Strengthening operational resilience: the information security perspective

Gianluca Pometto – Head of Group Security – UniCredit

Berlin, 17th October 2023

Empowering
Communities to Progress.

UniCredit

Gianluca Pometto

Head of Group Security **- UniCredit**

linkedin.com/in/pometto

Agenda

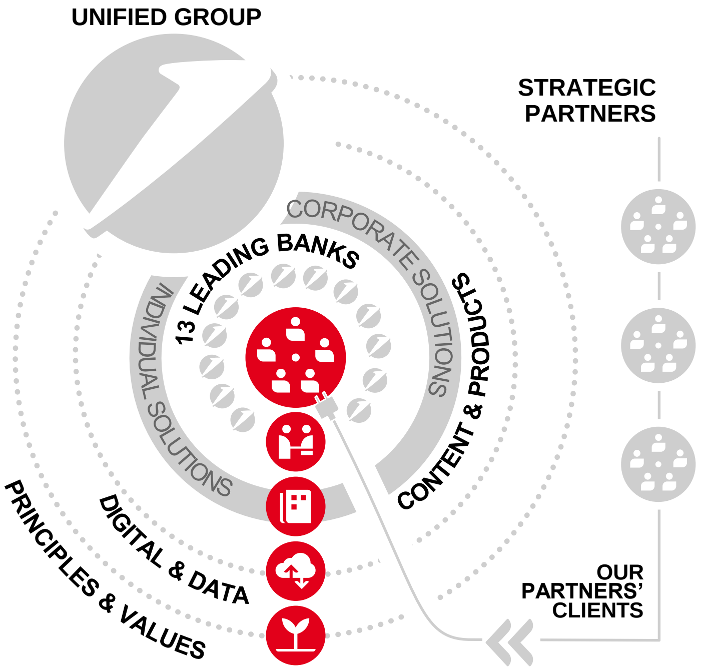
Current **external threats landscape** is challenging as never seen before.

UniCredit defined its Group Security Strategy to **support the Digital evolution**, and **to be ready for the unexpected.**

1. **UniCredit: who we are**
   At a glance
2. **Security landscape: top security threats**
   The complex as is scenario
3. **DORA regulation**
   What we did
4. **How we are dealing with this scenario**
   Our drivers
5. **Q&A**

UniCredit: who we are

At a glance: a pan-European Group



13 Banks

81k people

1 leaner Corporate Centre embedding Digital & data

4 Coverage regions

2 product factories serving all regions

A pan-European Commercial Bank connecting with clients in a unified way across Europe

