



Cybersecurity and digital transformation for Financial Institutions

25/01/2024

Agenda



01 The Intesa Sanpaolo Group



02 Understanding cyber issues in Financial Services



03 Cybersecurity in Intesa Sanpaolo Group



04 Sum up



Intesa Sanpaolo is the leading Italian bank and a key player in the European and Global banking scene..



The Intesa Sanpaolo Group is one of the **leading banking groups in Europe** and is committed to supporting the economies of the countries in which it operates



Intesa Sanpaolo **is the leader in Italy in all business areas** (Retail, Corporate and Wealth Management)



The Group was formed through the merger of Banca Intesa and San Paolo IMI. Over the years, the Group has **acquired more than 20** Italian banks (e.g. UBI, Banco di Napoli, Banca dell'Adriatico)

13,6

million **customers in Italy**

~330

billion distributed to **the real economy** over the horizon of the next plan

3.349

branches in the Italian national territory

+90K

employees in the Group

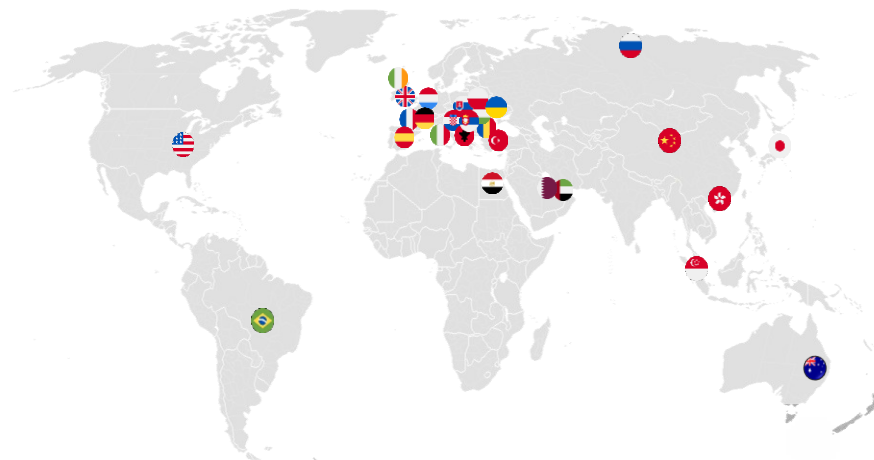
+300

billion in **Assets under Management**

32

billion in credit provided in 2021-2022 to support **ESG/Climate transition**, out of €76 bn for the period 2021-2026¹

Intesa Sanpaolo's presence in the world



Abroad, Intesa Sanpaolo has 7.2 M customers
and 944 branches

Agenda



01 The Intesa Sanpaolo Group



02 Understanding cyber issues in Financial Services



03 Cybersecurity in Intesa Sanpaolo Group



04 Sum up

Cybercrime is on the rise globally driven by the pandemic and geopolitical changes, targeting digitized services...

Key growth drivers



Increased relevance of digital channels for customer interactions and **instant payments**



Extension of digitized processes and increase of digital interactions with third parties



New geopolitical tensions which increased nation-state attacks



Global cyber attacks ²
Global fraud losses
Global Phishing attacks ⁴
Ransomware attacks ⁶
Cyber Incident ⁷

Daily reports of cyber attacks on the FBI³(#)



~ 2489

Number of cyber attacks with significant damage⁴ during 2022 (an increase of 60% of attacks detected)

362 Billions \$

Estimated losses for global fraud on online payments in '23-'28⁵

+52%

An **increased** of phishing attacks **during 2022** compared to 2021

+37%

An **increased during 2023** compared to 2022 (the average enterprise ransom payment exceeding \$100,000)

82%

Human error due to **inappropriate behavior** triggers cyber incidents.

1. Examples of attacks on Ukraine: WhisperGate destructive malware, February 23 DDoDs, HermeticWiper malware | 2. 30% of ransomware-based attacks with increased ransom demands | 3. Source: FBI Internet Crime Complaint Center | 4. Clusit Report 2023 on ICT security | 5. Juniper Research – July 2022 | 6. Zscaler ThreatLabz 2023 Ransomware | 7. IBM Cybersecurity Intelligence Index Report

In the context of the current evolving landscape of cyber risks stemming from the geopolitical tensions arising..



