

Security and Risk: Quick Summary

Gabriel Rovesti

Contents

1. Disclaimer	3
2. M1.1 - Basic concepts	4
2.1. Key terms	4
2.2. Cybersecurity objectives and dilemmas	4
2.3. Risk assessment	5
2.4. Governance structure terms	6
2.5. Standards and Best Practices documents	6
2.6. Standard of Good Practice (SOGP)	7
2.7. ISO/IEC 27000	7
2.8. ISO/IEC 27001	8
2.9. ISO/IEC 27002	8
2.10. IEC 62443	8
3. M1.2 - Basic concepts	11
3.1. NIST Cybersecurity Framework	11
3.2. MITRE Att&ck	12
3.3. National Framework for Cybersecurity	13
3.4. OWASP	14
3.5. Cybersecurity Management Process	14
4. M2.1 - Planning for Cybersecurity	15
4.1. Security governance	15
4.2. Strategic planning	17
4.3. Organizational structure	17
4.4. Security report	18
4.5. Security roles	18
4.6. Security policies	19
4.7. Security approach and framework	19
4.8. Security direction, evaluation and best practices	20
4.9. Risk assessment	20
4.10. Risk management	22
4.11. Asset identification	22
4.12. Threat types and identification	23
4.13. Control identification	24
4.14. Vulnerability identification and classification	25
4.15. Risk assessment approaches	25
4.16. Factor Analysis of Information Risk (FAIR)	27
4.17. Likelihood assessment	28
4.18. Impact assessment	28
4.19. Risk evaluation and treatment	29
5. M2.2 - Planning for Cybersecurity	31
5.1. Threat modelling	31
5.2. STRIDE (Threat Modelling)	31

5.3. DREAD (Risk Classification)	32
5.4. OCTAVE (Risk Management)	33
5.5. Security management	33
6. M3.1 - Cybersecurity Operations and Management	35
6.1. Human Resource Security	35
6.2. Hiring process	35
6.3. During and after employment	35
6.4. Security awareness	35
6.5. Hardware management	36
6.6. Office equipment	36
6.7. Equipment disposal	37
6.8. Industrial Control System (ICS) security	37
6.9. Mobile device security	38
7. M3.2 - Cybersecurity Operations and Management	39
7.1. System access and its functions	39
7.2. Authentication factors and means	39
7.3. Authenticators	39
7.4. Vulnerability of a password	39
7.5. Hashed password and salt	40
7.6. Password cracking	40
7.7. Password file access control	40
7.8. Possession-based authentication	40
7.9. Biometric authentication	41
7.10. Access control	41
7.11. Access control elements	41
7.12. Access control policies	41
7.13. Access control structures	42
7.14. Customer access	42
8. M3.3 - Cybersecurity Operations and Management	43
8.1. Computer Security Incident Response Team (CSIRT)	43
8.2. Security Incidents	43
8.3. Managing, detecting and responding to incidents	43
8.4. Malware and protection	44
8.5. Intrusion Detection	44
8.6. Data Loss Prevention	45

1. Disclaimer

Given the course has so much content, a complete notes file is available, basically an extended transcript of file, here I will give a full revised short summary to avoid the unreadable sets of slides of this course. Hope this could be useful, between all of my other works.

2. M1.1 - Basic concepts

2.1. Key terms

Cyberspace

- Consists of:
 - artifacts
 - information
 - interconnections

CyBOK - Cyber Security Body of Knowledge

- It aims to codify the foundational and generally recognised knowledge on cyber security
- It's grouped into five broad categories

Cybersecurity

- Collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches used to protect environment and assets
- It's grouped into five broad categories

Asset

- Data contained inside an information system or a system capability
- Generally hardware, software, etc.

Risk

- Possibility that human actions may lead to consequences or have an impact to humans value
- Estimate the likelihood of events, measuring their impact

Threat

- A potential for violation of security, exploiting a vulnerability and getting danger

Vulnerability

- A flaw or weakness in a system's design that can be exploited violating security policies

Information security

- Preservation of confidentiality, integrity and availability of information
- In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability

2.2. Cybersecurity objectives and dilemmas

Objectives:

- *Confidentiality*: property of data not disclosed to unauthorized entities
- *Integrity*: Property of data not been changed
- *Availability*: Resource or property being accessible or usable upon demand
- *Authenticity*: Property of being genuine and being able to verify that users are who they say they are
- *Accountability*: Property ensuring that the actions of a system entity may be traced uniquely to that entity, which can then be held responsible for its actions

Dilemmas:

- Scale and Complexity of Cyberspace
- Nature of Threat
- User needs vs Security implementation
- Difficulty estimating costs and benefits

2.3. Risk assessment

Risk:

- is the possibility that human actions or events lead to consequences that have an impact on what humans value

Many processes regard risk:

- Risk assessment
 - a process of collating observations and perceptions of the world that can be justified by logical reasoning or comparisons with actual outcomes
- Risk management
 - the process of developing and evaluating options to address the risks in a manner that is agreeable to people whose values may be impacted
- Risk governance
 - set of ongoing processes and principles that aims to ensure an awareness and education of the risks faced when certain actions occur, and to inspire a sense of responsibility

Risk assessment:

- has to use analytic and structured processes to capture the potential for desirable and undesirable events, and a measure of the likely outcomes and impact
- it involves reviewing information collected as part of the risk (and concern) assessments
- this information forms the basis of decisions leading

It's important for many reasons:

- Identification and, if possible, estimation of hazard

- Assessment of exposure and/or vulnerability
- Estimation of risk combining the likelihood and severity (impact)
- Handle all cases inside the cyberspace
- Number of global standards aiming to formalize that

2.4. Governance structure terms

- Standards
 - Mandatory requirements regarding processes, actions and configurations that are designed to satisfy Control Objectives
- Control Objectives
 - Targets or conditions to be met
- Policies
 - High-level statements of management intent from an organization's executive leadership that are designed to influence decisions and guide the organization to achieve the desired outcomes
 - Policies are enforced by standards and further implemented by procedures
- Procedures
 - Documented set of steps necessary to perform a specific task or process in conformance with an applicable standard
 - They help address the question of how the organization actually operationalizes a policy, standard or control
- Guidelines
 - Recommended practices that are based on industry-recognized secure practices
 - We apply the guidelines where we cannot apply the standard

2.5. Standards and Best Practices documents

A number of organizations, based on wide professional input, have developed best practices types of documents as well as standards for implementing and evaluating cybersecurity (just to quote here)

- National Institute of Standards and Technology (NIST)
- International Organization for Standardization (ISO)
- International Electrotechnical Commission (IEC)
- International Telecommunication Union Telecommunication Standardization Sector (ITU-T)
- Internet Society (ISOC)
- Internet Engineering Task Force (IETF)

- International Society of Automation (ISA)
- Information Security Forum (ISF)
- Control Objectives for Information and Related Technology (COBIT) for information security issued by Information Systems Audit and Control Association (ISACA)
- Center for Internet Security (CIS)

2.6. Standard of Good Practice (SOGP)

A security policy:

- is a set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources
- it includes associated responsibilities, security principles followed by all relevant individuals
- it applies to all employees
- has many different types (e.g., access control, network security, etc.)