Data as of 31.12.2022

Group Security 1/2

A team of

~ 700 people in 14 countries

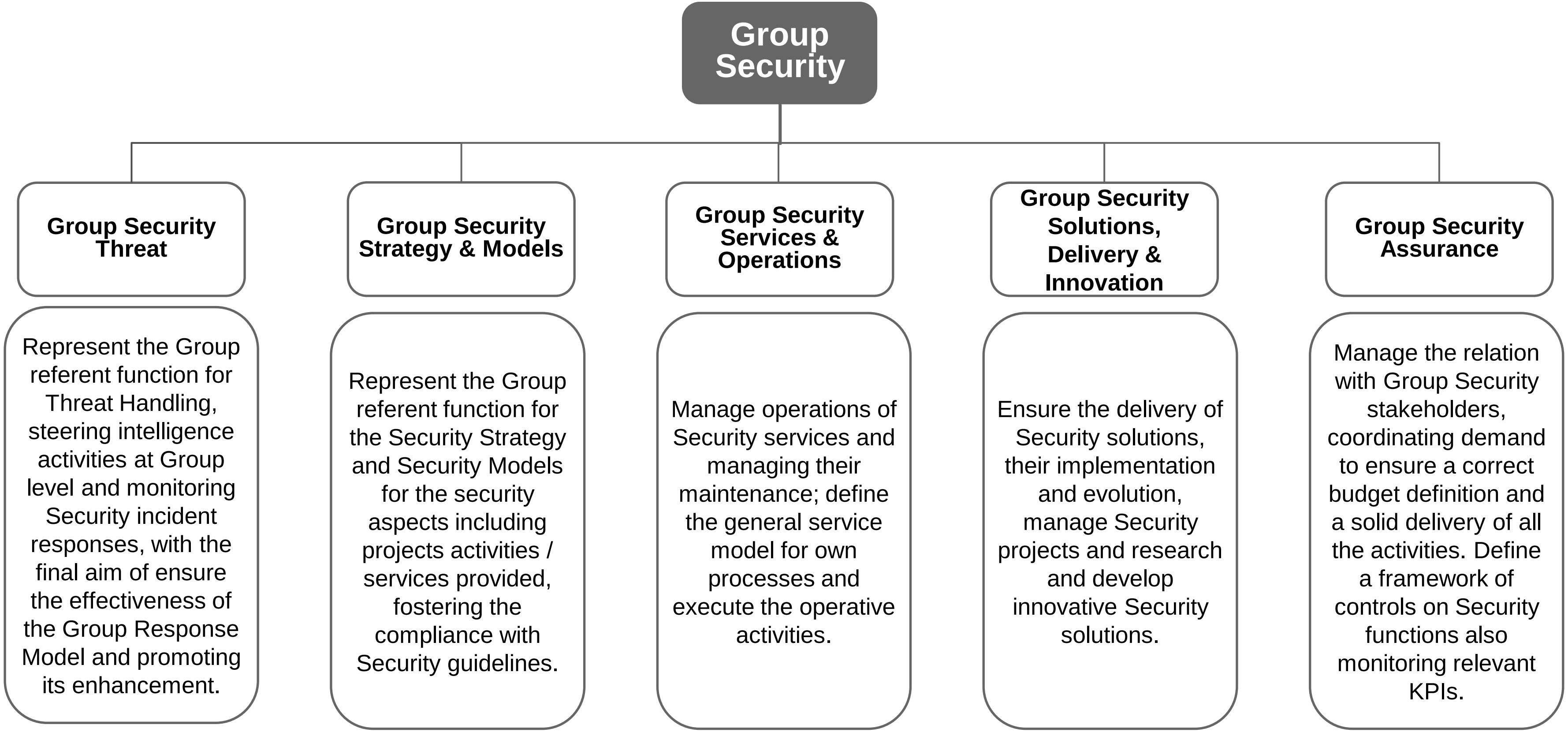
cooperating every day

A Group approach

for global solutions

UniCredit at a Glance

Group Security 2/2



Group Security

Group Security Threat

Represent the Group referent function for Threat Handling, steering intelligence activities at Group level and monitoring Security incident responses, with the final aim of ensure the effectiveness of the Group Response Model and promoting its enhancement.

Group Security Strategy & Models

Represent the Group referent function for the Security Strategy and Security Models for the security aspects including projects activities / services provided, fostering the compliance with Security guidelines.

Group Security Services & Operations

Manage operations of Security services and managing their maintenance; define the general service model for own processes and execute the operative activities.

Group Security Solutions, Delivery & Innovation

Ensure the delivery of Security solutions, their implementation and evolution, manage Security projects and research and develop innovative Security solutions.

Group Security Assurance

Manage the relation with Group Security stakeholders, coordinating demand to ensure a correct budget definition and a solid delivery of all the activities. Define a framework of controls on Security functions also monitoring relevant KPIs.

