



EUROPEAN CENTRAL BANK

EUROSYSTEM

Fundamentals of cybersecurity and the Cyber Resilience Oversight Expectations (CROE)

CEMLA

*Emran Islam &
Constantinos
Christoforides*

November 2019, Mexico

Agenda

1 Context, main definitions and the CROE

2 Governance and Continuous Evolution

3 Identification & Situational Awareness

4 Protection

5 Detection

6 Response and Recovery

7 Annexes

Main definitions of cyber...

➤ Cyber

“Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems”

Source: FSB Cyber Lexicon (adapted from CPMI-IOSCO Cyber Guidance)

➤ Cyber security

“Preservation of confidentiality, integrity and availability of information and/or information systems through the **cyber medium**. In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved ”

Source: FSB Cyber Lexicon (adapted from ISO/IEC 27032:2012)

➤ Cyber resilience

“The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents”

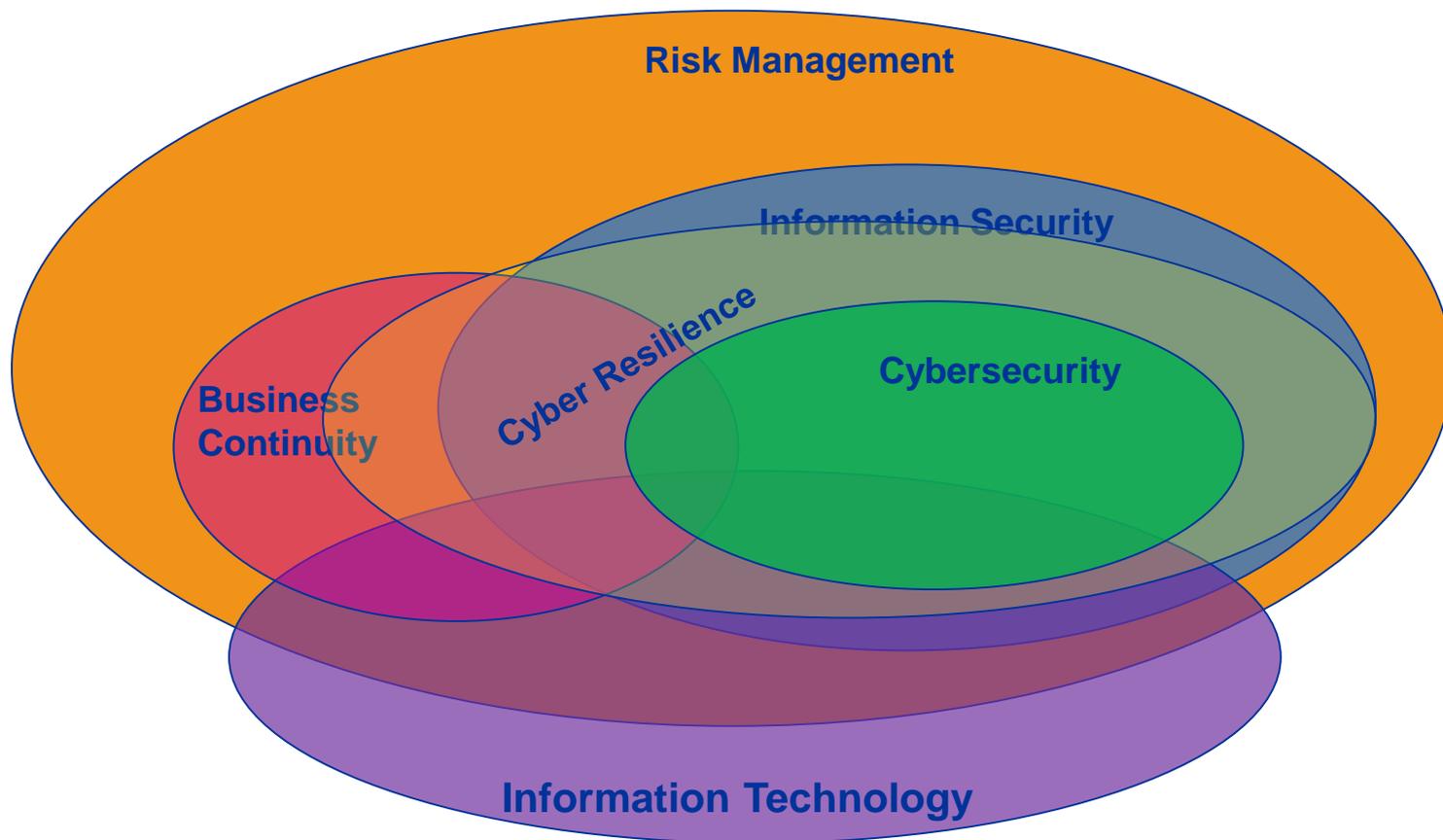
Source: FSB Cyber Lexicon (adapted from CPMI-IOSCO, NIST, and CERT glossary)

Strategic relevance of cyber threats

- **Characteristics of cyber threats**
 - Quickly **increasing** in **number**, **typology**, **persistence** and **complexity**
 - Can make **existent controls and business continuity measures ineffective**
 - Often occurring **immediately** after the **discovery of a vulnerability**
- **Characteristics and motivations of the attackers**
 - **Well organized** threat actors across **different countries**
 - Able to set **sophisticated attacks** difficult to detect
 - Disrupting organisations – loss of trust, credibility, business
 - Stealing funds
 - Obtaining sensitive information
- **Macro-vulnerabilities of the financial sector**
 - **Technological dependencies**
 - **Interconnections and mutual dependencies** → risk of quick distribution of threats from one entity to another
 - **Growing dependency** on TSP (Technical Service Providers)

Context, main definitions

A dynamic context where the scope of each activity continuously changes...



Do not stick to the definitions, but look at the purpose and at the rationale behind the security measures!

CPMI-IOSCO Guidance on Cyber Resilience for FMI

The Guidance is structured in chapters defining five main risk management categories and three general components that should be considered when talking about cyber resilience applied to FMI.