Economic goals

Hackers who attack to extort money



New



Geopolitical objective (disruption)

States that recruit hackers to create instability in enemy countries



Hacker pro Russia

Attacks on key national infrastructures of 'hostile' countries"



Hacker against Russia

Attacks on Groups present in Russia



ISP is subject to **both types of attacks**, being a key infrastructure, in addition to having a presence in Russia.

Our Strategic Intelligence confirms the presence of Nation – States as new threat actors



Nation-States as new threat actors

State-sponsored cyber attacks are an increasingly serious threat. They are often associated with certain countries, but increasing digitalization has extended the ability to carry out attacks to virtually all countries.

Used techniques



Block of corporate data (Ransomware)

- Increase of attacks, with the use of innovative techniques
- Diffusion on web of "cyber attack weapons" for less experienced attackers



Interruption of service (DDoS²)

- Innovative attacks that combine multiple known techniques in a single event
- Attacks to evaluate the ability of anti-DDoS providers to guarantee at the same time service levels to their clients



Exploited weaknesses



Unprotected access

- A single **user without Multi Factor Authentication** caused a health insurance company to lose 10 million data (with a potential fine of around €32 million)
- The exploitation of the **credentials of an external collaborator** allowed access to critical Uber systems



































Unprotected services

- Web exposure of **services without adequate security measures** caused a data breach for a telephone company, impacting 10 million customers

More than 82% of successful cyber attacks use the human factor as a weakness

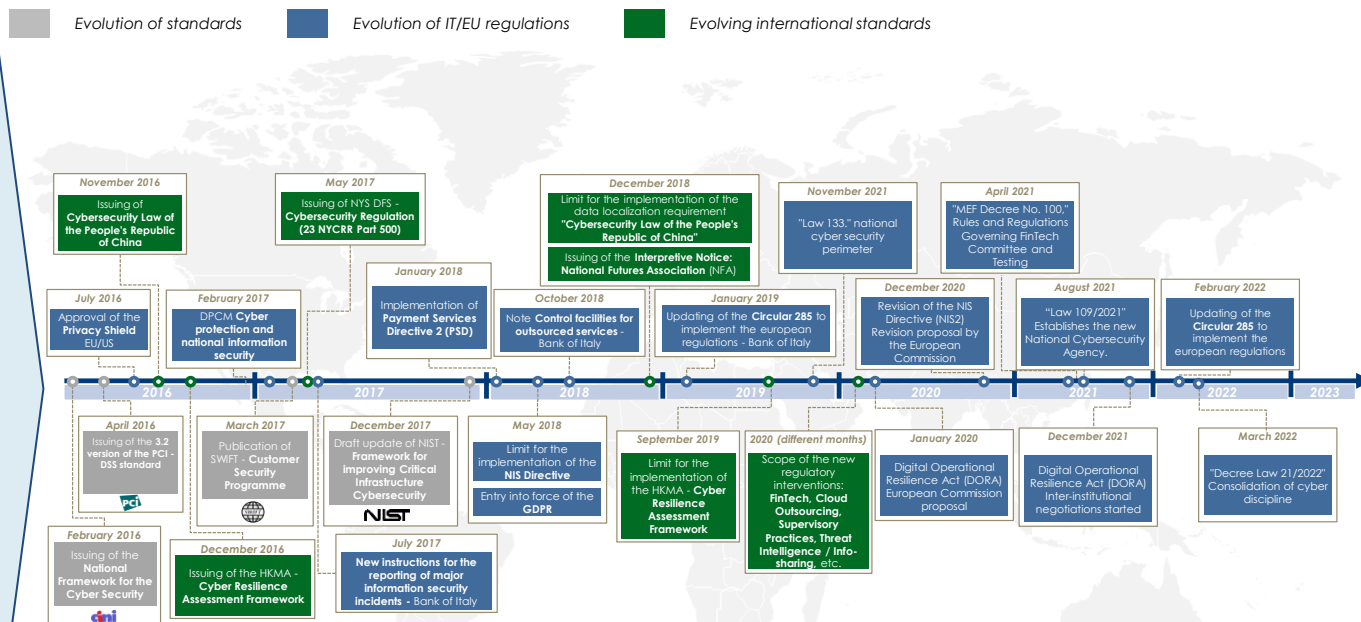
1. Source: Hakluyt's Strategic Intelligence report - 2022 | 2. DDoS (Distributed Denial of Services) consists, simplifying, of a type of computer attack that attempts to make a website or a network resource unavailable by overloading them with harmful traffic and thus making them unusable.

