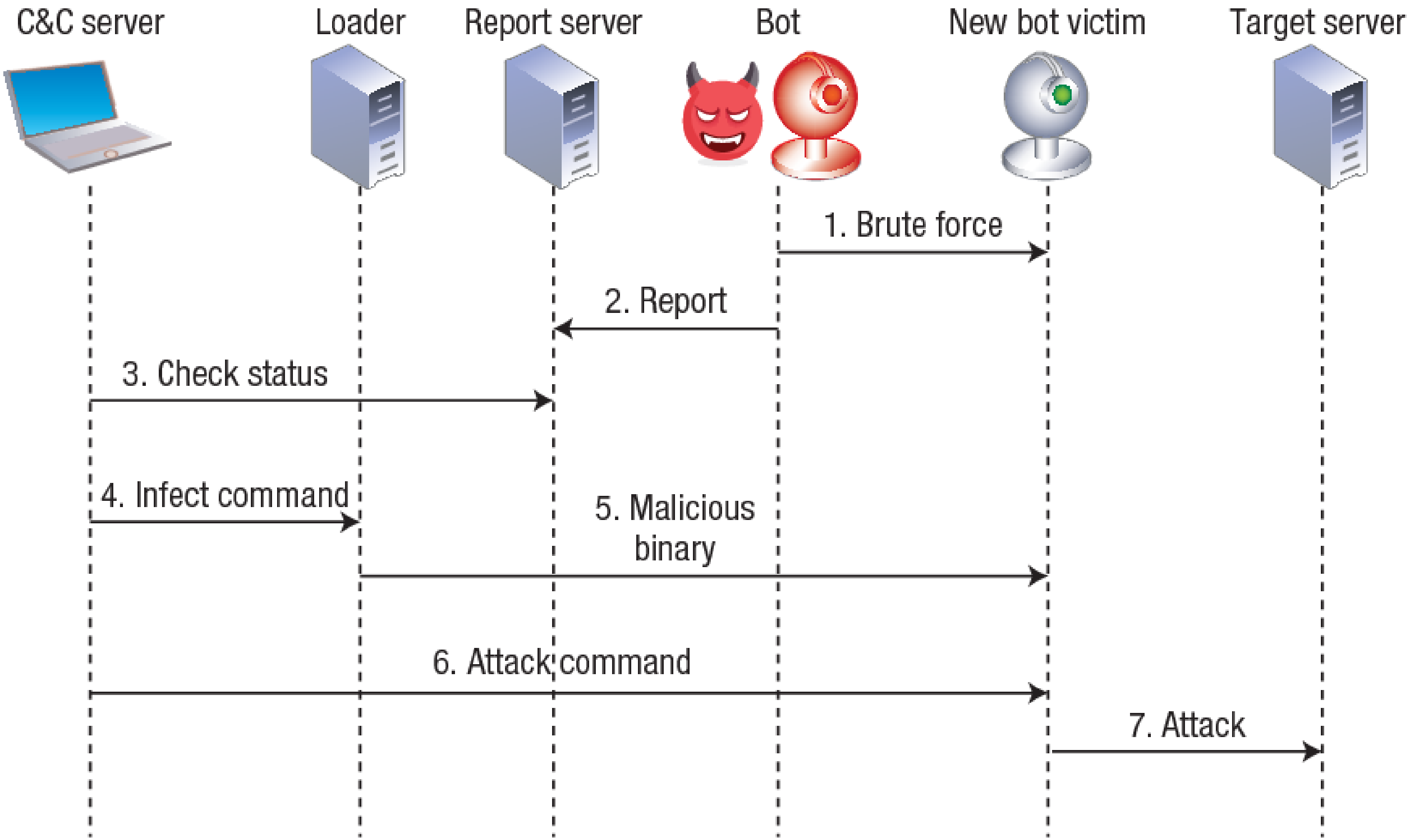
- Due to the increased complexity
- Due to every reducing time-to-market, or cost

