CYBERSECURITY @ *BARILLA*

Alberto Maldino

Cybersecurity Director, Barilla Group

08/10/2024

Barilla
The Italian Food Company. Since 1877.

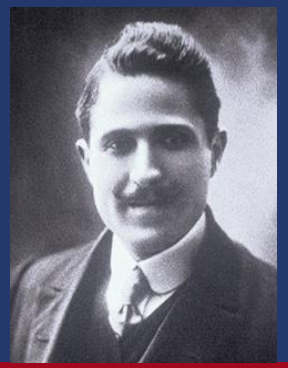
THE *JOY OF FOOD* FOR A *BETTER LIFE*

BRINGING PEOPLE
CLOSER TO THE JOY OF GOOD FOOD
AND MAKING QUALITY
THE CHOICE FOR A BETTER LIFE,
FROM EACH INDIVIDUAL TO THE PLANET.

BECAUSE THIS IS HOW WE ARE
NURTURING THE FUTURE, *TODAY*.

Barilla
The Italian Food Company. Since 1877.

THE ITALIAN FOOD COMPANY. *SINCE 1877.*



PIETRO BARILLA

1877-1912

GUALTIERO and RICCARDO BARILLA

1912 - 1947

GIANNI and PIETRO BARILLA

1947 - 1993

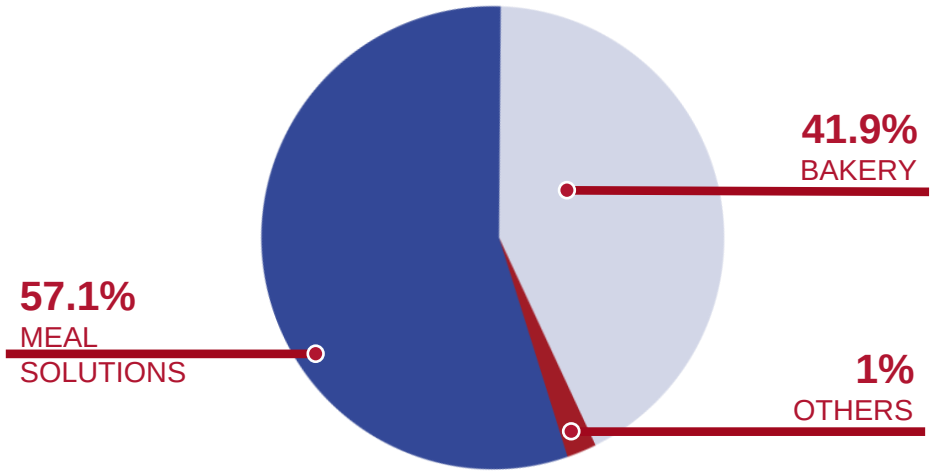
GUIDO, LUCA and PAOLO BARILLA

1993 - TODAY

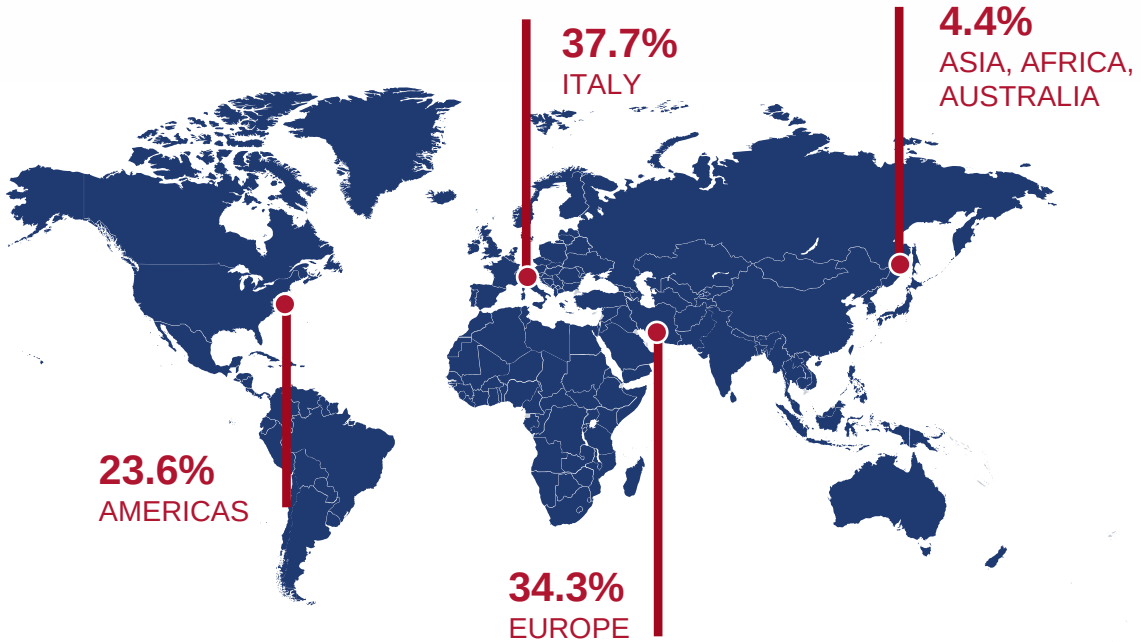
Barilla
The Italian Food Company. Since 1877.