Security landscape: top security threats

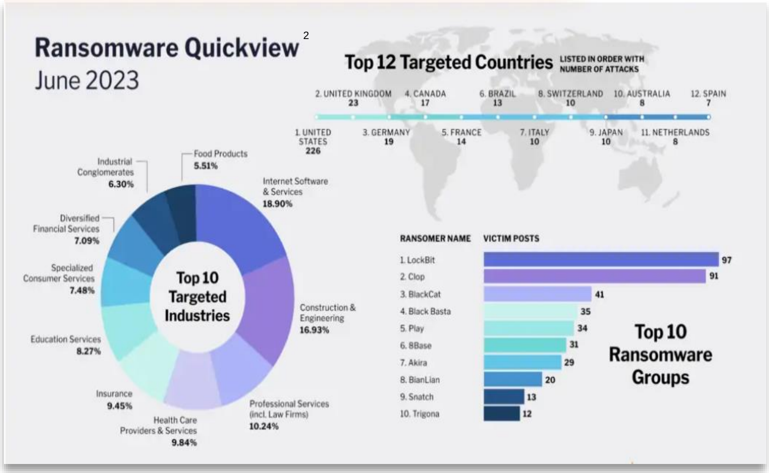
The complex as is scenario

This year-on-year rise of cybercrime has serious implications for the financial sector – posing both **business and reputational risks** for an industry that relies on digital infrastructure and technology. Organizations must be ready to deal with this **increasingly complex scenario**.

Top Security Threats[1]

- Ransomware
- Malware
- Social Engineering Threats
- Threats against data
- Threats against availability: Denial of Service

Some figures…



Ransomware Quickview[2]
June 2023

$5.13M

Average total cost of ransomware (3)

$4.45M

Average total cost of breach (3)

(1) Threat Landscape, ENISA, 2022 (2) State of Cyber Threat Intelligence, Flashpoint, 2023 (3) Cost of a data breach report, IBM, 2023

Cyber Attacks

Not if, but when

Know your environment

Know your weaknesses

Know the attacks and the attackers

> ***“There are only two types of companies: those that have been attacked and those that don't know it yet”***

Be prepared

Be ready for the unexpected

Raise awareness

Robert S. Mueller, former Director of the FBI, 2012

DORA regulation

What we did

DORA creates a **new regulatory framework** aiming to the **strengthening of the financial sector's resilience to security threats.** DORA sets **uniform requirements across all regulated European financial entities, including their ICT third-party service providers.**

UniCredit Group context

Initial assessment and gap analysis completed, leading to the identification of the **most relevant impacts**

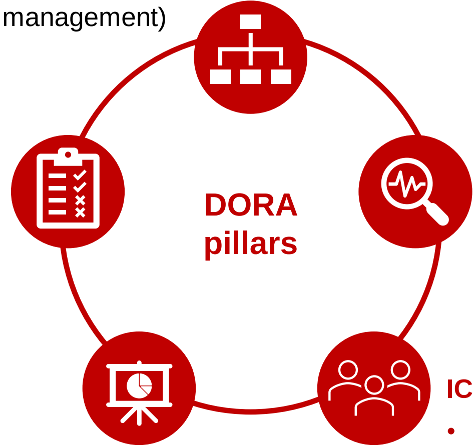
Active participation to the **public consultations on the first batch of RTS*** (DORA L2 documents)

Based on the RTS analysis and outcomes, **consolidation of the gap analysis and definition of the implementation plans**

**Regulatory Technical Standards*

DORA regulation

Main challenges for UniCredit



DORA pillars

ICT GOVERNANCE

- **Responsibilities of the Management Body**, requiring it to define, approve, oversee and be accountable **for the digital operational resilience management**
- **Awareness and training programs on digital resilience** (staff and management)

ICT RISK MANAGEMENT FRAMEWORK

- **ICT Risk Management Framework** (required to be approved by Management Body) including:
  - ○ **Digital Operational Resilience Strategy**
  - ○ **ICT risk tolerance level for ICT disruption scenarios supported by security KPIs and KRIs**

ICT THIRD-PARTY MANAGEMENT

- **Mapping of ICT third party service providers and link with the critical or important functions**
- **Resilience management in the UCG Third-party risk management**

ICT INCIDENT MANAGEMENT

- **Classification of incidents based on “materiality thresholds”** (e.g. data losses, geographical spread)
- **Classification of significant cyber threats**

DIGITAL OPERATIONAL RESILIENCE TESTING

- **Advanced threat-led penetration testing** extension to **all EU Legal Entities**
- **Technical specifications of testing subject to RTS** expected by January 2024

How we are dealing with this scenario

Our drivers

Continuous assessment, intelligence sources

Assessments aimed at measuring our overall posture and maturity level, also compared to the market, increasing our attractiveness and leading to potential savings.
Forward looking to anticipate cyber-risk trends.