Security in computing systems: Complex problems

Networks allow novel attack mechanisms

- "Anonymous" attacks from any place in the planet
- Fast spread across geographical boundaries
- Exploitation of insecure hosts and applications

- **Attackers can build complex attack chains**
  - First exploration
  - Lateral movement
  - Exfiltration
  - Check: https://attack.mitre.org/matrices/enterprise/



Mirai botnet operation and communication.
Mirai causes a distributed denial of service (DDoS) to a set of target servers by constantly propagating to weakly configured Internet of Things (IoT) devices.

source: Kolias, Constantinos et al. “DDoS in the IoT: Mirai and Other Botnets.” Computer 50 (2017): 80-84.

Security in computing systems: Complex problems

Users are mostly unaware of the risks

- They do not know the problems,
- ... the impact
- ... the good practices
- .... nor the solutions

Users are mostly careless

- Because they take risks
- Do not care (Do not have/identify any responsability
- Do not estimate the risk correctly

Main vulnerability sources

Hostile applications or bugs in applications

- Rootkits: Insert elements in the operating system
- Worms: Software programs controlled by an attacker
- Virus: Pieces of code that infect other files (ex, macros)

Users

- Ignorant or careless
  - telnet vs. ssh, IMAP vs. IMAPS, HTTP vs HTTPS
  - False sense of security (I have an anti-virus, so I'm protected!)
- Hostile

Defective administration

- Default configuration is seldom the most secure
- Security restriction vs flexible operation
- Exceptions to individuals

Communication over uncontrolled/unknown network links

- Public hotspots, campus networks, hostile governments

Security level (of a computer)

Defined by:

- Available security policies
- Correctness and effectiveness of their specification/implementation

Evaluation criteria

- NCSC Trusted Computer System Evaluation Criteria (TCSEC, Orange Book)
  - Classes: **D**, **C** (1, 2), **B** (1, 2, 3) e **A** (1)
  - D: insecure (minimum protection level)
  - A1: most secure
    - very demanding and expensive protection policies
    - formal validation of the specification with highly supervised implementation
- EC Information Technology Security Evaluation Criteria (ITSEC)
  - Levels: **E1** to **E6**
    - Level of formal specification
    - Correctness of the implementation

Case Study: NCSC TCSEC (C)

C1 – Discretionary Security Protection

- Identification and authentication
- Separation of users and data
- Discretionary Access Control (DAC) capable of enforcing access limitations on an individual basis
- Required System Documentation and user manuals

C2 – Controlled Access Protection

- More finely grained DAC
- Individual accountability through login procedures
- Audit trails
- Object reuse
- Resource isolation

Case Study: NCSC TCSEC (C)

Object Reuse Policy:

- All authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects.
- No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system.

Storage object: An object that supports both read and write accesses.

Security policies for distributed systems (some)

Must encompass several hosts and networks

Security Domains

- Definition of the set of hosts and networks of the domain
- Definition of the set of accepted/authorized users
- Definition of the set of accepted/not accepted activities

Security Gateways

- Definition of the set of allowed in-out interactions

Security Controls

- Define the points for future auditing

Perimeter defense

(minimal defense, but frequently not sufficient)