- Risk management categories are:
 - i. Governance
 - ii. Identification
 - iii. Protection
 - iv. Detection
 - v. Recovery
- General components are:
 - i. Test
 - ii. Situational awareness
 - iii. Learning and Evolution



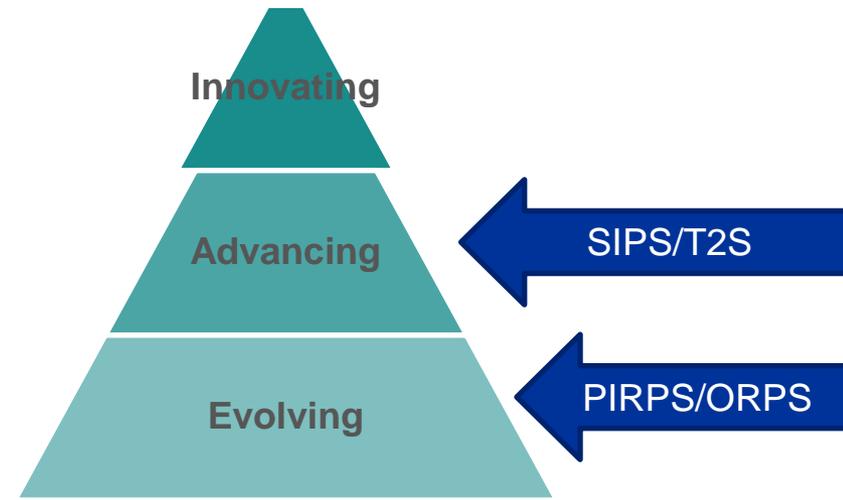
Cyber Resilience Oversight Expectations – December 2018

CROE – why?

- Sets up a more detailed elaboration of the CPMI-IOSCO Cyber Guidance to aid FMIs and overseers in implementing the Guidance and assessing the FMI's compliance against it
- Provides good practices which can be referred to when giving feedback to FMIs regarding assessments in the future
- Takes into consideration the industry best practices, already set out in different frameworks – e.g. *FFIEC Cybersecurity Assessment Tool, the NIST Cybersecurity Framework, ISF Standard of Good Practice, CobiT and ISO/IEC 27001*
- Provides the basis for overseers to work with FMIs over longer term to raise the FMI's maturity level
- Can be used as:
 - Assessment Methodology for overseers; and
 - Tool for self-assessments for FMIs.

Levels of expectations: the three-level approach

- Based on the **three level** approach;
- Each chapter is divided into the three levels of expectations;



- Applied in order to **adapt** to a changing cyber environment;
- FMIs are expected to **continuously evolve** on the cyber maturity scale;
- Provide an **insight** about the FMI's level of cyber resilience and what it needs to improve in terms of cyber expectations;
- Takes into account the **proportionality** principle (specific minimum requirements for SIPS/T2S, PIRPS, ORPS).

Levels of expectations: the three-level approach

Evolving level

- Essential capabilities are established and sustained across the FMI to identify, manage and mitigate cyber risks, in alignment with the approved cyber resilience strategy and framework, and
- performance of practices is monitored and managed.
- **All payment systems must meet the Evolving Expectations, aspiring to move to Advancing level**

Advancing level

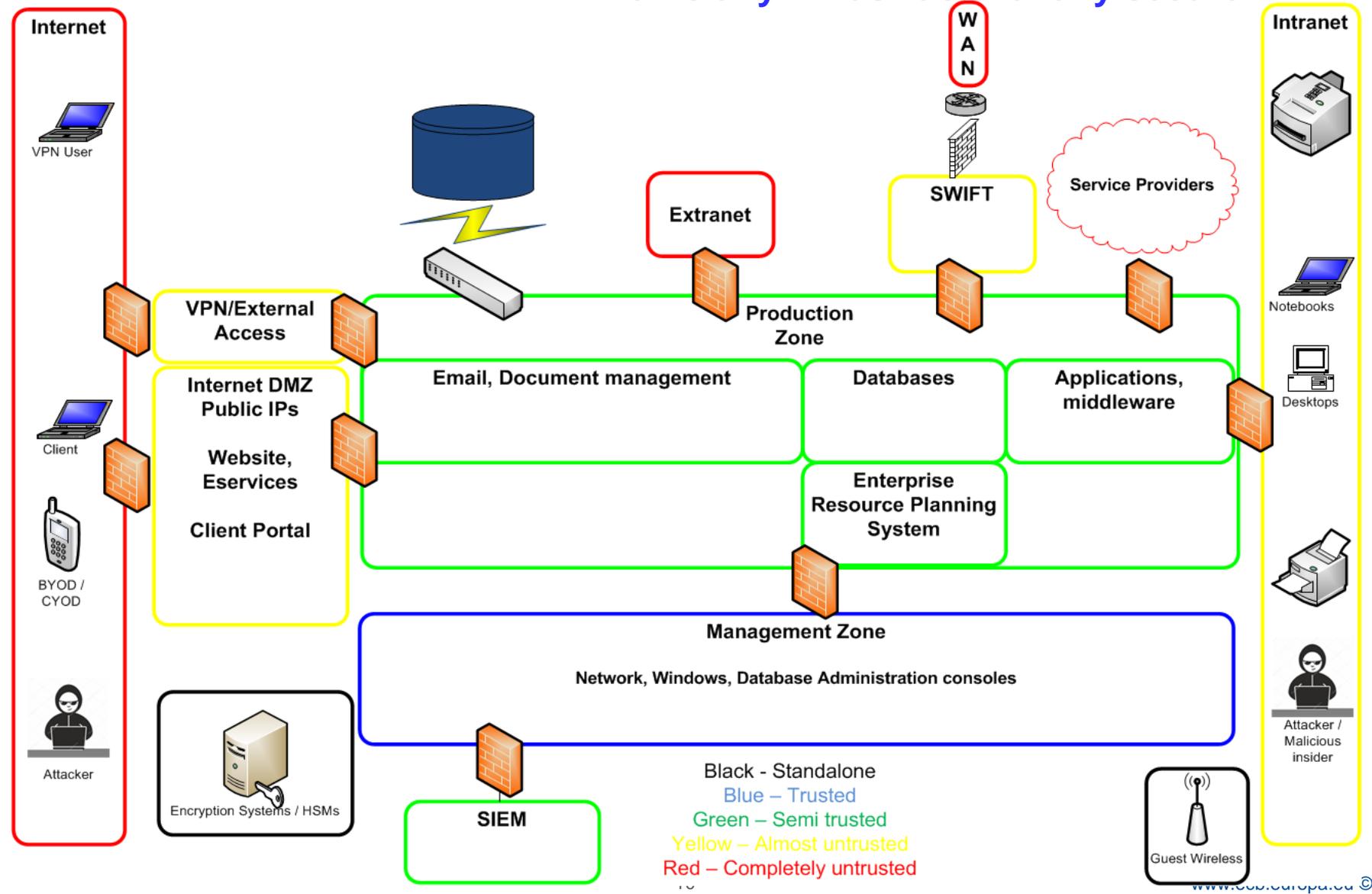
- Evolving level *Plus*
- practices incorporate more advanced implementations that have been improved over time, and
- capabilities are harmonized across the FMI to proactively manage cyber risks to the enterprise.
- **All SIPS must meet the Advancing Expectations, aspiring to move to Innovating level**