SOGP:

- is issued by the Information Security Forum (ISF). The goal of the ISF is the development of best practice methodologies, processes, and solutions
- is a business-focused comprehensive guide to identifying and managing information security risks
- is based on research projects and input from ISF members as well as analysis of the leading standards on cybersecurity
- is of particular interest to business manager or chief information security officers
- has several categories broken down into several topics, consistent with the structure of the standards
- has 3 main activities:
 - planning for cybersecurity
 - managing the cybersecurity function
 - security assessment

2.7. ISO/IEC 27000

The ISO and IEC have developed a growing family of standards in the ISO/IEC 27000 series that deal with ISMS - Information Security Management System.

- Information security management system (ISMS) consists of the policies, procedures, guidelines with the scope of protecting its information assets
- Systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives

- Based upon a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks

ISO 27000 suite has principles which contribute to the successful implementation of an ISMS:

- raising awareness
- assigning responsibilities
- incorporating security
- ensuring a comprehensive approach
- preventing and detecting

It is composed by 4 categories:

- Overview and vocabulary
- Requirements
- Guidelines
- Sector-specific guidelines

2.8. ISO/IEC 27001

ISO 27001 is a management standard initially designed for the certification of organizations. It's composed by:

- Certification Audit
- Qualified individuals to develop and maintain an ISMS
- Obtaining certifications (third-party assessments) to enhance the value
- It can be mapped easily to meet ISF SOGP

2.9. ISO/IEC 27002

It provides the broadest treatment of ISMS topics in the ISO 27000 series and allows for selection of controls for ISMS.

- Allows to choose the controls needed to satisfy ISMS requirements
- Grants specific security controls to protect confidentiality, integrity and availability of information
- Uses a checklist of topics to map ISF SOGP correctly

2.10. IEC 62443

IEC 62443 deals with security of the industrial control system, popularly known as the Industrial Automation and Control System (IACS)

- It ensures that a product supplier, integrator or an asset owner follows an efficient method for secured process with a key aspect on safety of the personnel

It's divided into four *parts*:

- General: basic terminologies and concepts
- Policies: required to implement a cybersec system
- System: describes security requirements for systems
- Component: same but for components

Different from normal IT systems given they are rarely patched or changed, but time dependency here is critical, less awareness overall.

It defines also some *roles*:

- product supplier
 - responsible for development and testing of the control system, embedded device and host device
- system integrator
 - responsible for the integration and starting up, with conformance to specific security levels
- asset owner
 - responsible for operational and maintenance capabilities

Let's list some *concepts*:

- Defense in depth
 - Layered security mechanism that enhances security of the whole system
 - Layers to be found here: data, application, host, internal network, perimeter, physical, policies
 - If one layer gets affected, the others will work anyway
- Security zones
 - Physical or logical groupings of assets that share common security requirements
- Conduits
 - Special type of security zone that groups communications that can be logically organized into information flows within and also external to a zone
 - They control access to the zone

Finally, its *security levels*:

- It focuses on the zones, making decisions on the use of countermeasures and can be applied to Defense in Depth
- Different ones to list:
 - SL1 = Prevents eavesdropping
 - SL2 = Prevents unauthorized disclosure

- SL3 = Prevents information to an entity searching for it using sophisticated means moderate resources
- SL4 = Prevents unauthorized disclosure of information with extended resources

And also *maturity levels*:

- They define the benchmarks
- They are required to identify the maturity level associated with the implementation of each requirement
- Different ones to list:
 - ML1 = Initial
 - ML2 = Managed
 - ML3 = Defined
 - ML4 = Improved

3. M1.2 - Basic concepts

3.1. NIST Cybersecurity Framework

NIST is a U.S. federal agency that deals with measurement science, standards, and technology

- Their publications have a worldwide impact and bring an excellent resource on the field, providing prescriptive standards, tutorials and surveys defining for each countermeasures to act against threats
- The NIST Computer Security Resource Center (CSRC) is the source of a vast collection of documents that are widely used in the industry
- In response to the growing number of cyber intrusions at U.S. federal agencies, directed the NIST to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure
- The framework is a collection of best practices that improve efficiency and protect components, used for nongovernment organizations, with the clear goal of continuous improvement while managing supply chain risk

Composed by three *parts*:

- *Core*: cybersecurity activities, desired outcomes, and applicable references
- *Implementation tiers*: Provide context on how an organization views cybersecurity risk
- *Profiles*: Represents the outcomes based on business needs, categories and subcategories

An organization can use the CSF core, profiles, and tiers with the supplementary resources to understand, assess, prioritize, and communicate cybersecurity risks:

- Understand and assess gaps of the organization
- Prioritize actions for managing risks
- Communicate with a clear language inside/outside the organization the risks

Composed by six *key functions*, each divided into specific categories and subcategories, each with sections, practices and standards:

- *Govern*
- *Identify*
- *Protect*
- *Detect*
- *Respond*
- *Recover*

Composed by *tiers*, which define the priority and the level of commitment:

- *Tier 1: Partial*

- *Tier 2: Risk informed*
- *Tier 3: Repeatable*
- *Tier 4: Adaptive*

Composed by *profiles*, selection of categories and subcategories which define a target profile and enable management, needing for maintenance and guidelines with concrete descriptions.

Some important documents of NIST to quote:

- NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations (this in particular, quoted by many slides sets)
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems (2006)
- NIST SP 800-12, Introduction to Information Security, (2017)
- NIST SP 800-55, Performance Measurement Guide for Information Security (2008)
- SP 800-100, Information Security Handbook: A Guide for Managers (2006)

3.2. MITRE Att&ck

The MITRE Corporation is a private, not-for-profit company to provide engineering and technical guidance for the federal government and works in the public interest across all safety and cybersecurity fields.

MITRE started ATT&CK in 2013 to document common tactics, techniques, and procedures (TTPs) that advanced persistent threats use against Windows enterprise networks.

- This is an open framework for implementing cybersecurity detection and response programs
- It's available free of charge and includes a global knowledge base of adversarial tactics, techniques, and procedures (TTPs) based on real-world observations
- ATT&CK mimics the behaviour of real-life attackers, helping IT, security, and compliance organizations efficiently identify security gaps, evaluate risks, and eliminate vulnerabilities
 - Common taxonomy = same language
 - Database = tracking of activities and threat actors
- ATT&CK is largely a knowledge base of adversarial techniques, which focus isn't on the tools and malware but on how they interact, organizing a collection of tactics to efficiently detect and isolate threats
 - Tactics = Why to perform an action & what the adversary is trying to do
 - Techniques = How adversaries achieve their actions

This framework to address four main issues:

- Adversary behaviours: adversary tactics allowing to develop analytics
- Lifecycle models that didn't fit inside existing adversary lifecycle

- Applicability to real environments looking at observed incidents
- Common taxonomy across different types of adversary groups

We can even make a MITRE Att&ck Decomposition in case of enterprises:

- PRE-ATT&CK framework focusses on the preceding preparation phases. Preventing an attack is much cheaper
- A whole matrix is available, describing tactics and procedure examples

3.3. National Framework for Cybersecurity

The National Framework for Cybersecurity and Data Protection (“Framework”) represents a tool for measuring an organization’s security posture in terms of maturity and completion of activities aimed at reducing cyber risk.