Perimeter Defense

Protection against external attackers

- Internet
- Foreign users
- Other organizations

Assumes that internal users are trusted and share the same policies

- Friends, family, collaborators

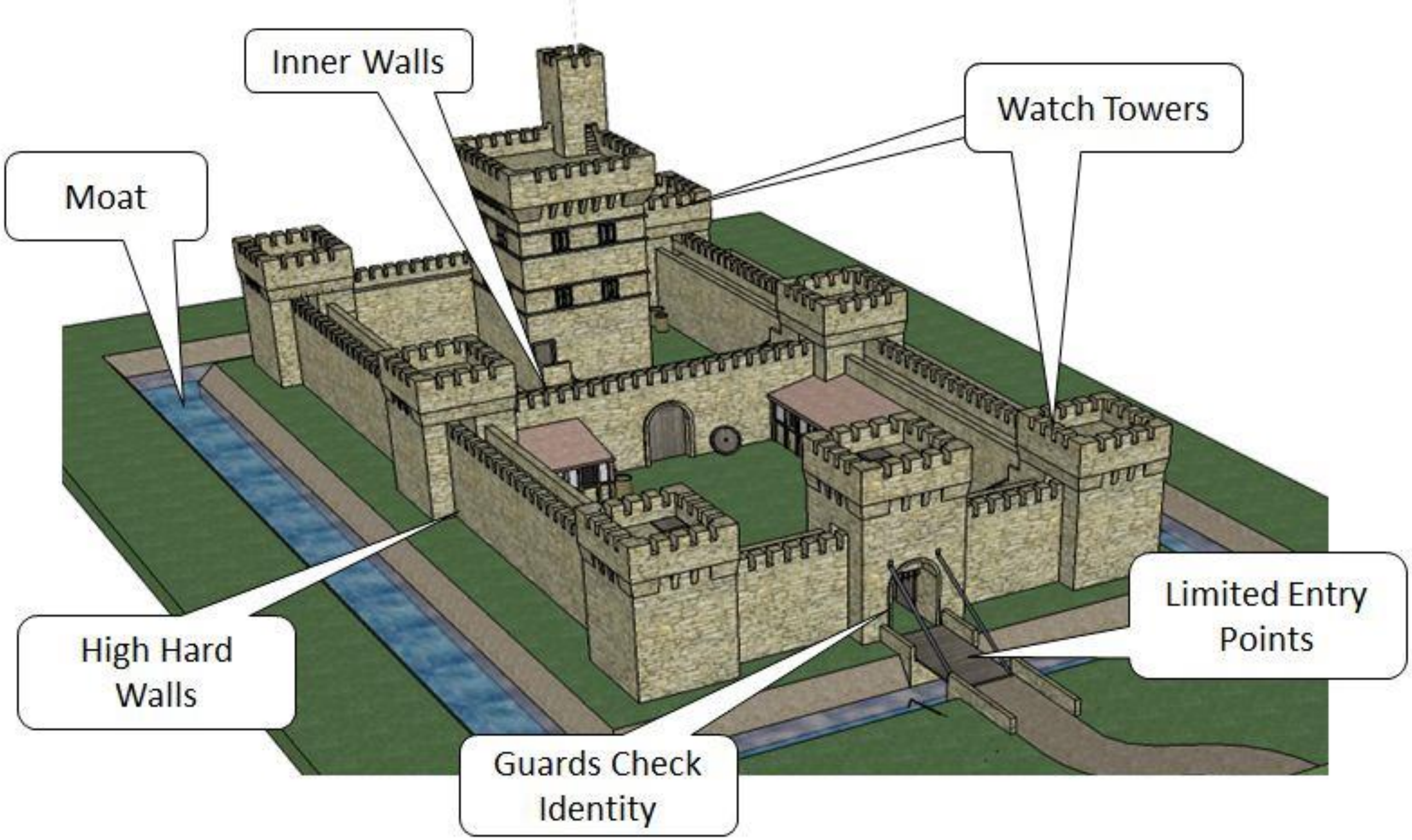
Used domestic scenarios or small offices