..highlighting a significant rise in ransomware attacks

Company	Date of attack	Attack description	Other attacks
	January 2021	"Supply-chain" attack developed over 1.5 years to insert a vulnerability in SolarWind's Orion Software, which allowed it to spy on all users who used it	<div>2021</div> <div>     </div>
	May 2021	"Ransomware" attack made with advanced tools that prompted the company to make the decision to block the pipeline to contain the attack	<div>     </div>
	July 2021	"Ransomware" attack considered the largest attack in history, as it spread to about 1,000 of its clients and 40,000 computers worldwide	<div>     </div> <div>     </div>
	November 2021	"Ransomware" attack that crashed information systems . The company admitted that stores, including those in Italy, had their terminals down for four days during the Black Friday period	<div>2022</div> <div>     </div>
	March 2022	"Ransomware" attack introduced through one of the system administrators' accounts , which blocked timetable boards and disabled ticket machines at several stations for up to two days	<div>     </div>
	February 2023	"Ransomware" attack that has blocked ION systems for listed derivatives, disrupting service delivery for several significant financial institutions .	<div>2023 YTD</div> <div>   </div>

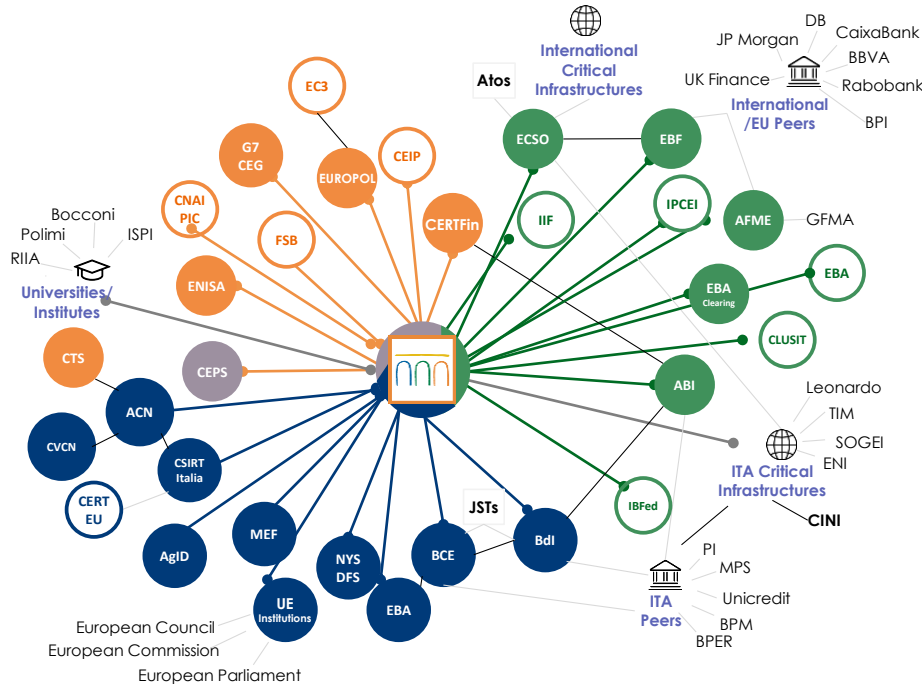
Furthermore, in recent years, lawmakers and "Standard Settlers" have been particularly focused on cybersecurity

In recent years, the various bodies that regulate aspects of **cybersecurity in the financial world** have increased their focus on cybersecurity, with a **substantial body of legislation** being produced both **nationally and internationally**



..and we continuously engage in activities to guarantee and strengthen collaboration with stakeholders

● Regulator ● Entity ○ Low interaction



- **EBF¹** : support to the drafting of **detail requirements** of **DORA** as Chair of Cybersecurity Expert Group EBF¹
- **G7² Cyber Expert Group**: participation in operational tables to propose actions in the field of **third party cyber risk management**
- **FSB³** : contribution to the definition of the **framework** for the convergence and **harmonization** of **Cyber Incident Reporting** at an international level
- **EUROPOL⁴** : process underway to create a partnership and to include ISP in the **advisory group finance**
- **ACN⁵** : collaboration on **Technical Scientific Committee**, and start defining a national **Hypersoc** and **Vault**

..whats next?