Innovating level

- Evolving level *Plus*
- Advancing level *Plus*
- capabilities across the FMI are enhanced as needed, in the midst of the rapidly evolving cyber threat landscape, to strengthen the cyber resilience of the FMI and its ecosystem, by proactively collaborating with its external stakeholders;

FMI IT Infrastructure

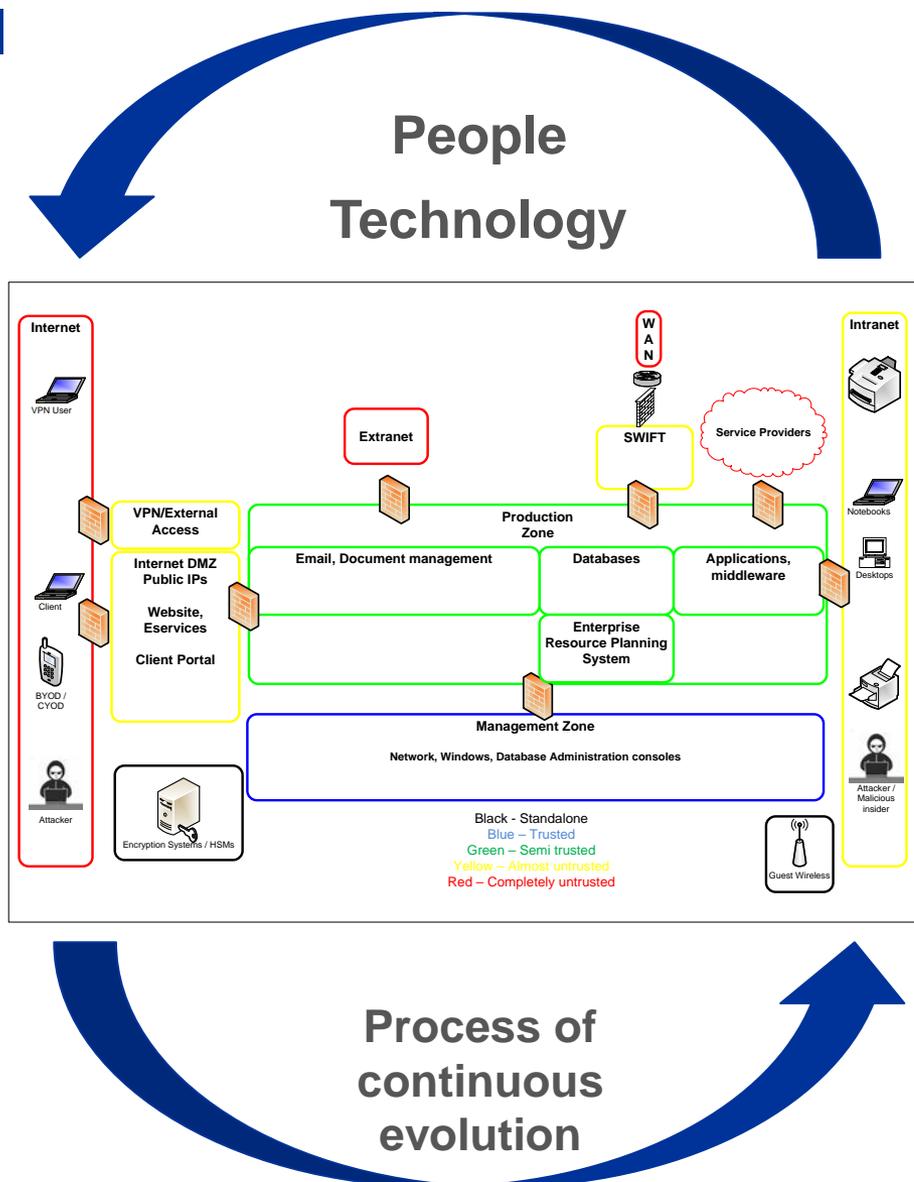
No technology is full-proof
nor is any infrastructure fully secure



Cyber Resilience in FMI

The CROE covers the following topics and how to use these domains to make the FMI resilient:

- i. Governance
- ii. Identification and Situational Awareness
- iii. Protection
- iv. Detection
- v. Response and Recovery
- vi. Testing



Agenda

1 Context, main definitions and the CROE

2 Governance and Continuous Evolution

3 Identification and Situational Awareness

4 Protection

5 Detection

6 Response and Recovery

7 Annexes

Information security / cyber resilience framework

Purpose

- The framework is developed to **describe how** the **objectives** and **targets** of the strategy shall be achieved systematically and how it will **continuously evolve**

What does it look like?

- Could be a myriad of **documents** depending on the size and scope of the FMI
- Includes policies, procedures, processes, workflows, forms etc.

Information security / cyber resilience framework

The framework should **cover** the key areas of:

- **Roles and Responsibilities** for Information Security/ Cyber Resilience
- **Identification** including asset classification and risk assessment
- **Protection** of information assets such as antimalware, encryption, segregation of duties, Privileged Identity management, Network Security, Change and patch management
- **Physical** Security controls
- **HR** security
- **3rd party security** management
- **Detection**, Logging and monitoring
- **Response** to a security incident, forensics and information sharing
- **Recovery** and Business continuity
- **Situational awareness** (Threat Intelligence)
- **Continuous evolution and metrics**
- **Information Risk Assessment**

Agenda

1 Context, main definitions and the CROE

2 Governance and Continuous Evolution

3 Identification and Situational Awareness

4 Protection

5 Detection

6 Response and Recovery

7 Annexes

What does the FMI know about its IT infrastructure?

The Information Security/ Cyber Security in a nutshell:

- 
1. In order to **protect** information assets you need to know what you have and where it is, catalogue it and keep it up to date.
 2. Then determine the **sensitivity / criticality** of these information assets both for existing IT systems and new ones.
 3. Then understand the **risks** to these assets based on the **threats** and **vulnerabilities**.
 4. **Implement** controls to mitigate risks (or perform other risk mitigation actions).
 5. **Re-evaluate** the risks after risk mitigation.

Conversely Step 1 is critical as you cannot safeguard what you do not know you have!

Information Asset Management in an FMI

Manual

- Done via excel or other form of register ☹️
- Must include details and serials to match
- Process required to update – resource intensive
- Maybe out of date/often inaccurate

Automated

- Done via the network discovery or via software (e.g. CMDB)
- Up to date, runs regularly
- Could have limited visibility with stand alone / isolated machines
- May lack details on underlying information to give a full picture
- Need to be augmented and managed also – no silver bullet

Hybrid

- Mix of manual and automated – usually the case in FMIs.