Limitations

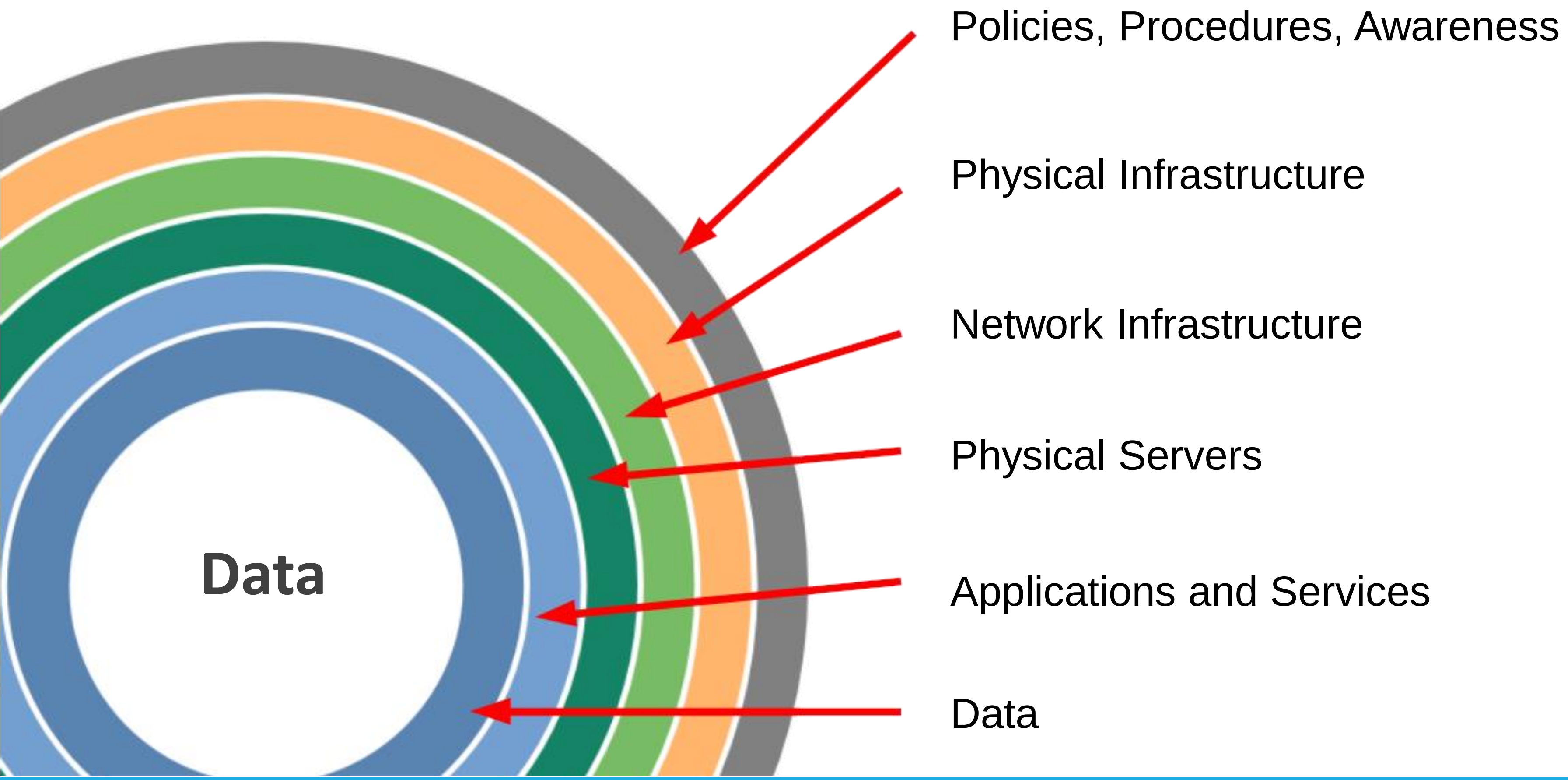
- Too simple
- Doesn’t protect against internal attackers
  - Previously trusted users
  - Attackers that acquired internal access

Defense in Depth

(with flaws, but better)



Defense in Depth



Policies, Procedures, Awareness

Physical Infrastructure

Network Infrastructure

Physical Servers

Applications and Services

Data

Mechanisms for distributed systems

Trusted Operating Systems

- Security levels, certification
- Secure execution environments for servers
- Sand-boxing / virtual machines

Firewalls & Security Appliances

- Traffic control between networks
- Monitoring (traffic load, etc.)