- This is in use in Italy, complying with the GDPR and taking up elements from NIST Framework
- Some key principles:
 - Core
 - Controls
 - Informative references
 - Priorities levels
 - Maturity levels
 - Contextualization
 - Prototype of contextualization
- The following is for the framework methodology:
 - Phase 1 - Contextualization
 - Contextualizing the Framework to the reality of interest, achieving a Target Profile and desired reference to carry out assessments
 - Phase 2 - Measurement
 - In this second phase, the organization’s current cyber security posture is identified, done through interviews with relevant individuals
 - Phase 3 - Evaluation
 - The results of the measurement phase are evaluated according to several possible scopes. This operation allows to calculate, starting from the values of coverage and maturity of each subcategory, metrics of interest for the scope itself

The output of the evaluation phase, and therefore the result of the entire assessment, is expressed through the metrics defined in the Framework, aggregated according to different criteria and projected onto different *scopes*, interpreting assessment results:

- Scope framework = assess how far current posture is set by Target Profile
- Risk management scope = how consistent the posture is with risk mitigation
- Compliance scope = align cybersec requirements to organization scopes

3.4. OWASP

Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software, being a source for devs and technologies to secure the web. Some documents to list here:

- OWASP Top 10
 - Standard awareness document for developers and web application security, representing broad consensus about most critical security risks to web apps
 - Risks are ranked based on frequency, severity and impact
- OWASP Cheat Sheet
 - Created to provide a set of simple good practice guides for application developers and defenders to follow
- OWASP Mobile Top 10
 - Consists of the most critical security risks to mobile applications. It represents a broad consensus about the most critical security risks to mobile applications
- OWASP Mobile Application Security (MAS)
 - It provides a security standard for mobile apps (OWASP MASVS) and a comprehensive testing guide (OWASP MASTG)
 - It covers the processes, techniques, and tools used during a mobile app security test, as well as an exhaustive set of test cases that enables testers to deliver consistent and complete results
 - There is a checklist - OWASP Mobile Application Security Checklist - containing links to the MASTG test case for each MASVS requirement, see if they are compliant
- OWASP Risk Rating Methodology
 - Attackers can take a variety of routes through your application to cause damage
 - Procedure of following a path of several steps for the classification of threats: identifying, estimating, determining, deciding and customizing

3.5. Cybersecurity Management Process

- An essential characteristic of cybersecurity provision is that it is not a single end that is attained but an ongoing process
- The goal of effective cybersecurity is constantly receding as management makes an effort to keep up with changes in the cyberspace ecosystem

- Two cyclic processes working at an executive level (organizational) and at a business level (infra-structural)

4. M2.1 - Planning for Cybersecurity

4.1. Security governance

Governance allows to:

- Establish policies and continuous monitoring of their proper implementation
- Includes the mechanisms required to balance the powers of the members (with the associated accountability) and their primary duty of enhancing the prosperity and viability

Security governance:

- is the process of establishing and maintaining a framework and supporting management structure and processes
 - also, the system by which activities are directed and controlled
- allows to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls
- wants to provide assignment of responsibility, all in an effort to manage risk

To better understand the role of security governance, it is useful to distinguish between *security*:

- *governance*
 - process that develops the security program that adequately meets the strategic needs of the business
 - it communicates the mission priorities and overall risk tolerance
- *management*
 - supervision and making of decisions necessary to achieve business objectives through the protection of the organization's information assets
 - uses information as inputs into the process that realizes the security program and defines the profiles
- *implementation/operations*
 - implementation, deployment and ongoing operation of security controls defined within a cybersecurity framework
 - it integrates into the lifecycle and monitors security performance continuously

The *security program* is the management, operational, and technical aspects of protecting information and information systems

- It consists of policies, procedures, and management structure and mechanism for coordinating security activity

In an ISMS:

- reports help to define the threat and level of risk
- standards and best practices provide guidance on managing risk
- feedback help improve the effectiveness of policies and technical mechanisms

Security governance establishes different principles:

- ITU-T X.1054 establishes as a key objective “the alignment of information security objectives and strategy with overall business objectives and strategy”
- We can list 6 principles:
 1. Establish organization wide information security
 2. Adopt a risk-based approach
 3. Set the direction of investment decisions
 4. Ensure conformance with internal and external requirements
 5. Promote a security-positive environment for all stakeholders
 6. Review performance in relation to business outcomes

Given IT as a whole represent systems which have interest in the context of a business or other enterprise, having interest or concern for others:

- The IT Governance Institute defines five basic outcomes of information security governance that lead to successful integration of information security with the organization’s mission
 - Strategic alignment
 - Risk management
 - Resource management
 - Value delivery
 - Performance measurement

NIST SP 800-100 lists the following key activities, or *components* that constitute effective security governance:

- Strategic planning
- Organizational structure
- Establishment of roles and responsibilities
- Integration with the enterprise architecture
- Documentation of security objectives in policies and guidance

4.2. Strategic planning

Let's define three hierarchically related aspects of strategic planning:

- Enterprise strategic planning
 - Involves defining long-term goals and objectives for an organization and the development of plans to achieve, with ongoing oversight
- IT strategic planning
 - Considering development and changes to involve new arrangements with outside providers and use of mobile devices
 - Activities may create unintended barriers to flexibility, introducing risk. IT management must be guarded against that
 - There is a whole process for this one:
 - Two to five years business and technology outlook: look at major trends
 - Strategic deep dive: identify a number of high-impact areas to inform the overall planning process
 - Current-state assessment: analysis of current state of all IT-related systems and policies, bringing sets of recommendations
 - Imperatives, roadmaps and finances: discussion of strategic objectives and a budget for investment plans, reflecting the organization priorities
 - Governance process and decision making: approval of budget, information taken from preceding phases used to guide the governance process
 - Regular reviews: monthly-based reviews culminating in a year-end assessment, continuing to improve into following years, hence modifying inputs and processes
- Information security strategic planning
 - Aligned with enterprise and IT strategic planning
 - A *strategic plan* is a document used to communicate, within the organization, the organization's goals, the actions needed to achieve those goals, and all the other critical elements developed during planning exercises
 - This should be approved by executives and committees, while regularly reviewed

4.3. Organizational structure

The organizational structure to deal with cybersecurity depends on the size of the organization, its type, and the organization's degree of dependence on IT.