Risk Assessment

- A methodology for Information Risk Assessment (**IRM**), based on best practices must be adopted by the FMI in order to measure risks to the information assets.
- A systematic and periodic risk assessment process is **key** to identify the risks to the information assets by measuring the **business impact** in case **cyber threats materialise** in combination with the **threats and vulnerabilities** that exist.
- The risk assessment is undertaken in a **methodical** manner capable of producing **comparable** and **reproducible** results:
 - Identification of **mission critical** processes;
 - Identification of **associated information systems / asset**;
 - **Business impact analysis** for system / asset;
 - **Threats and vulnerabilities** analysis for each **system / asset**;
 - **Estimation of risk**;
 - **Risk mitigation measures and acceptance of residual risk**;

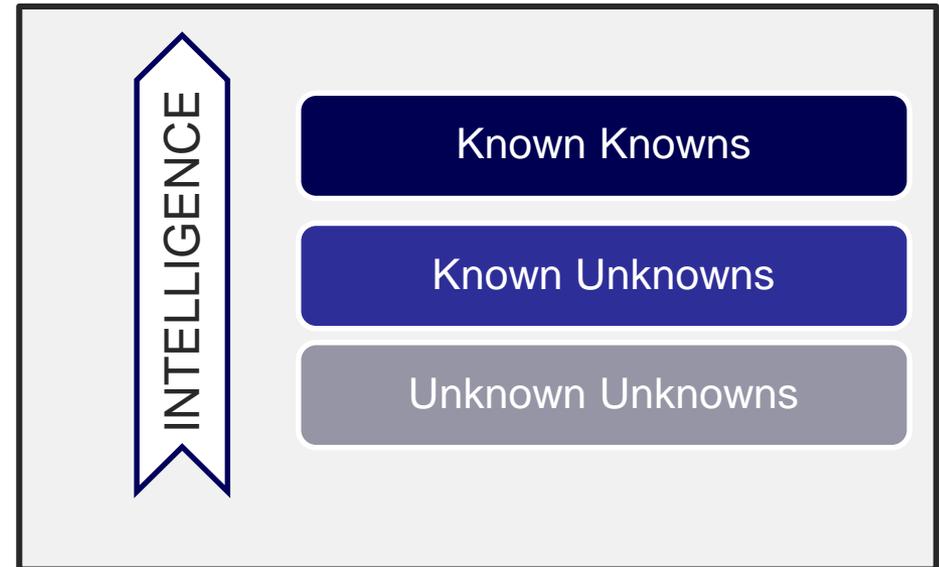
The importance of Threat Intelligence

- Definition:

Threat = Motivation of adversary combined with Capability of adversary

+

Intelligence = Any piece of information that can inform the decision making



- The rationale:

- *Know* your *enemy*
- Go *beyond the perimeter* of the organisation
- Go from *reactive* to *proactive* measures
- Allows FMIs to *prioritise* their *actions*

Threat Intelligence



- Usually a mix of **Commercial** and **Open source** Intelligence feeds.
- Use of **Indicators of Compromise (IoC)** and **Tactics, Techniques and Procedures (TTP)** to enhance the detection, e.g. SIEM solution, by being able to know how the FMI's adversaries attack.
- Use the adversaries TTPs to **plan** and **implement** better and more effective preventive controls.
- TI is **continuous** => threat levels, actors, techniques change.
- **Plugs in** with all **other Information Security / Cyber capabilities**, such as security testing providing value and guidance to perform more targeted testing such as **Red teaming**.

Information Sharing

- Share information regarding cyberattacks including **attackers' modus operandi, indicators of compromise, and threats and vulnerabilities**
- Levels of information sharing:
 - **Strategic** – Sharing information that helps organisations understand the type of threat they are defending against; the motivation and capability of the threat actor; and the potential impacts thereof
 - **Tactical** – Sharing information from direct adversary action inside your systems or from other sources that have the potential to immediately influence your tactical decisions
 - **Operational** – Sharing with participants network/technology service provider during an attack and vice versa
- FMI should share **timely information** (as an emergency process) to participants during and following a cyber attack to aid in the response, resumption and recovery of its own ecosystem.
- How is information shared? What are the **communication channels?**

Agenda

1 Context, main definitions and the CROE

2 Governance and Continuous Evolution

3 Identification and Situational Awareness

4 Protection

5 Detection

6 Response and Recovery

7 Annexes

Controls

Uniform control implementation and design offer:

- **Harmonised** approach to security controls
- Expandable and **scalable** controls
- Say the «**what**» and «**how**»
- Form the basis to create **security requirements** for new systems or changes to systems.
- Used to **benchmark controls** and enhance the overall posture
- Ensure security controls **comply** with any regulation or legal requirements

ISO 27001 and ISO 27002, NIST Framework, COBIT, ISF Standard of Good Practice for Information Security.....CSC Top 20, PCI-DSS, Australian Directorate Top 8

Identity lifecycle and management

- It refers to the creation, management, review and deletion of accounts
- Fundamental to manage identification, authentication, authorization and accountability

User Group → User

User → Roles

Role → Permissions

HR Dept → A. Waters

A. Waters → Recruitment_op, Payroll

Recruitment_op → Read, Write open vacancies

→ Create new vacancy

Permission (or privilege) → Operation (or action) on an object.

- Each user (human or technical) should exist as an identity in a system (individual-not shared) e.g. Document Management System, in the database or in any other repository has their own **access rights** which should be reviewed on a timely manner.
- In mature organizations identities are orchestrated by an **IAM (Identity and Access Management)** system or at the very least augmented via reporting tools.
- If no IAM system has been implemented there are separate islands of identities across systems with their own authorisation rules. This means systems are **handled independently**. **Resource intensive** and it almost always hails the **existence of security gaps**.

Information Repositories

- **Enterprise Content/Document Management System** –Contains documents which may include confidential information
- **Shared** folders, files and drives (contain reports)
- **Databases** (contain transactions/payments)
- **Cloud** platforms (share information with third parties)
- **Email** – an overlooked crucial information repository
- **End user repositories stored on clients** (workstations/ mobile devices)

Privileged Identity Management (PIM)

Everything in an FMI IT infrastructure from network equipment, clients, servers, operating systems, physical access systems, CCTV, telephony systems.... **have privileged accounts** (e.g. administrators), different from standard user accounts. Also technical accounts are used for intercommunication between systems (e.g. backups, updates):

- These accounts are the most sought after by attackers as they allow them to get access to **more systems** and/or to **escalate** their privileges.
- Some of these accounts possibly can access many machines e.g. IT Helpdesk, **Domain Controller Administrator**.
- PIM solutions are frequently used to **automate** these processes (ensure contingency arrangement), but have limitations and their setup is crucial for them to operate in a secure manner.
- If no automated solution exists, setting strong passwords frequently, assigning, revoking these accounts can be very labour intensive and is usually **troublesome**.