Secure communications / VPNs

- Secure channels over insecure, public networks
- Secure extension of organizational networks

Mechanisms for distributed systems

Authentication

- Local
- Remote (network authentication)
- Single Sign-On
- Using secrets, token, bio-metrics, device, location

Certification Authorities / PKI

- Management of public key certificates

Encryption of files and sessions

- Privacy / confidentiality of network data
- Privacy / confidentiality of long-term stored data

Mechanisms for distributed systems

Intrusion detection

- Detection of forbidden / abnormal activities
- Network-Based / Host-based

Vulnerability scanners

- Scanning for problem fixing or exploitation
- Network-based / Host-based

Penetration testing

- Vulnerability assessment
- Demo penetration attempts
- Testing of installed security mechanisms
- Assessment of badly implemented security policies

Today – Standard users

Use the same devices for all interactions

- Talk with other users
- Access leisure services and websites
- Access critical services (eg, banks)
- Work (?)

Service and system use based on a final objective

- Buy, sell, read, listen, communicate
- No or little security considerations

No training, fearless

- Bad at predicting the risk of their actions
- Consider that security issues only happen to large entities/others
  - Think they are not relevant
- With wrong base concepts
  - “Algorithms” to generate passwords, password reuse
- With no investment in security infrastructure (except an antivirus?)
  - Trust an antivirus more than anything else
- Without disaster recovery processes

Today - Companies

Focused on a business

- The product they provide
- Financials
- Human Resources

Interact with security aspects as required

- To fulfil existing norms and regulations
  - RGPD, sector specific regulation
- May have security strategies
  - From nothing to an extreme focus in “security driven culture”
- May provide training and invest in security
- May have frequent audits
- May even have a CISO: Chief Information Security Officer

Category	Basic Organizations	Progressing Organizations	Advanced Organizations
Philosophy	Cybersecurity is a "necessary evil."	Cybersecurity must be more integrated into the business	Cybersecurity is part of the culture.
People	CISO reports to IT. Small security team with minimal skills. High burnout rate and turnover.	CISO reports to COO or other non-IT manager. Larger security team with some autonomy from IT. Remain overworked, understaffed, and under-skilled.	CISO reports to CEO and is active with the board. CISO considered a business executive. Large, well-organized staff with good work environment. Skills and staff problems persist due to the global cybersecurity skills shortage.
Process	Informal and ad-hoc. Subservient to IT.	Better coordination with IT but processes remain informal, manual, and dependent upon individual contributors.	Documented and formal with an eye toward more scale and automation.
Technology	Elementary security technologies with simple configurations. De-centralized security organization with limited coordination across functions. Focus on prevention and regulatory compliance.	More advanced use of security technologies and adoption of new tools for incident detection and security analytics.	Building an enterprise security technology architecture. Focus on incident prevention, detection, and response. Adding elements of identity management and data security to deal with cloud and mobile computing security.

Source: Enterprise Strategy Group, 2014.

Today - Nations

Focused on national sovereignty

- Acting independently or as part of strategic groups (e.g, NATO)

Have entities dedicated to cybersecurity

- Cyber Defense
  - Part of their defense forces (e.g. army)
  - Ad-hoc entities hired or shadow
- Cyber resilience of the nation entities
  - Utilities, university, companies, citizens
- Criminal Investigation

May have offensive actions against other entities

- Companies, individuals, groups, other nations
- Cold war alike, totalitarian governments, sovereignty

Today – Offensive Groups

Will conduct attack against any other entity

- In ad-hoc or coordinated manner
- May have great amount of funds available
  - By economic groups or nations
- May act as a collective without strict coordination