- The Information Security Governance Framework includes the governing cycle to direct, monitor, and evaluate the ISMS

- This cycle is in accordance with ISO 27001 that the organization shall establish, implement, maintain, and continually improve an ISMS
- The evaluation function triggers communication with stakeholders in the form of a report, both for accountability and corporate values respect

It has a full cycle to respect:

- Direct: leading strategies, developing a security policy
- Monitor: performances measured with metrics
- Evaluate: assessing and verifying the results of monitoring
- Communicate: reporting stakeholders' requirements

4.4. Security report

Reporting enables stakeholders to ensure that information security is being managed effectively, including policies, evaluation and responses to a system.

- Includes costs and benefits
- Value of inventory and information assets
- Economic value of security and information assets
- Risk reduction

A report should include:

- Introduction
- Statis
- Updates
- Significant issues (if any)
- Decisions required (if any)

4.5. Security roles

We can have different roles to consider:

- C-level
 - Refers to high-ranking executives in an organization
 - Officers who hold C-level positions set the company's strategy, make high-stakes decisions, and ensure that the day-to-day operations align with fulfilling the company's strategic goals
- Chief executive officer (CEO)
 - Responsible for the success or failure of the organization
- Chief operating officer (COO)

- Generally second in command to the CEO. Oversees the organization's day-to-day operations on behalf of the CEO, creating the policies and strategies
- Chief information officer (CIO)
 - In charge of IT strategy and the computer, network, and third-party
- Chief security officer (CSO)/Chief information security officer (CISO)
 - Tasked with ensuring data and systems security
- Chief risk officer (CRO)
 - Charged with assessing and mitigating significant competitive, regulatory, and technological threats to an enterprise's capital and earnings
- Chief privacy officer (CPO)
 - Charged with developing and implementing policies designed to protect employee

It is important to have a structure with clear responsibilities but also metrics to measure the goals

4.6. Security policies

NIST SP 800-53 rev.5 "Security and Privacy Controls for Information Systems and Organizations" defines an information security policy as: "an aggregate of directives, rules, and practices that prescribes how an organization manages, protects, and distributes information".

- It is an essential component of security governance, providing a concrete expression of the security goals and objectives
- The policies, together with guidance documents on the implementation of the policies, are put into practice through the appropriate selection of controls to mitigate identified risks
- The policies and guidance need to cover information security roles and responsibilities, a baseline of required security controls, and guidelines for rules of behavior for all users of data and IT assets

4.7. Security approach and framework

Effective security governance requires the development of a framework, which is a structured approach for overseeing and managing risk for an enterprise.

- The implementation and ongoing use of the governance framework enables the organization's governing body to set clear direction for and demonstrate their commitment to information security and risk management
- The definition, monitoring, and maintenance of a security governance framework involves a number of tasks:
 - Appoint a single executive to be ultimately responsible for security governance
 - Decide and communicate to top executives the objectives of the security governance framework
 - Ensure integration of the security architecture with the enterprise architecture

- Include a process that enables the governing body to evaluate the operation of the information security strategy
- Regularly review the organization's risk willingness to ensure that it is appropriate for the current environment in which the organization operates
- Formally approve the information security strategy, policy, and architecture

4.8. Security direction, evaluation and best practices

A governing body is responsible for ensuring that there is effective security direction.

- SOGP recommends that effective security direction be provided by a combination of a single individual responsible for information security supported by a governing body
- The single individual is a CISO or equivalent implementing security approach
- The SOGP also recommends that the governing body include the CISO and have a mission to support the CISO
- Other members of the governing body could include human resources
- Governing body assists in the coordination of security activities and ensuring that the CISO has the resources and authority

Those are responsible for enterprise governance and information security governance need to be open to evaluation of their efforts at governance. The metrics fall into three categories:

- Executive management support and security awareness
- Business and information security relationship
- Information protection

Security governance also enlists some best practices:

- Security Governance Framework
- Security Direction
- Information Security Strategy
- Stakeholder Value Delivery
- Information Security Assurance

4.9. Risk assessment

Risk assessment is a complex subject and a good way to begin looking at risk assessment is to consider the terminology.

- These terms are based largely on definitions in ISO 27005 "Information Security Risk Management System Implementation Guidance", but also NIST SP 800-30 "Guide for Conducting Risk Assessments"

Threats and vulnerabilities need to be considered together:

- A *threat* is an agent acting on a vulnerability produces a security violation, or breach
- A *vulnerability* is a weakness in a system's security procedures, design, implementation, or internal controls

The level of risk is a measure that an organization can use in assessing the need for and the expected cost of taking remedial action in the form of risk treatment. This is measured in *impact* on two elements:

- Asset: Develop an inventory of the organization's assets, which includes an itemization of the assets and an assigned value for each asset.
- Threat: For each asset, determine the possible threats that could reduce the value of that asset

Then, for each asset, determine the impact to the business, in terms of cost or lost value, of a threat action occurring.

There is also the *likelihood*, made up of three elements:

- Threat: For each asset, determine which threats are relevant
- Vulnerability: For each threat to an asset, determine the level of vulnerability to the threat
- Controls: Determine what security controls are currently in place to reduce the risk

Then determine how likely it is that a threat action will cause harm, based on the likelihood.

- Security Risk = Impact x Likelihood
- The level of risk is determined as the combination of the cost of the threat occurring combined with the likelihood of the threat occurring
 - This is especially important in terms of determining a budget allocation

Challenges that an organization faces in determining the level of risk fall into two categories:

- The difficulty of *estimating*
 - Four main elements:
 - Put value on assets
 - Determine the entire range of threats
 - Vulnerabilities one may not be aware of
 - Effectiveness of given controls
- The difficulty of *predicting*
 - Four main elements:
 - Change and impact on assets
 - Assess and determine effect on threats, even without complete knowledge of them
 - Changes within the organization may create unexpected vulnerabilities
 - New technologies may provide opportunities and is difficult to predict the nature of such

4.10. Risk management

NIST Cybersecurity SP 800-37 “Risk Management Framework for Information Systems and Organizations” states that:

- Risk management includes a disciplined, structured, and flexible process for organizational asset evaluation; security and privacy control selection, implementation, and assessment; system and control authorizations; and continuous monitoring
- It also includes enterprise-level activities
- It is an iterative process:
 - Assess likelihood and impact
 - Identify security controls
 - Allocate resources, roles and responsibilities
 - Monitor and evaluate risk treatment effectiveness
- Risk management for large organization use a broader framework (ISO 27005), iterative process made up of continual changes, consisting of separate activities:
 - Context establishment
 - Risk assessment
 - Risk treatment
 - Risk acceptance
 - Risk communication and consultation
 - Risk monitoring and review

4.11. Asset identification

A first step in risk assessment is to document and determine values for the organization’s assets:

- An asset is anything of value to the business
 - Key concerns are loss of a device or device malfunction
 - Availability is another key consideration taking into account disruption losses and recovery expenses
- The challenge is to develop a uniform way of documenting the assets
- The input for asset evaluation needs to be provided by owners and custodians of assets

There are different *categories* of assets:

- Hardware
 - Servers, laptops, networking and telecommunications equipment

- Key concerns are loss of a device, through theft or damage, lack of availability or device malfunction
- Software
 - These include applications, operating systems and other system software
 - Availability is a key consideration here, and asset evaluation must take account of disruption losses and recovery expenses
- Information
 - These comprise the information stored in databases and file systems, both on-premises and remotely in the cloud
 - Asset valuation needs to take into account the impact of threats to confidentiality, privacy, integrity, and authenticity
- Business
 - These include assets that don't fit into the other categories and also intangible ones (know-how, reputation, controls, etc.)