External drivers

Threat Landscape
(ransomware, social engineering...)

Regulatory Requirements
(GDPR, SWIFT, PSD2, DORA...)

Business, Digital IT Strategy

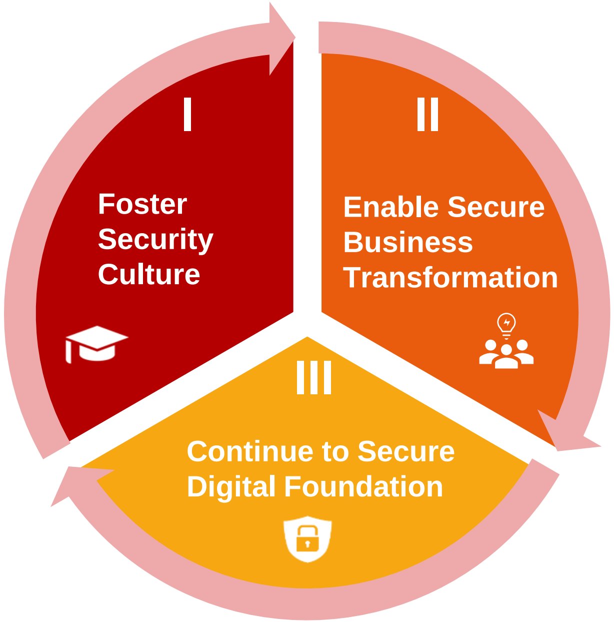
Considering Business Strategic Imperatives and Digital Transformation Pillars as inputs for our Security Strategy ensure full alignment with the Unlocked Strategy and with the Digital IT Strategy.

- I Insource Core Competency
- II New Way of Working
- III Reshape Arch & Platform
- IV Build Digital Experience

Group Security Strategy

Strategic Pillars 1/2

Considering internal/external inputs as well as strategic principles, **3 strategic pillars** have been identified. These pillars are used as "backbone" to **define and classify the evolution** initiatives.


I
Foster Security Culture
II
Enable Secure Business Transformation
III
Continue to Secure Digital Foundation

I

Continuous Upskilling also through hiring and nurturing of talents
Spread Security Awareness across the Group's Banks and Customers
Foster Security training and coaching

II

Security as an enabler to improve Digital Customer Journey
Customer Business centricity through Seamless User Experience
Seamless User Experience improving security automation in delivery
Secure customer's interests and Business operations