Attackers want to reach privileged accounts!

Identity attacks

- Social engineering (**Vishing, Phishing**) and keyloggers
- **Credential stuffing** – testing credentials from breaches linked to employees or clients in the FMI environment. Users may use the same passwords in their personal and professional lives.
- **Hash dump from system** – Once a system has been compromised like a user workstation the user can “dump” credentials. Note credentials of many users maybe found on even a client!
- **Sniffing credentials on network/ Man In the Middle** – once in the FMI infrastructure an attacker could impersonate another machine to obtain valid credentials or sniff them from any insecure/vulnerable protocols
- Taking advantage of **default username/passwords**.

Compromising identities is an essential part of a cyberattack

Identity attacks countermeasures

- **System Hardening** - System Configuration to make hacking systems more difficult and make the dumping of credentials less useful, more difficult to crack
- Proper **network security** to prevent attackers moving laterally
- Separation of **duties** of both users and systems to make credentials and systems captured by attackers less useful
- Privileged Identity Management solutions to **protect privileged accounts** as much as possible
- **Logging and Monitoring** of user logons, logoff, actions and correlations with other events.
- **Multi Factor Authentication** on critical systems/data/privileged accounts
- **Security Awareness** for all users.

Information classification

- Primary process to **protect** data to guarantee confidentiality, integrity, and availability whether it is at rest or in motion.
- Criteria for classification: **sensitivity**, **lifetime**, disclosure damage, modification damage, ...
- Useful to prioritize the risk and to define the access rules, authorization levels, and security controls
- **Main aspects :**
 - Identification of the **owner** and of the main **roles and responsibilities**
 - **Labeling** resources → classifying and declassifying
 - **Documenting** the classification
 - **Definition of security requirements** for both data at rest, in use, and in transit
 - **Implementation of controls** and security **measures** (e.g. encryption, watermark, Data Loss Prevention systems, back up) for both data at rest and in transit
 - **Training** of the users
 - **Data retention** and **disposal**

Information classification

Common technologies and controls to aid:

- **Data Loss Prevention System (DLP)** - System that monitors and protects data in use, data in transit and data at rest, with the aim to identify and prevent any unauthorised use and transmission of sensitive information (data exfiltration).
- **Digital Rights Management** – Originally was meant to protect copyrighted material but is now used to technically enforce data classification but in a different manner than above. E.g. you can send a DRM protected file via email externally but it will be encrypted and made unreadable.
- **Watermark** - cryptographic technique able to embed the sensitivity classification in a document, in a way that can be detected by DLP, too. Usually a watermark is not perceivable, and can be placed in a digital file (digital watermark).
- **USB/Removable media control** – disabling the use of USB, CD/DVDs and other ports with very specific exceptions.
- **Application Control** – allowing only the use of specific software throughout the infrastructure (deters many malware).
- **Browsing and Email control** – Restricting where users can go on the Web and who they can receive emails from or send to.

Data – at rest and in transit

- **Data at Rest**

- *How encryption is applied to:*
 - *Documents*
 - *Databases*
 - *Email messages*
 - *Backups*
 - *Workstation/ mobile devices*
 - *User credential storage*
 - *Storage/USB*

- **Data in transit**

- *How encryption is applied to:*
 - *Email messages*
 - *Remote access sessions*
 - *Helpdesk/ Administrative remote management*
 - *Web services internal and external*
 - *Wireless network*
 - *Web and wired network*



Implementation / Key / Certificate management is crucial! Who is responsible and how are they protected?

HR resources security policies

- Humans are often the weakest link in a security chain.
- HR security should be embedded in **every stage** of the **employment life cycle**:
- Before hiring new staff:
 - Carry out **security (white record) check, credit and reference check** with different levels of depth depending on the specific tasks and responsibilities
 - Clearly state **job responsibilities**
 - **Grant** the necessary **access rights**, based on the principles of **need to know, least privilege, and segregation of duties**
- During employment:
 - Apply **job rotation and mandatory vacations**
 - **Periodically review access rights** and change them in a timely manner if needed (preferably in automated way)
 - Require participation in **security awareness and training sessions**
 - **Redo pre-employment checks**