In order to effectively protect assets, an organization needs to provide a systematic method of documenting assets. This is done in an asset register that documents important security-related, including assets features and information ones.

4.12. Threat types and identification

Threat identification is the process of identifying sources with the potential to harm system assets. Threat sources are categorized into three areas:

- Environmental
 - Examples include floods, earthquakes, tornadoes, landslides, avalanches
- Business resources
 - Examples include equipment failure, supply chain disruption
- Hostile actors
 - Examples include hackers, hacktivists

Many efforts have been made to categorize types of threats, and there is considerable overlap in the definition of some common terms. A large category of threat is malicious software, or malware, which is a general term encompassing many types of software threats (e.g., malware, virus, worm, etc.)

- It is difficult to get reliable information on past events and to assess future trends
- Organizations are often reluctant to report security events in an effort to save corporate image and some attacks may be carried out without being detected by the victim until much later
- Three important categories of threat information sources are:
 - In-house experience

- Already inside the organization
- Security alert services
 - Concerned with detecting threats as they develop to enable organizations to patch code, change practices or react
- Global threat surveys
 - Many available and ranked according to the volume of security incidents surveyed
 - For each threat, the report provides a kill chain, which is a systematic process used to target and engage an adversary to create desired effects

There is also *SOC - Security Operation Center*, which is a facility that tracks and integrates multiple security inputs, checks risk, determines the targets of an attack, contains the impact of an attack, and recommends and/or executes responses appropriate to any given attack.

4.13. Control identification

Controls for cybersecurity include any process that modifies information security risk. Controls are administrative, technical, management, or legal in nature.

Control identification is defined in ISO 27005 and suggests the following steps:

- (1) Review documents containing information about the control
- (2) Check with the people with responsibility related to information security and the users about which controls are implemented
- (3) Conduct an on-site review of the physical controls, comparing those implemented with the list of what controls should be there
- (4) Review results of audits

NIST SP 800-53 should be consulted in the development of any risk treatment plan, considering it defines multiple families.

- For each control, the catalog provides a description of the control, supplemental guidance on implementation, a description of control enhancements

This NIST Interagency Report (NISTIR) provides guidance on how small businesses can provide security and NISTIR 7621 provides the following useful checklist of controls:

- Identity
- Protect
- Detect
- Recover

4.14. Vulnerability identification and classification

Vulnerability identification is the process of identifying *vulnerabilities*, which are weakness or flaws inside procedures, design or implementation.

There are different categories:

- Technical vulnerabilities
- Human-caused vulnerabilities
- Physical/environmental vulnerabilities
- Operational vulnerabilities
- Business continuity and compliance vulnerabilities

In the area of technical vulnerabilities, it is possible to be more precise and exhaustive:

- National Vulnerability Database (NVD)
 - It provides enhanced information above and beyond what's in the CVE list, including patch availability and severity scores
 - It also provides an easier mechanism to search on a wide range of variables
 - Parameters are related to the vulnerability's level of exploitability and the parameters related to the vulnerability impact metrics
- Common Vulnerability Scoring System (CVSS)
 - Overall score assigned, in a scale from 0.0 to 10.0
- Common Vulnerabilities and Exposures (CVE)
 - Simply a list of all publicly disclosed vulnerabilities with their data

4.15. Risk assessment approaches

Two factors of risk assessment, impact and likelihood, can be treated either quantitatively or qualitatively:

- Impact
 - A quantitative approach we can assign a specific monetary cost
 - Otherwise, qualitative terms, such as low, moderate, and high, are used
- Likelihood
 - The quantitative version of likelihood is simply a probability value
 - The qualitative likelihood can be expressed in such categories as low, medium, and high

For quantitative risk assessment:

- If all factors are expressed quantitatively, then it is possible to develop a formula that measure of the cost of security breaches as follows:
 - $\text{Level of risk} = (\text{Probability of adverse event}) \times (\text{Impact value})$
 - We can express the residual risk level using the mitigation factor that reflects the reduction in the probability of an adverse event:
 - $\text{Residual risk level} = (\text{Probability of adverse event}) / (\text{Mitigation factor}) \times (\text{Impact value})$
- If factors can be quantified with a reasonable degree of confidence, then previous equations should be used to guide decisions concerning how much to invest in security control
- As new security controls are implemented, cost of security breaches declines, but total cost of security increases
- At the end for the qualitative risk we need to define levels of risk

For qualitative risk assessment:

- It determines a relative risk rather than an absolute risk, usually sufficient for identifying the most significant risks
- It is clear that subjective estimates are inherent in the process, while evaluating between opinions and risks
- Has different impact categories:
 - Low (limited adverse effect)
 - Moderate/medium (serious adverse effect)
 - High (severe adverse effect)
- Ranges of probability are assigned to qualitative likelihood categories, usually Low/Medium/High, both based on estimates on number per year an event occurs
- The vulnerability to a particular threat is a function of the capability, or strength which can be expressed by a likelihood matrix, basically a function of frequency classifying impact
- A coarse analysis must be subject to judgment
- On average, each type of breach may be expected to yield the same amount of annual loss
 - Deal with low-likelihood, high- impact breach or with the high-likelihood, low-impact breach: is for management to decide
- A simple approach to risk assessment is to use a risk analysis worksheet, which is a table with one row for each potential threat/vulnerability pair. It has the following columns:
 - Security issue
 - Likelihood
 - Impact
 - Risk level

- Recommended security controls
- Control priorities
- Compliance requirements include those imposed by the organization's security policy. It should be rated as follows:
 - 0 = not implemented
 - 1 = partially implemented
 - 2 = implemented but not yet documented
 - 3 = implemented and documented

4.16. Factor Analysis of Information Risk (FAIR)

For purposes of risk assessment, it is useful to group security controls in a manner that reflects the risk assessment process.