BARILLA GROUP *PROFILE*

TURNOVER BY BUSINESS AREA*
(4,869 MILLIONS EURO)



TURNOVER BY GEOGRAPHICAL AREA*



* Financial Report 2023

MORE THAN **1,995,000** TONS OF **OUR PRODUCTS** ACCOMPANY MILLIONS OF PEOPLE DURING MOMENTS OF CONSUMPTION THROUGHOUT THE DAY

The information relate to Barilla Group for the period from 1st January to 31st December 2023

PASTA, SAUCES, READY MEALS*

BAKERY*

OTHER BUSINESSES*

* Year To Date

BARILLA
IN THE WORLD

UNITED STATES	CANADA	MEXICO	BRAZIL
1	1	1	1
2	1	1	1
1			

EUROPE	UK	ITALY	TURKEY	UNITED ARAB EMIRATES	RUSSIA	SINGAPORE	JAPAN
15	1	1	1	1	1	1	1
8	1	2	1		1	CHINA	AUSTRALIA
		15				1	1
		1					
		1					

9,040
BARILLA
PEOPLE
*this data includes employees from Pasta Evangelists and Barilla Mexico

20
BRANDS
* Year to date

30
PRODUCTION
DISTRICTS
*that envisage one or more sites

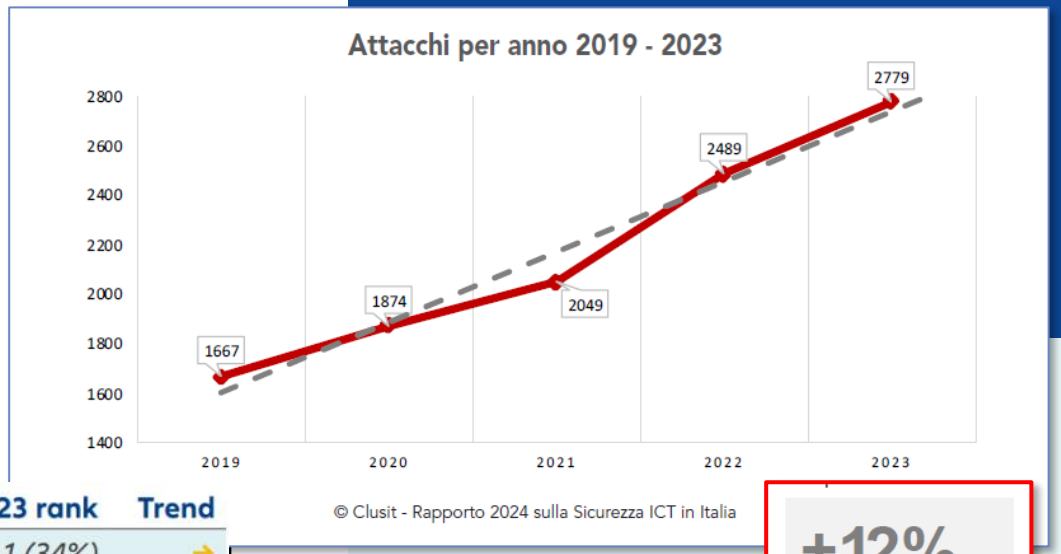
15 IN ITALY
15 ABROAD

Barilla
The Italian Food Company. Since 1877.

Facts & Figures

Cyber Attacks Trends

Allianz's latest research underscores the diverse risks looming over businesses in 2024, urging proactive strategies for resilience and mitigation.