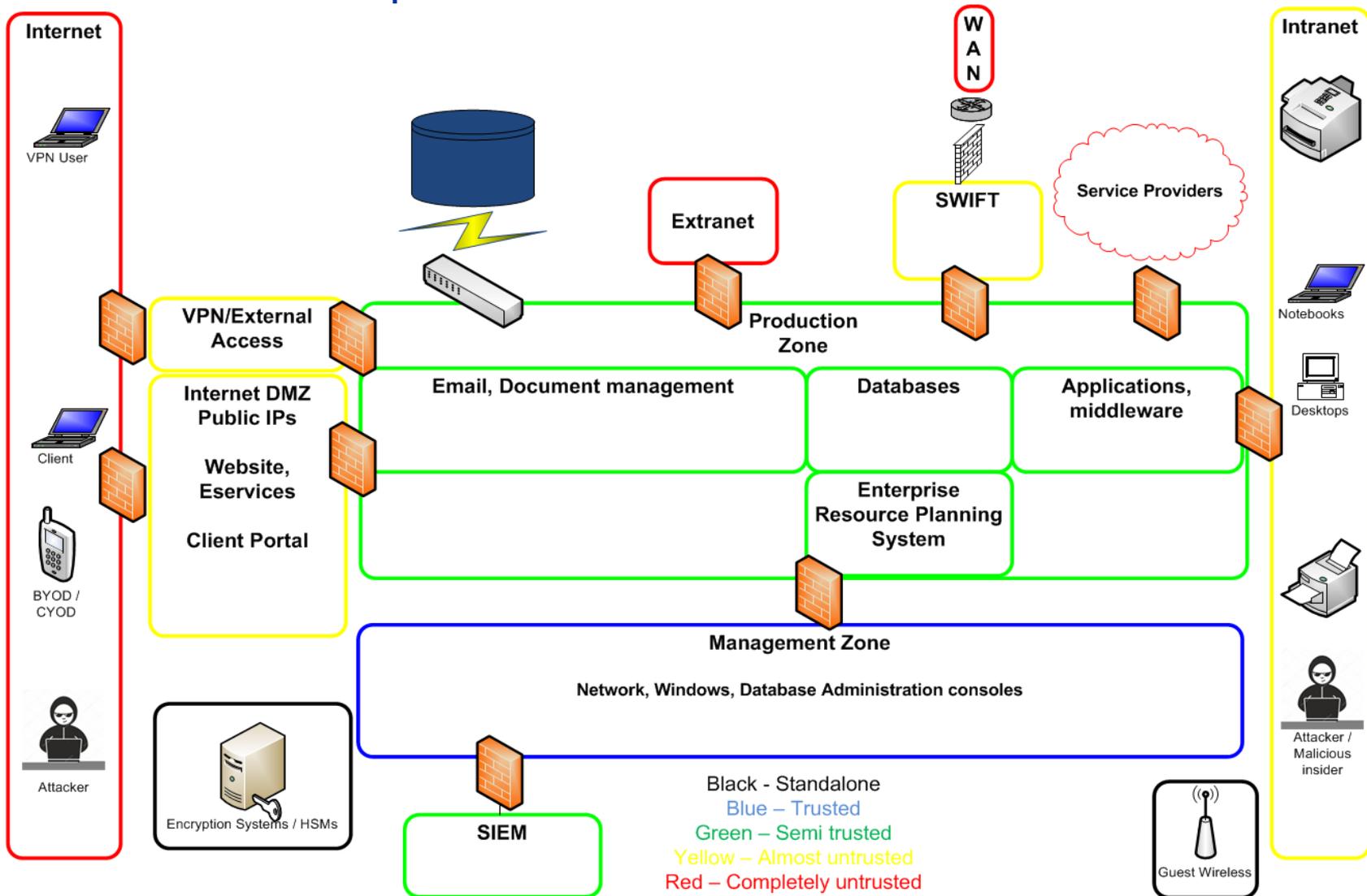
HR resources security policies

- At the termination of the employment contract:
 - **Revoke** in a timely manner accounts and access rights
 - **Ensure** return of information assets devices
 - Put in place **specific security procedures** in case of forced termination by the FMI, in order to minimize any risk

Overall Culture

- **Promote** a security culture within the FMI: employees should understand they play a relevant role in guaranteeing security, and that they could be also the weakest point. The Board should promote the security culture in the organisation.
- **Establish** a security awareness programme: the FMI should introduce mandatory training and awareness sessions for all employees or for specific user groups, based on their specific task and responsibilities. Exercises (e.g. phishing tests) or ad hoc workshops should also be also organised.

Practical example on the FMI IT architecture



Databases in an FMI

- Operationally very **significant**
- Contain **transactions, payments, customers information, etc.**
- **Multiple technologies** may be used for various databases.
- Should **not be accessed directly** – only via application.....
- **Sensitive data** usually encrypted
- Apart from security, database structure **optimisation, capacity** and **performance** are **critical** for an FMI to operate its database without problems

Database Security (DB) in an FMI

- **Encryption**

- Sensitive data is **encrypted** either in **columns or tables**
- Alternatively the **whole database** may be encrypted
- Even DB Administrators cannot “see” this data
- **Encryption key** is stored in another location-wallet but is accessible under circumstances. → An attacker who hacks the DB may not see the data, but if an account of a privileged application user is hacked the attackers would obtain access.

- **DB Firewall**

- The DB Firewall controls **who can access** the DB and how as well as **detects attacks** from queries and stopping them
- Without a DB Firewall a user could in theory access the DB and perform queries.
- It is not uncommon to have users that access the DB directly and they must be controlled and monitored
- All user actions are **logged** and sent to a centralised solution for correlation

Web application servers in an FMI

- Web application and application servers are needed to **provide a way** in which **users interact** with the structured data (=database).
- Could be that an application has both a **separate web application and application server** but it is also likely that only an application server is needed.
- Applications if vulnerable could be **compromised** to infect users and to capture credentials from them.

Web application security: web application firewall (WAF), proper configuration, securely coded web application (testing!)



It is possible to attack and get information from the database via the application/web application. Whatever is input in the application is then conveyed to execution in the database

Network Security

- **Attacks from external network**
 - Direct attacks via the **Internet**
 - Attacks against **external facing web services** e.g. payment gateway, customer portal etc.
- **Attacks between internal machines**
 - **Forbidden or suspicious communication** between machines especially between network segments (Pivoting-lateral movement of active attackers)
 - **Hacked machines**
 - **Unauthorised (remote) administrative activity**

Moving within the network is an essential part of a cyberattack

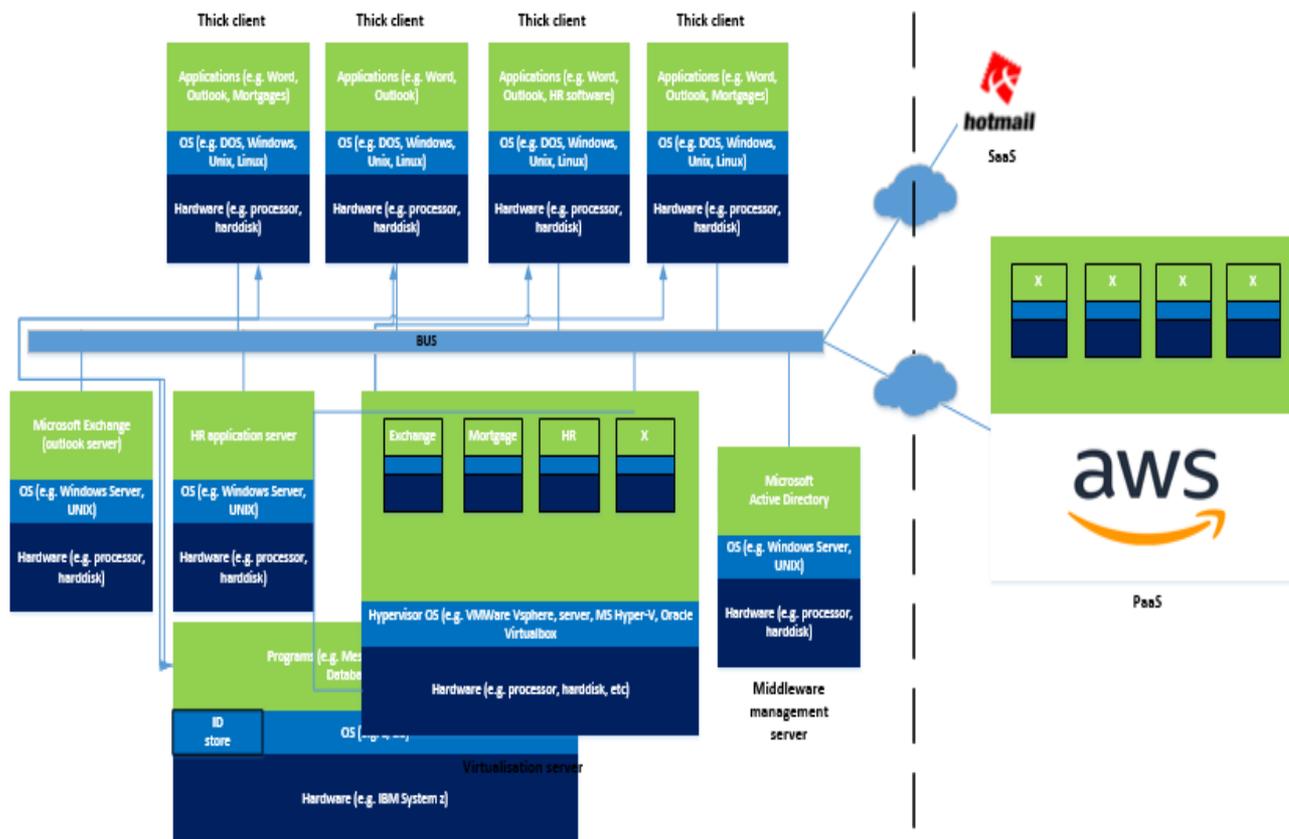
Remember! It is important to have in place:

- Machine **authentication** to prevent unauthorised machines
- Proper **procedures** to **authorise new machines on network** and to **decommission** existing ones.
- Properly configured firewalls, IPS and other security devices.

General Client and Server Protection

- **Clients → Workstations, Mobile Devices**
 - Hardening/Group Policy from Domain Controller if Windows
 - Non admin rights to users
 - Central management/patching
 - Antivirus, antimalware - endpoint protection
 - Intrusion prevention system
 - File Integrity Monitoring
 - Removable media restrictions
 - Browsing and email control
 - Logging and Monitoring
- **Servers → Database, Application, Web, Management duties or Utilities**
 - Hardening/Group Policy from Domain Controller if Windows
 - Antivirus, antimalware - endpoint protection
 - Intrusion prevention system
 - File Integrity Monitoring
 - Removable media restrictions
 - Logging and Monitoring
 - Central management/patching

Technologies – the complex reality



Cloud Services

VoIP - Voice over IP

Video Conference equipment

Storage Area Network (SAN) and fibre channel switches

Virtual containers

Decentralised Databases

AS400 Nonstop servers

Hardware Security Modules

Change Management

- Change management is deeply connected to the **asset management** process and to the **identification** of the most critical assets. To this regard, it is crucial to have **criteria** to prioritise changes (and to be able to perform emergency changes)
- Changes to system configurations should be strictly **controlled** and **monitored**, to avoid harmful effects in terms of confidentiality, integrity, and availability
- Changes should be **properly documented and communicated to the organisation** → failing to document changes can cause only trouble to the organisation
- There should also be the possibility of **rolling back unsuccessful** changes
- **Different** procedures/processes could exist for various systems, types of changes etc.

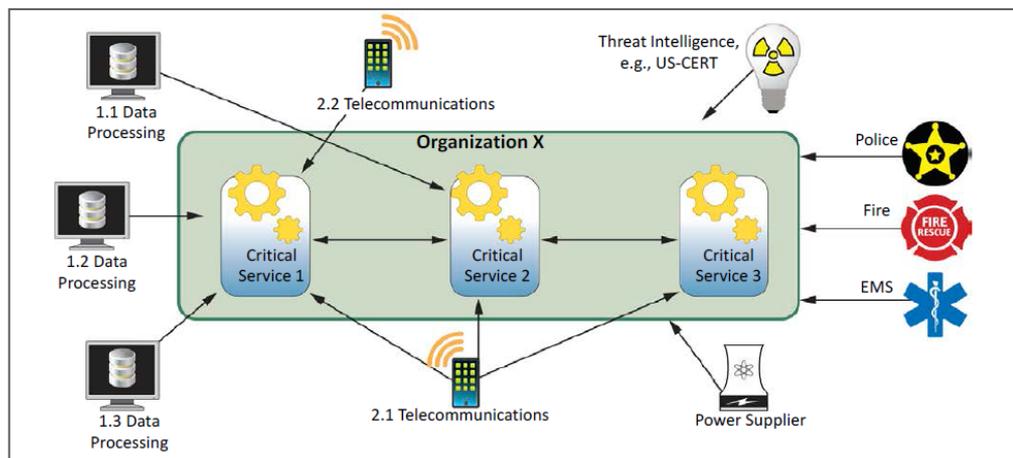
Patch management



Main **aspects** to be considered in a patch management process:

- **Severity** of the vulnerability → Priority for patching
- **Timing** for installing the patch
- Patching **configuration**:
 - **Automated , centralised, decentralised**
- **Dependencies** on other patches
- **Testing** of the impacts of patches (i.e. downgrade of system performances)
→ preferable to test patches on isolated systems
- **Approval** process
- **Roll back process** in case of failure
- **Critical** to prevent/detect cyberattacks
- System **downtime**, lack of **testing** systems and **resource intensiveness** are a big issue.

Third Party Risks



Lowering of control

Loss of knowledge in the organization

Dependence on the service provider

Long and complex outsourcing chains

Legal and Compliance

Conflict of interest

Dependence on internet access

Operational

Reputational (Data leakage)

Vendor lock-in

Concentration on a few service providers

Physical controls

- Adequate physical controls should be applied to protect office premises, data centers, sensitive areas (e.g. technical rooms with network devices/cabling..).
- Examples:
 - Access controls (reception, badges, locks, security guard, intrusion alarms...);
 - Smoke detectors, fire extinguishing systems;
 - UPS;
 - Air conditioning;
 - Water flood detectors;
 - ...
- Physical security controls should be periodically reviewed/ audited:
 - Users with access rights to data rooms /sensitive areas;
 - Data center certifications (e.g. Tier, ISO27001, ISAE 3402 type II,...)



Agenda

1 Context, main definitions and the CROE

2 Governance and Continuous Evolution

3 Identification and Situational Awareness

4 Protection

5 Detection

6 Response and Recovery

7 Annexes

Security Incident

- **Multiple ways** of detection of a security incident exist:
 - **Event** with operational impact such as an outage
 - **Security** event investigation
 - **Human** observance
 - **Processes**, such as reconciliation
 - **Threat intelligence** – Indicators of Compromise (IOCs)
 - **Third Party** notifications
 - **Machine Learning** systems / Anomaly detection → got very advanced recently
 - **Deception** Technology → creation of fake targets

- Focus should be on:
 - **Training** and empowering staff to **report** anything suspicious.
 - Building the **technical capabilities** to **log** and **monitor** systems for potential security incidents.