- FAIR is an important contribution to risk assessment first introduced in 2005 and has been standardized by the Open Group, providing a methodology for analyzing risk
- The standards is probabilistic rather than predictive, understanding “the probable frequency and magnitude of future loss”
- It provides a more detailed set of guidelines than ISO 27005, providing definitions more specifically tied to risk analysis and based on a belief that subjective qualitative analysis is inadequate

The FAIR (Factor Analysis of Information Risk) risk analysis document, groups controls into four categories:

- (1) Avoidance controls
- (2) Deterrent controls
- (3) Vulnerability controls
- (4) Responsive controls
- FAIR adopts a top-down approach
 - based on historical data, to develop an estimate of loss event frequency, simply on the basis of how frequently a loss event has occurred in the past
- FAIR has different Risk Assessment Levels:
 - If the organization's management or security analysts do not have confidence that a good loss event frequency can be directly estimated: estimating threat event frequency and estimating vulnerability
 - The assessment of threat event frequency involves two aspects:
 - determining frequency of contact with assets
 - probability of acting against assets

- Contact can be physical or logical
 - Physical access is possible for employees and outside actors
 - Logical access is via a network
- Contact can be unplanned, or random, or it can be regular
 - Can have five levels of frequency: VH, H, M, VL, L (L=Low / M= Medium / H = High)
- Determine the probability that the threat agent will take action
- The two dimensions of vulnerability are the threat capability and the control strength and estimating capability involves looking at two factors:
 - Skill
 - Resources

4.17. Likelihood assessment

- The process of developing some sort of agreed-upon likelihood score that estimates the chance of a threat action
- The assessment considers the presence, tenacity, and strengths of threats as well as the presence of vulnerabilities and the effectiveness of security controls already in place
- This assessment is applied to each identified potential threat action and likelihood assessment for a given threat is shown in the following steps:
 - Step 1. Determine the likelihood that a threat event will occur
 - Step 2. Determine the degree of vulnerability
 - Step 3. Determine the likelihood that a security incident will occur
- This analysis needs to be repeated for every threat to every asset

4.18. Impact assessment

The process of developing some sort of agreed-upon impact score or cost value that estimates the magnitude or the adverse consequence of a successful threat action.

- The essence of impact assessment is that, for a given threat to a given asset, you determine the impact on the asset if the threat were to become an actual security incident
- Detailed guidance on how to characterize impact and depends on two categories of loss:
 - primary loss
 - occurs directly as a result of the threat agent's action upon the asset
 - the owner of the affected assets is considered the primary stakeholder in an analysis
 - this event affects the primary stakeholder in terms of productivity loss, response costs, and so on

- there are two aspects: asset and threat
- next step is determining what threat action might apply to this asset: access/misuses/disclosure/modification/deny access
- secondary loss
 - occurs as a result of secondary stakeholders reacting negatively to the primary event
 - here, magnitude and loss event frequency are measured

Once the loss magnitude is estimated and the loss event frequency derived, it is a straightforward process to derive an estimate of risk, done separately for primary/secondary, then combining them to determine an overall risk.

- This is done, for example, via risk assessment matrices

4.19. Risk evaluation and treatment

Evaluation process:

- Once a risk analysis is done, senior security management and executives can determine whether to accept a particular risk and if not determine the priority in assigning resources to mitigate the risk

NIST SP 800-100 provides some general guidance for evaluating risk and prioritizing action:

- High
 - Strong need for corrective measures
- Moderate
 - A plan must be developed to incorporate these actions
- Low
 - Corrective actions must be determined in impact and understood if still required to accept the risk

ISO 27005 lists these options for treating risk:

- Risk reduction or mitigation
 - Done by implementing security controls, changing likelihood/consequences and removing threat sources
- Risk retention
 - Also called risk acceptance, it's a conscious decision to to pursue an activity despite the risk presented or to abstain from adding to the existing controls
 - This treatment is acceptable if the risk magnitude is within the risk tolerance level
- Risk avoidance
 - If the risk in a certain situation is considered too high and the costs of mitigating the risk down to an acceptable level exceed the benefits, the organization may choose to avoid the circumstance

- Risk transfer or sharing
 - Sharing or transferring risk is accomplished by allocating all or some of the risk mitigation responsibility or risk consequence to some other organization

5. M2.2 - Planning for Cybersecurity

5.1. Threat modelling

A strategic process aimed at considering possible attack scenarios and vulnerabilities within a proposed or existing application environment for the purpose of clearly identifying risk and impact level.

- Think and find security issues
- Understand security requirements
- Develop and delivery better products
- Four step process
 - What are you building
 - What can go wrong
 - What should you do if things go wrong
 - Was analysis a good job
- Useful to create diagrams, giving an overview and identifying trust boundaries and Data Flow Diagrams (DFD)
 - made of data, processes, external entities, data store and trust boundaries themselves

5.2. STRIDE (Threat Modelling)

STRIDE is a threat classification system developed by Microsoft that is a useful way of categorizing attacks that arise from deliberate actions. This allows to see how different threats affect each other using previous tools.

- Spoofing identity
 - Illegally accessing authentication information
 - Area of authentication
- Tampering with data
 - Involves the malicious modification of data and unauthorised changes
 - Area of integrity
- Repudiation
 - Deny performing a malicious action
 - Area of non-repudiation (users who deny performing an action)
- Information disclosure
 - Threats that involve the exposure of information to individuals who are not supposed to have access to it

- Area of confidentiality
- Denial of Service (DoS)
 - Attacks that deny service to valid users
 - Area of availability
- Elevation of privilege
 - An unprivileged user gains privileged access and has sufficient access to compromise or destroy the entire system
 - Area of authorization

5.3. DREAD (Risk Classification)

DREAD is part of a system for risk-assessing computer security threats that was formerly used at Microsoft. Its categories are:

- Damage Potential
- Reproducibility
- Exploitability
- Affected users
- Discoverability

Evaluation of the threats that will be subject to security analysis, carried out the following methodology through:

- a rating defined on ten levels and applied to five risk categories
- levels are grouped into three categories, corresponding respectively to a High (8-10), Medium (4-8), and Low (0-4) risk levels
- this is a qualitative risk assessment

Mitigation is the point of threat modelling:

- Address each threat
- Redesign/Apply standard/Use software/Invent mitigations
- Accept vulnerability
- Address each threat

A model then needs to be checked (completely/accurately/covered/enumerating) and updating the diagram accordingly.

5.4. OCTAVE (Risk Management)

OCTAVE (Operationally, Critical, Threat, Asset, and Vulnerability Evaluation) is an approach to identify, assess, and manage risks to IT assets.