Outlook

The aftermath of the COVID-19 pandemic and ongoing Russia-Ukraine war has exposed cracks in societies that are being further strained by episodic upheaval. Yet the global system has thus far proved surprisingly resilient. A widely anticipated recession failed to materialize last year, and financial turbulence was quickly subdued, but **the outlook remains uncertain.**

Global risk ranked by severity (2 years)¹



Misinformation and disinformation



Extreme weather events



Societal insecurity



Cyber in-security



Interstate armed conflict

1. World Economic Forum Global Risks Perception Survey 2023 – 2024 | Cyber Pandemic: [link](#)

Agenda



01 The Intesa Sanpaolo Group



02 Understanding cyber issues in Financial Services

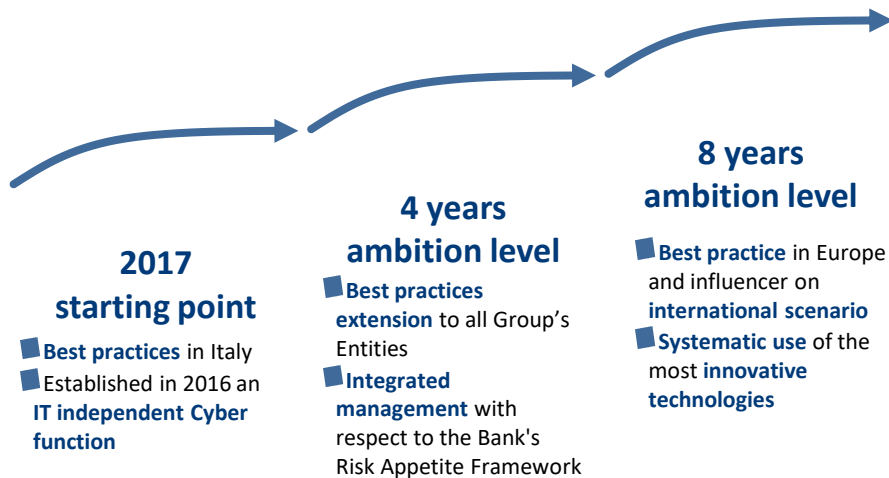


03 Cybersecurity in Intesa Sanpaolo Group



04 Sum up

In 2017 the Group started the evolution of Cybersecurity & Business Continuity, with a high level of ambition..



Since 2018, the **Group's Cyber Plan** is annually updated and approved by the Board of Directors



The Plan introduced a **new holistic approach** for addressing Cyber issues through **technological controls** and new **organizational, process and human factor controls**



An integral part of the Plan is **Strategic Intelligence**, which analyzes the external macro-context to outline the main Cyber threats on the **Intesa Sanpaolo Group context**

The cyber 22-25 plan has been updated consistent with the changing external environment and the new ISP Business Plan



The continuous increase in **digitization** and the introduction of new ways of working..



...result in the **growth** of Cyber risk, with significant increases in attempts to defraud customers and attacks on infrastructure..



...which require the **strengthening of safeguards** for the whole Group and **throughout the value chain** to avoid the "weak link"

Ambition 22-25

Fostering a secure and resilient path of customer digitization, increasing society's confidence in the digital economy and the Group's competitive advantage

Key objectives

Protecting the Bank and Customers using the most innovative technologies and anticipating future threats

Making Cybersecurity a key factor in the ESG sustainability of the digital economy, for all stakeholders

Grow and become an international benchmark

Agenda



01 The Intesa Sanpaolo Group



02 Understanding cyber issues in Financial Services



03 Cybersecurity in Intesa Sanpaolo Group



04 Sum up



Artificial Intelligence

And digitalization



Human in the loop

82%

Incidents are caused by improper behavior.

Increasingly Digital Criminals



New threats



Cyber Security

and awareness

362

Billions of Dollars in Losses²



Economic Impacts



Reputational Impacts



Geopolitical objective

Global Pandemic





Mauro Marigliano
[Mail me](#)
[LinkedIn](#)