Logging and Monitoring

- Logging is the process to **capture** details related to **events** and **activities** occurring on a system → *who did what, when, where and how*
- The object is to **track** and **record** all the activities, to provide **accountability, detect anomalies, incident management, response, and investigations**
- Logs come from firewalls, IDS, IPS, routers, servers, domain controllers, applications, devices,...
- Logs must be **protected** to guarantee **integrity** and **availability**



- Due to the high volumes and different types of logs, the log analysis is generally supported by specific **systems**, able also to normalize and correlate different information → **Security Information and Event Management (SIEM)**
– **Splunk, Arcsight, Q Radar** etc.

Logging and monitoring in an FMI - SIEM

Security Incident Event Management (SIEM) is able to **gather**, monitor, **manage**, and **correlate logs** in real time, in order to **detect anomalous behaviour** in the organization's technology infrastructure (devices, network, applications, etc).

- **Critical** components and IT infrastructure should be **logged** at the level of Operating System, Application, Database, network devices, security devices, IDS/IPS, firewall, antivirus, document management system, etc.
- Any **missing logs** is **missing visibility** from a cyberattack
- Logs must be **properly configured** for each and every to ensure they are capturing the necessary information but not capturing “noise” that will lead to false positives
- The logs need to be **protected** from deletion or modification from administrators but also be available for a significant amount of time to aid in investigations. The logs could also be **digitally signed** to enable use as presentation of evidence in court if need be
- Logs are useless without **security intelligence**, **business parameters** and **correlation** → we are talking about millions of lines!

Logging and monitoring in an FMI – SIEM

- **What** correlation rules are in place? **How** are they updated, based on what criteria? How **frequently**?
- A SIEM constantly generates security alerts to be investigated and analysed by security **analysts** independent from operations.
- Events must be timely **analysed** and recognised either as an incident or as false positive etc.
- These **parameters** used to generate alert must be **revaluated** and **changed** in a controlled and authorised manner.
- Designating an alert as **false positive** must be **controlled**.
- SIEM upon deployment **will** generate a lot of **false positives** and there is an effort from analysts to constantly fine tune and maximise the efficiency of the logging and monitoring effort.

ALL ALERTS ARE POTENTIAL SECURITY INCIDENTS

Agenda

1 Context, main definitions and the CROE

2 Governance and Continuous Evolution

3 Identification and Situational Awareness

4 Protection

5 Detection

6 Response and Recovery

7 Annexes

Incident Response in an FMI

- It is a documented **policy statement**, with a generic procedure and **specific** plans in case of specific cyberattacks (e.g. ransomware, exfiltration, integrity breach)
- Incident **log** must exist (and not empty)
- **Technical Response**
 - Who? What? How? When?
 - Main elements:
 - Forensic capability and associated processes
 - Contagion strategies and desktop walkthroughs of the plans
 - Ensured readiness and availability of the technical teams
- **Business Side**
 - Tight integration with CRISIS Management and Business Continuity
 - Incident Response Team: Who does what, how, by when and who leads?
 - Has Incident Response Team been trained and do they test their readiness regularly?

TESTING!

Incident Response in an FMI

- FMI employees as well as third parties, insourced employees must be able to **report** security incidents, it is **not only** the Security Operation Centre's job to detect incidents and incidents (e.g. an employee stealing confidential information from a printer is not something a SOC would detect).
- Forensics which also include **malware analysis** are in-house in large FMIs and could be integrated with SOC (creating a SOC-Computer Emergency Response Team (CERT)) and outsourced in smaller FMIs (but with specific response times in contract).

Crisis Management

- **Operational incidents, security incidents**, as well as other events (e.g. damaging the reputation of the organisation) must interface with and trigger CRISIS Management.
- It is important to understand that an event such as a core system downtime would be treated as an **operational incident**, would be investigated to determine it is not a security incident, and also trigger a **CRISIS management** response as clients are affected.
- Main actions:
 - Informing all relevant authorities and communicating with stakeholders
 - Issuing press releases
 - Investigating the problem and determining the most prudent course of action
 - Approving initiation of recovery activities
 - In general steering the FMI in a way to minimise risk in light of the incident that occurred.
- For this to be effective the proper people (seniority and skill) must be **trained** and be involved as well as routinely test their readiness.

Recovery

Overlaps with traditional Disaster Recovery Planning and Business Continuity Planning of the FMI, the FMI must also be ready to **recover** its operations in case of cyberattack and test such plausible scenarios (e.g. a cyberattack compromises the network and customer data of the production systems)

- How **resilient** are the systems underpinning critical operations?
- Are the **backups** kept in a way to be safeguarded from a cyberattack? How quickly can the business data be restored?
- Can the FMI **restore** the latest trusted software from offline golden copies? And can it do it fast enough if there are hundreds of machines?
- How long would it take to **recover** software and data and be ready to continue operations?
- How is the **Ecosystem** involved.

This is an iterative process and a never ending one. There are always more scenarios and a higher degree of resilience plus faster recovery to be accomplished.

Recovery

- Identifying critical operations and setting correct **Recovery Time Objectives** and **Recovery Point Objectives** is key. It is also crucial that the correct IT infrastructure and other necessary components (could be individuals, third parties) that underpin the critical operations be correctly accounted.
- There should be a link from the IRM assessment of a system and its recovery capability. The higher the criticality from an availability perspective the faster a system should recover.
- FMIs usually **have multiple sites** with IT infrastructure using technologies such as optical fibres to facilitate communications and Storage Area Networks (SANs) to replicate data. In case of cyberattack this leads to increased propagation and means FMIs must be ready to operate in a world where these sites have been compromised.
- Scenarios for designing and testing recovery (from a cyber perspective) should also be based on **Threat Intelligence** information. Of course recovery under other scenarios such as terrorism, strikes, pandemics, natural disasters, region unavailability, civil unrest/war should be evaluated and tested.

Conclusion - Key messages

- To reach and evolve to high levels of cyber resilience:
 - A **continuous monitoring of new trends in cyber attacks** and **update of defence mechanisms** are key
 - Focus not only **technology**, but consider also **processes** and **people**
 - Design, test, implement and update both **preventive, detective** and **reactive** controls.
 - Do **not forget 4** crucial elements as:
 - **The establishment of a proper governance**
 - **The identification and prioritization of risks**
 - **Use of an established framework**
 - **The risk stemming from third parties and new technologies must be identified and managed**