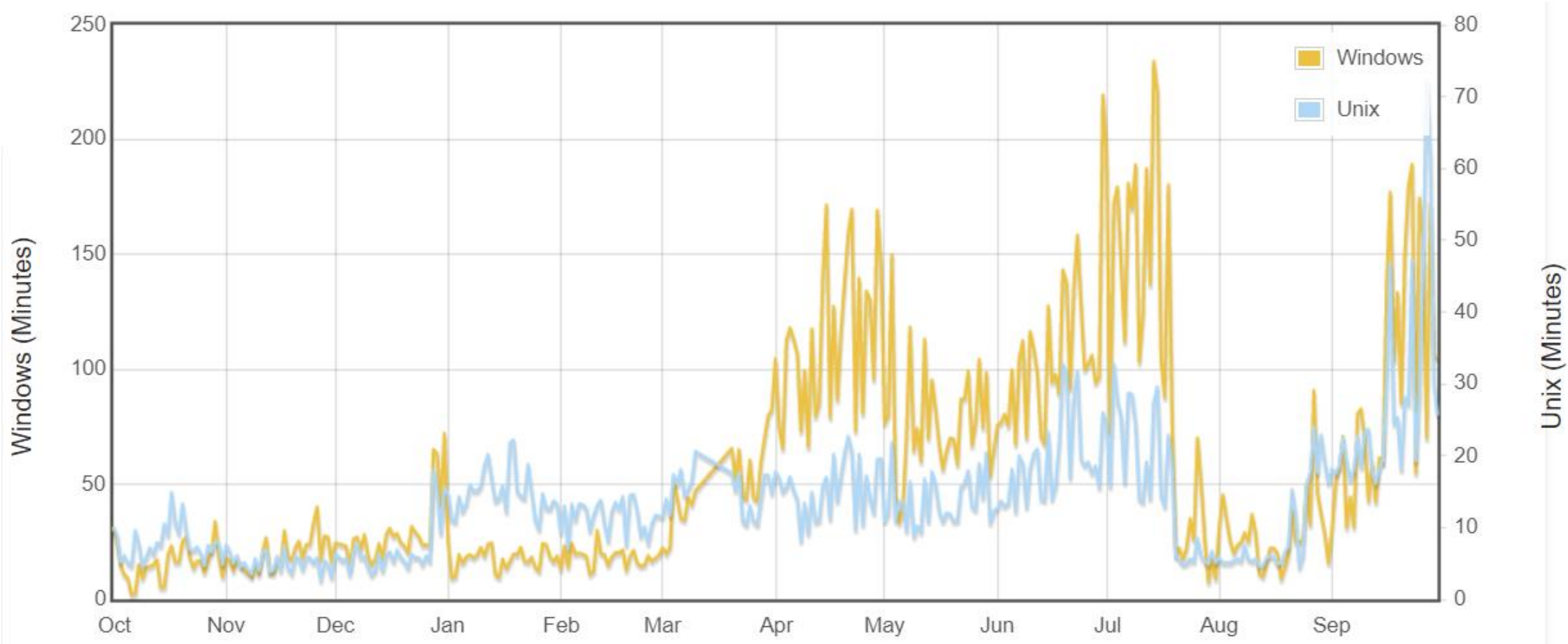
Sometimes considered Advanced Persistent Threats

- Will develop attacks over the course of months or even years
- May keep control of an entity without being discovered

Motivations are many

- Hacktivism: Lulzsec, Anonymous, Antisec, (4chan?)
- Economic competition
- National Interest: APTs
- Crime: APTs, ransomware
- Cyberwar

Mean Survival Time
Oct 2020 – Oct 2021
(http://isc.sans.org/survivaltime.html)