- This process identifies the critical components of information security and the threats that could affect their confidentiality, integrity, and availability
- This helps understand what information is at risk and design a protection strategy to reduce or eliminate the risks to IT assets
- Define essential components for a context-driven, self-directed information security risk evaluation

There are three main methods:

1. The original OCTAVE method, (forms the basis for the OCTAVE body of knowledge)

- Was designed for larger organizations with 300 or more users
- The method was also designed to allow for tailoring by organizations adopting it
- Made up of three phases:
 - Phase 1: Identify important information-related assets
 - Phase 2: Integrate threat analysis and inform mitigation decisions
 - Phase 2: Perform risk identification and develop risk mitigation

2. OCTAVE-S

- For smaller organizations of about 100 users or less
- Performed by an analysis team that has extensive knowledge of the organization and made up of three phases similar to the previous one
- Does not rely on formal knowledge conducting workshops to gather information because it is assumed that the analysis team has working knowledge

3. OCTAVE-Allegro

- A streamlined approach for information security assessment and assurance
- This approach differs from previous OCTAVE approaches by focusing primarily on information assets and how are they used/stored/transported/processes, using workshops and questionnaires
- Well suited for use by individuals who want to perform risk assessment without extensive organizational involvement, expertise, or input

5.5. Security management

The security management function entails establishing, implementing, and monitoring an information security program, under the direction of a senior responsible person.

- It involves multiple levels of management
 - Chief Information Security Officer (CISO)

- Has overall responsibility for the enterprise information security program
- Should designate an individual or a group to monitor and reflect changes on all organization environment, signaling violations with reporting mechanisms
- The relation between executive management and the information security program, communicating and coordinating closely
- Different roles and key security program areas:
 - Security and capital planning
 - This process enables the CISO to oversee all security projects throughout the organization
 - It involves three steps:
 - Identify
 - Analyze
 - Select
 - Also, the cost planning is applied and identified between different categories
 - Awareness and training
 - Information security governance
 - System development life cycle
 - Security products and services acquisition
 - Risk and configuration management
 - Contingency planning
 - Performance measures
- Information Security Manager (ISM)
 - Has responsibility for the management of information security efforts

NIST SP 800-18 “Guide for Developing Security Plans for Federal Information Systems”, indicates that the purpose of a system security plan is to provide an overview of the security requirements of the system.

- The system security plan also delineates responsibilities and expected behaviour
- The system security plan is basically documentation of the structured process for a system
- It recommends that each information system in an organization have a separate plan document with different elements, basically categorizing everything

6. M3.1 - Cybersecurity Operations and Management

6.1. Human Resource Security

- Includes hiring, training, monitoring and handling employees
- Not only a technical challenge, also employees have to be aware of incidents and problems
- Harmful behaviors can occur, being both malicious and non-malicious

6.2. Hiring process

- ISO 27002 specifies “the hiring process ensures employees and contractors understand their responsibilities, suitable for their roles”
- They should be fully capable of perform the intended job, without making unfounded claims and avoiding “negligent hiring”
- Ask applicants as much detail as possible and in case get even criminal/credit record check, according to the country’s law
- Employees should agree and sign the terms and conditions of contracts, including non-disclosure agreement and ensuring assets are confidential, agreeing to respect both the policy and confidentiality

6.3. During and after employment

- Each job should have specific cybersec tasks associated
- Employers and contractors should be aware of responsibilities, policy and training programs
- Several principles for personnel security:
 - Least privilege
 - Separation of duties
 - Mandatory vacations
 - Limited reliance on key employees
 - Dual operator policy
- During the termination of employment phase, organization’s interests should be protected and all data/accounts/codes/assets regarding specific individuals will be removed

6.4. Security awareness

- Having a good security awareness and appropriate security training is as important as any other security countermeasure or control
- Activities that explain and promote security should develop into secure practices according to the specific role, accompanying good education/certification

- All employees have security responsibilities which the awareness program should constantly push, being focused on all people and categories
- A good program should include all aspects (e.g., communication, responsibility, help, security culture)
- According to ENISA we should have:
 - Plan/Assess/Design
 - Execute/Manage
 - Evaluate/Adjust
- Good communication materials should be available:
 - both in-house
 - and externally obtained
- Good education/certification programs should be also available, considering specialized training
- Role-based training also should encompass:
 - Manage
 - Design
 - Implement
 - Evaluate

6.5. Hardware management

- Hardware = any physical asset used to support corporate information or systems, including the software embedded within them and the operating systems
- Hardware Asset Management (HAM) deals specifically with hardware portion of IT assets, managing the physical components
- Its lifecycle is composed by:
 - Planning
 - Acquiring
 - Deploying
 - Managing
 - Disposing
- Destruction is important to handle data safely

6.6. Office equipment

- Every hardware inside an office, containing sensitive information processed by or stored inside of it

- Could be also multifunction devices (MFD)
- Each contains some processing power and each is an asset to protect opportunities for threat and protection
- Could be exposed to several threats:
 - Network services
 - Information disclosure
 - DoS attacks
 - Physical security
 - OS security
- They can have a checklist containing organization measures

6.7. Equipment disposal

- SOGP recommends sensitive information should be securely destroyed
- Three main actions:
 - Clear = sanitize storage locations
 - Purge = apply logical/physical techniques to destroy encryption key on devices
 - Destroy = renders target data recovery infeasible

6.8. Industrial Control System (ICS) security

- Used in control industrial processes, including Supervisory Control and Data Acquisition (SCADA)
- Consists of a combination of control components used to achieve industrial objectives
 - HMI - Human-Machine Interface
 - Remote diagnostics and maintenance
 - Sensors
 - Actuators
 - Control
- They are distributed in insecure locations, often with microcontrollers with limited processing power
- There could be several threats:
 - Blocked/delayed flow of information
 - Unauthorized changes to instructions
 - Inaccurate information

- ICS software or settings modified
- Interference with operation of equipment protection systems, safety systems and system settings

6.9. Mobile device security

- Mobile device = Portable computing and communications device
- Prior to the use of smartphones, user devices were clearly confined over defined perimeters
- Now devices are constantly connected and there's always the need for more
- Each has a full stack, from hardware/firmware/mobile OS/application, being an entire ecosystem
- Millions of apps are available and each should conform to the organization security requirements; some examples
 - Rooting/Jailbreaking
 - Sideloads
- Many vulnerabilities to list, given they are outside of the corporate perimeter
- *Bring Your Own Device (BYOD)* - many organizations find convenient to have such a policy, inspecting devices and their features
 - configuring devices in such a way it's possible to access, protect and wipe data from them safely, even remotely

7. M3.2 - Cybersecurity Operations and Management

7.1. System access and its functions

- Capability that restricts access to business applications, denying or limiting access to specific users
- *Functions:*
 - Authentication
 - Verifying the identity of user
 - Authorization
 - Granting of access by a security administrator, based on a security policy
 - Access control
 - Granting or denying specifying access requests
- Functions to establish rules and privileges and moderate access to an object in the system
- Each user has to be authorized properly, defining access privileges

7.2. Authentication factors and means

- Simplest way to access, including an identification and verification step
- Authentication factors are methods
 - The user has (possession factor) - tokens/smart cards/wireless tags
 - The user knows (knowledge factor) - passwords/PINs/tokens
 - The user is or does (inherence factor) - biometrics

7.3. Authenticators

- Means used to confirm a user/process/device
- Can be:
 - Multi-factor: use of one or more authentication means
 - Password-based: use of an ID and a password