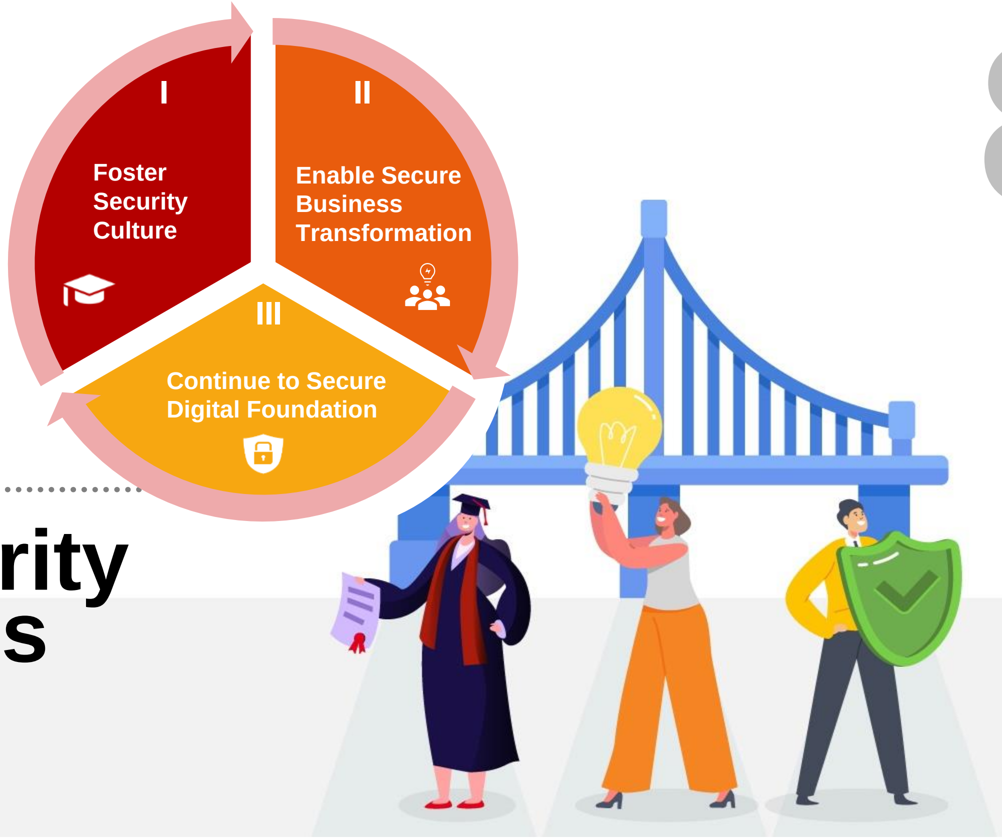
III

Flow transparently from on premises, hybrid and cloud grounds
Standard Digital Security Architecture flexibility and scalability
Improve our catalogue of security services to be consumed
Group-wide physical access control

Group Security Strategy

Strategic Pillars 2/2

3 Security Pillars



I
Foster Security Culture

II
Enable Secure Business Transformation

III
Continue to Secure Digital Foundation

8 Investment Areas

Foster Security Culture

- Security Culture and Oversight

Enable Secure Business Transformation

- Security Global Services & Products
- Single Sign On capabilities and Authentication service enhancement
- Customer Protection

Continue to secure Digital Foundation

- Secure Infrastructure Foundation
- Unified IAM Ecosystem
- Security Tech Stack
- Security Intelligence and Monitoring

Group Security Strategy

Approach for a Strategic Evolution

From	To
Fragmented technology	**Simplification** and **Standardization**
Fractionated User Experience	**Automation, transparency** and **biometrich authentication**
«Chasing the ambulance» response approach	**Proactive** and **preventive approach**
Straight risk reduction focus	Ensure **continuous risk mitigation** while **maximizing flawless user experience**

2023 Security Awareness Initiatives

Security starts from each of us

Main External Security Awareness Initiatives

«Conversations Unlocked» series - podcast on Spotify

«Outsmart love scammers» - article on One UniCredit

"Easy steps to navigate the web safely" video on One UniCredit and Social Media activities on Group Social Media platforms

«World Password Day» - Instagram story on Group profile

Article on «Forbes Italia»

HackInBo® Business Edition at Bologna - post on Group profile on LinkedIn

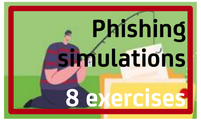
Security Culture Campaign – 5 Videos to be launched on UniCredit external channels in connection with ECSM

Main Internal Security Awareness Initiatives

8 Web-based trainings

New Authentication Methods

3 news



Phishing simulations

8 exercises

Security Culture

3 events

Security video cartoon

Internal Magazine article

Internal Social Media Platform, around 50 posts

Data Loss Prevention

1 news

2023 Culture Day

Security ready for the unexpected

as a service

as a differentiator

as a business

Q&A