+12%

è la crescita degli incidenti dal 2022 al 2023

The most important business risks in 2024: Global

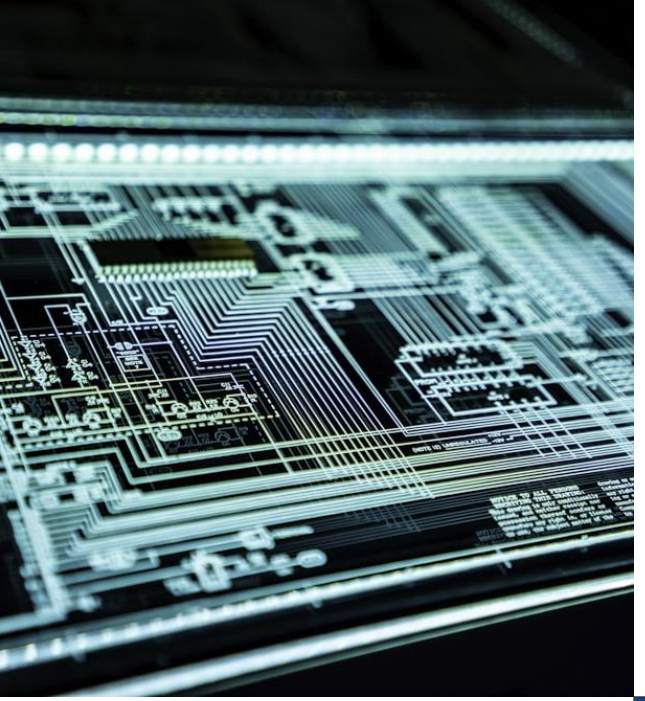
Rank		Percent	2023 rank	Trend
1	Cyber incidents *(e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)*	**36%**	*1 (34%)*	→
2	Business interruption *(incl. supply chain disruption)*	**31%**	*2 (34%)*	→
3	Natural catastrophes *(e.g., storm, flood, earthquake, wildfire, extreme weather events)*	**26%**	*6 (19%)*	↑
4	Changes in legislation and regulation *(e.g., tariffs, economic sanctions, protectionism, Euro-zone disintegration)*[1]	**19%**	*5 (19%)*	↑
5	Macroeconomic developments *(e.g., inflation, deflation, monetary policies, austerity programs)*[2]	**19%**	*3 (25%)*	↓
6	Fire, explosion	**19%**	*9 (14%)*	↑
7	Climate change *(e.g., physical, operational, and financial risks as a result of global warming)*	**18%**	*7 (17%)*	→
8	Political risks and violence *(e.g., political instability, war, terrorism, coup d'état, civil commotion, strikes, riots, looting)*	**14%**	*10 (13%)*	↑
9	Market developments *(e.g., intensified competition / new entrants, M&A, market stagnation, market fluctuation)*	**13%**	*11 (11%)*	↑
10	Shortage of skilled workforce[3]	**12%**	*8 (14%)*	↓

Source: Allianz Risk Barometer 2024

So What?

Cyber incidents such as **ransomware attacks, data breaches and IT disruptions** are the biggest concern for companies worldwide in 2024.

Barilla
The Italian Food Company. Since 1877.



Facts & Figures

Cyber Attacks Trends

17%

of these incidents in the Manufacturing industry involved the use of **Ransomware attacks**

IBM's recent research has unveiled compelling insights and data regarding the sectors **most impacted by cyber attacks from 2020 to present**, once again placing the **manufacturing sector in the first place**.

25.7%

of incidents within the top 10 industries targeted the **Manufacturing** industry