Defender will constantly spend resources in security

Attacker only needs to be successful once

- Attackers can screen for victims with low effort and in an automated manner

Cyber Higiene

Basic Controls that can be applied by any entity

- Individual Subjects
- Companies

Focus on the basic CIA properties

- And privacy for subjects

Violation of these principles frequently have an high impact

- Therefore, they are frequently exploited by offsec groups

Check: https://www.cncs.gov.pt/pt/curso-cidadao-ciberseguro/

Cyber Higiene - Passwords

Sequence of textual characters used to validate an identity

Impact: stealing passwords leads to identity theft

- May have social, legal, monetary cost

Cyber Higiene - Passwords

Use authentication with user generated passwords

Never reuse the same passwords

- Reuse will allow an attacker to compromise one system, obtain the password and then use it in another system

Use large complex passwords

- Simple passwords can be guessed by an attacker
- Btw… that nice algorithms based on the name of your pet plus a number is not safe!

Use a password manager

- They will generate random and unique passwords

Monitor exposure: https://haveibeenpwned.com/

Cyber Higiene - Updates

Updates created by the vendor to correct potentially explorable problems

Impact: system and data compromisse

- Data loss, hardware damage, extortion (ransomware)
- Use of the device as a pivot for other attacks

Cyber Higiene - Updates

Activate automatic updates

Install updates as quick as possible

- Sometimes, a delay of a couple of hours is critical
- Corrections may arrive after the attack was conducted

Verify if updates are actually active

- Some malware will compromise updates

Do not update from manual sources

- E.g. Android ROMs from the communication
- Firmware from other regions
  - Legal framework may be different (e.g. China vs Europe)

Do not use devices that lack updates

Cyber Higiene - Files

Malware will frequently disseminate through files that are open and/or executed

Impact: execution of untrusted code, compromising the system

- Data loss, hardware damage, extortion (ransomware)

Cyber Higiene - Files

Check ALL files that enter a system

Do not open files from strange origins

- Executables may contain malicious code
- Documents may also have malicious code
- Images/Videos may exploit vulnerabilities

Verify if the extension makes sense

- A common technique consists of disguising an executable as an image or word document

Cyber Higiene - Files

Check ALL files that enter a system

Do not open files from strange origins

- Executables may contain malicious code
- Documents may also have malicious code
- Images/Videos may exploit vulnerabilities

Verify if the extension makes sense

- A common technique consists of disguising an executable as an image or word document

Cyber Higiene – Anti Virus

Tools that check the system, looking for applications conducting malicious actions

Impact: Execution of malware will compromise the system

- Data loss, hardware damage, extortion (ransomware)

Cyber Higiene – Anti Virus

Install an antivirus product

- MS Windows already has an antivirus preinstalled

Keep the antivirus enabled!

- It is useless if disabled

Update the antivirus definition files

- Antivirus will only detect threats as stated in their definition files
- Most recent virus will not be detected
- No antivirus is foolproof

Cyber Higiene – Backups

Copies of data that are kept in a safe place

Impact: lack of backups will imply data loss

- Or vulnerability to extortion…

Cyber Higiene – Backups

Keep copies of data in some place

- A copy is a duplicate of something
- An external hard drive to keep data only works are a backup if there is a copy in another system!

Preform periodic copies

- In order to minimize the impact

Check copies

- Ensuring that the backup is effective

Encrypt and secure copies

- Ensuring that the attacker will not gain advantage by having access to the backups
- Achieving resilience against more disasters: Theft, fire, flood

Cyber Higiene – Behavior

Act according to security principals and the estimated risk

Impact: subversion of any process or system

- What is an anti virus worth if the users disable it?
- What are updates for if users postpone them?

Cyber Higiene – Behavior

Segment usage profiles

- Have devices for personal usage and devices for work
- … or at least segment using virtual machines or virtual spaces

Dot not access potentially dangerous places

- Remember: antivirus only work against known and popular threats

Do not open files in the email, Flash drivers… without scanning them first

Do not click on links received by email

- Phishing attacks aim at confusing users to exploit browser or steal data

And never introduce private information in websites