7.4. Vulnerability of a password

- Instead of using a file retrieved by ID, to avoid storing password one can use a one-way hash function of the password
- Different kinds of attacks exist
 - Dictionary attacks
 - Specific account
 - Popular password

- Password guessing
- Hijacking
- Monitoring/Exploiting
- Rely on hardware/SSO/password managers to avoid problems
- Select password not too short or easy to guess, eliminating guessable passwords

7.5. Hashed password and salt

- Combine the password with a fixed length salt value using an hashing algorithm
- In verification, the ID is used to see if result matches, therefore password is accepted
- Salt usage
 - prevents duplicate password
 - increases difficulty for attacks
 - nearly impossible to use same password for more systems
 - is non-deterministic

7.6. Password cracking

- Process of recovering secret password stored in a system
- Many approaches like developing a dictionary to crack all words or precomputing hash values

7.7. Password file access control

- Deny the attacker access to the password file
- Allowing it only for a privileged user
- File can become readable or physical security might be a problem, to use a policy to force users selecting passwords difficult to guess

7.8. Possession-based authentication

- Object the user possess for user authentications = hardware tokens
- *Memory cards*: have an electronic memory, store but do not process data, used for physical access alone
 - May require specific requirements and can be lost
- *Smart tokens*: have some specific physical characteristics, user interface, electronic interface and authentication protocol
 - Have a smart card, a microprocessor and a processing circuit
- *Electronic identity cards*: also called eID, they provide stronger proofs of identity, given they are verified by a government

- *One-Time Password (OTP) device*: it generates one time passwords, using a seed embedded

7.9. Biometric authentication

- Based on the specific individual characteristics
- Technically complex and expensive
- Nature and requirements should be considered, being universal, distinct, permanent and collectable
- Should meet some criteria:
 - Performance and accuracy
 - Difficulty of circumventing
 - Acceptability by users

7.10. Access control

- Gaining the ability to communicate or interact with a system. In other words, the process of granting or denying specific requests, via specific services and mechanisms
- ACCESS CONTROL = AUTHENTICATION + AUTHORISATION
- Has different inputs
 - Who issued the request
 - What is required
 - What rules apply
- *System access* deals with moderating access to system objects via authentication (establishing user identity) and authorisation (defining user privileges)

7.11. Access control elements

- *Subject*
 - Entity capable of accessing objects
 - Typically considered accountable for their actions
 - Can be creators of resources, groups of users or every user possible to access
- *Object*
 - Resource which access is controlled and used to contain and/or receive information
- *Access rights*
 - The ways in which a subject can access an object

7.12. Access control policies

- Dictates what types of access are permitted

- Different categories exist:
 - *Discretionary access control (DAC)*
 - Based on requestor identity and on access rules, granting specific permissions
 - *Mandatory access control (MAC)*
 - Comparison between security labels (sensitiveness of resources) with security clearances (which resources to access)
 - Has to be mandatory, so not to enable user wishes
 - *Role-based access control (RBAC)*
 - Access control based on user roles
 - Role permissions can be inherited through an hierarchy
 - Can apply to a single or several individuals
 - *Attribute-based access control (ABAC)*
 - Access control based on attributes associated with and about subjects and objects, combining attributes under which an access takes place

7.13. Access control structures

- Access matrix = using access control lists (ACLs) or capability tickets
- Governed by a set of rules granting the subject access

7.14. Customer access

- Each customer needs to be uniquely approved and identified, both individual and in groups, responding to organization's business requirements
- Each one should be aware and trained
- Balance between customer satisfaction and meeting security requirements
- Subject to the same types of technical controls, defining access privileges and selecting an appropriate authentication procedure

8. M3.3 - Cybersecurity Operations and Management

8.1. Computer Security Incident Response Team (CSIRT)

- Responsible for rapidly detecting incidents
- Minimizing loss and destruction
- Mitigating the weaknesses that were exploited
- Restoring computing services
- Calculates the added value to invest in safety resources
- In small organizations can be the security team, in large ones they are two separate entities

8.2. Security Incidents

- Any action that threatens one or more of the classic security services
- Unauthorized access or modification
- Procedures to manage them
 - Sorting, detecting, identifying, documenting

8.3. Managing, detecting and responding to incidents

- Should be detected and reported
 - Manually (reports)
 - Automatically (with integrity/log tools)
- Triage
 - find the single point of contact for services and request additional information to categorize the incident and notify parts of the enterprise
- Documentation to respond to them
 - Detail/Describe/Identify categories, personnel, circumstances
 - Should immediately follow a response to the incidents
 - What
 - How
 - Details
 - Impact
 - Allows for reviewing the risk assessment and strengthening controls

- Once an incident is opened, has to go through a number of states until no further action is required and is considered closed

Security controls are in place throughout:

- Hardware
- Software
- Firmware

8.4. Malware and protection

- Program inserted into others compromising confidentiality, integrity, availability
- Many types and should be protected against them as much as possible
 - Clickless
 - Fileless
 - Adwares
 - Worms/Viruses, etc.
- Businesses are experiencing more and more
- Practical steps to take, avoiding attack and defending against different attack surfaces
- Protection software to use to protect against them, automating actions as much as possible, verifying all defenses and collecting results from all points of attack
 - Scanning
 - Monitoring
 - Identifying
 - Disinfecting
- Software has to be accompanied by other measures like whitelist, firewalls and virtualization

8.5. Intrusion Detection

- The sooner the intrusion is detected, the less damage can be done
- When an intrusion happens, confidentiality is lost on all levels and collecting informations can help assessing risks and other means of security
- No exact distinction between an attack and normal use of resource: some overlap might happen
- Identification between legitimate and new user
- Approaches
 - *Misuse detection*: take the strange behaviour and consider it as normal attack, via usage of patterns and signatures. It cannot detect novel/unknown attacks

- *Anomaly detection*: detect activities different from normal behavior and be able to detect previously unknown attacks, having a trade-off between false positives and false negatives
- Intrusion Detection System
 - Sensors: collecting data and inputs
 - Analyzers: receive data from sensors and support evidence
 - User interface: give user output
- Techniques
 - Host-based
 - Layer of security to detect intrusions, events and send alerts
 - Detect thresholds and profiles
 - Network-based
 - Monitor the traffic on the networks and see if packets match signatures
 - Can use sensors to gather data and feed information
 - It can see data inside the network but also outside of firewalls

8.6. Data Loss Prevention

- Information leakage can happen in an untrusted environment
- Monitor, and protect data in use and data at rest through deep content inspection
- Often includes unencrypted content
- Sensitive data should be precisely identified in an enterprise via different means
 - rule-based/fingerprinting/exact-partial file matching
- Data states
 - Data at rest = big risk with info stored throughout the enterprise
 - Data in motion = data transmitted over enterprise networks, subject to active/passive monitoring of information across enterprise networks
 - Data in use = part of media and saved physically somewhere, controlling the movement in end-user systems