#1

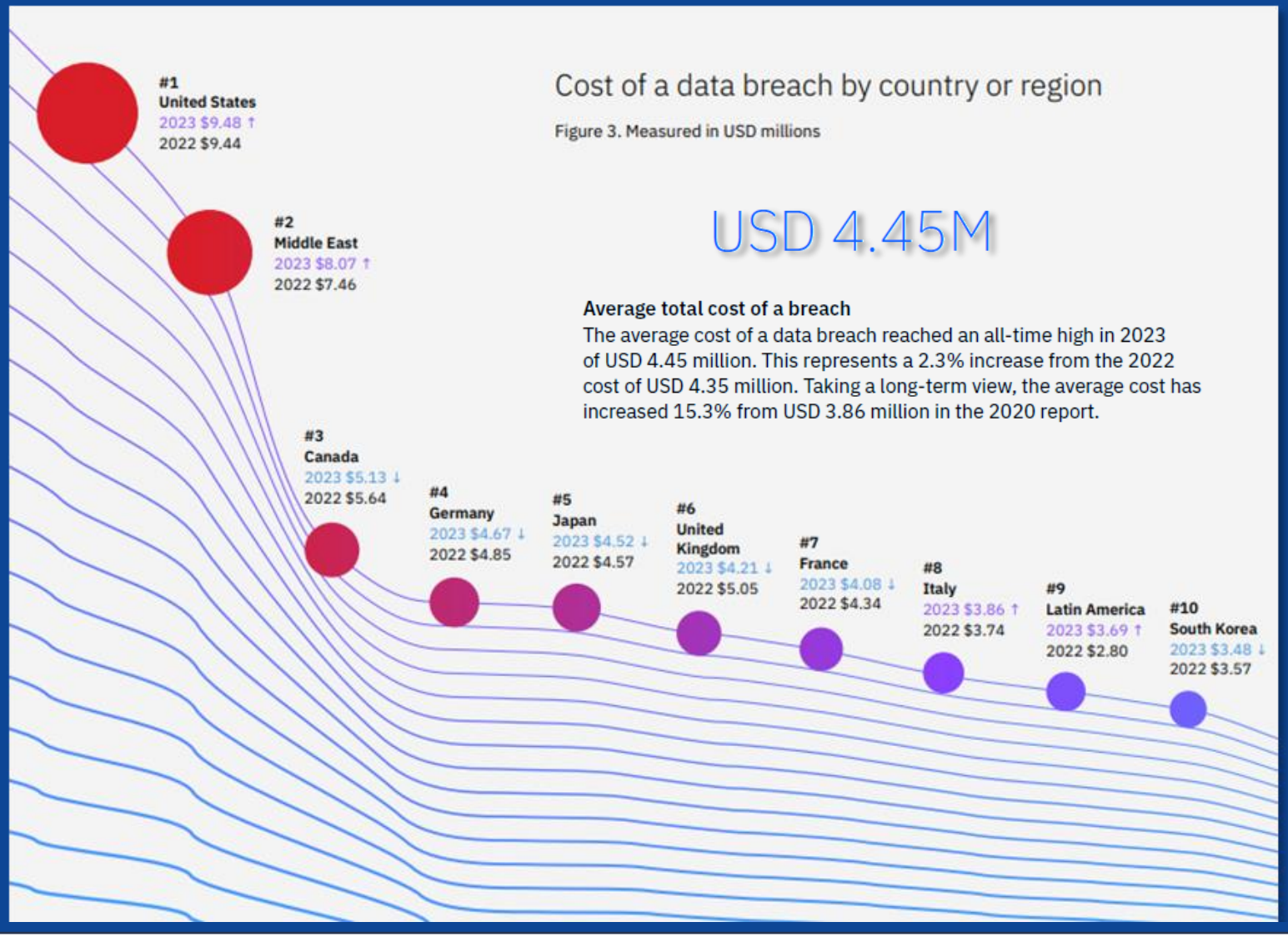
The **Manufacturing** sector stands at the **forefront** as the most targeted industry for cyberattacks worldwide, with a constant increase since 2019

Share of attacks by industry 2019–2023

Industry	2023	2022	2021
Manufacturing	25.7%	24.8	23.2
Finance and insurance	18.2%	18.9	22.4
Professional, business and consumer services	15.4%	14.6	12.7
Energy	11.1%	10.7	8.2
Retail and wholesale	10.7%	8.7	7.3
Healthcare	6.3%	5.8	5.1
Government	4.3%	4.8	2.8
Transportation	4.3%	3.9	4
Education	2.8%	7.3	2.8
Media and telecommunications	1.2%	0.5	2.5

Source: IBM X-Force Threat Intelligence Index 2024

Facts & Figures



IBM's report highlights the costs of data breaches in the world, with **all Regions where Barilla operates in the first places**.

So What?

This underscores the critical need for heightened awareness and proactive measures across industries to effectively mitigate both financial and reputational risks associated with data breaches.

Source: IBM Cost of a Data Breach Report 2023

Barilla
The Italian Food Company. Since 1877.

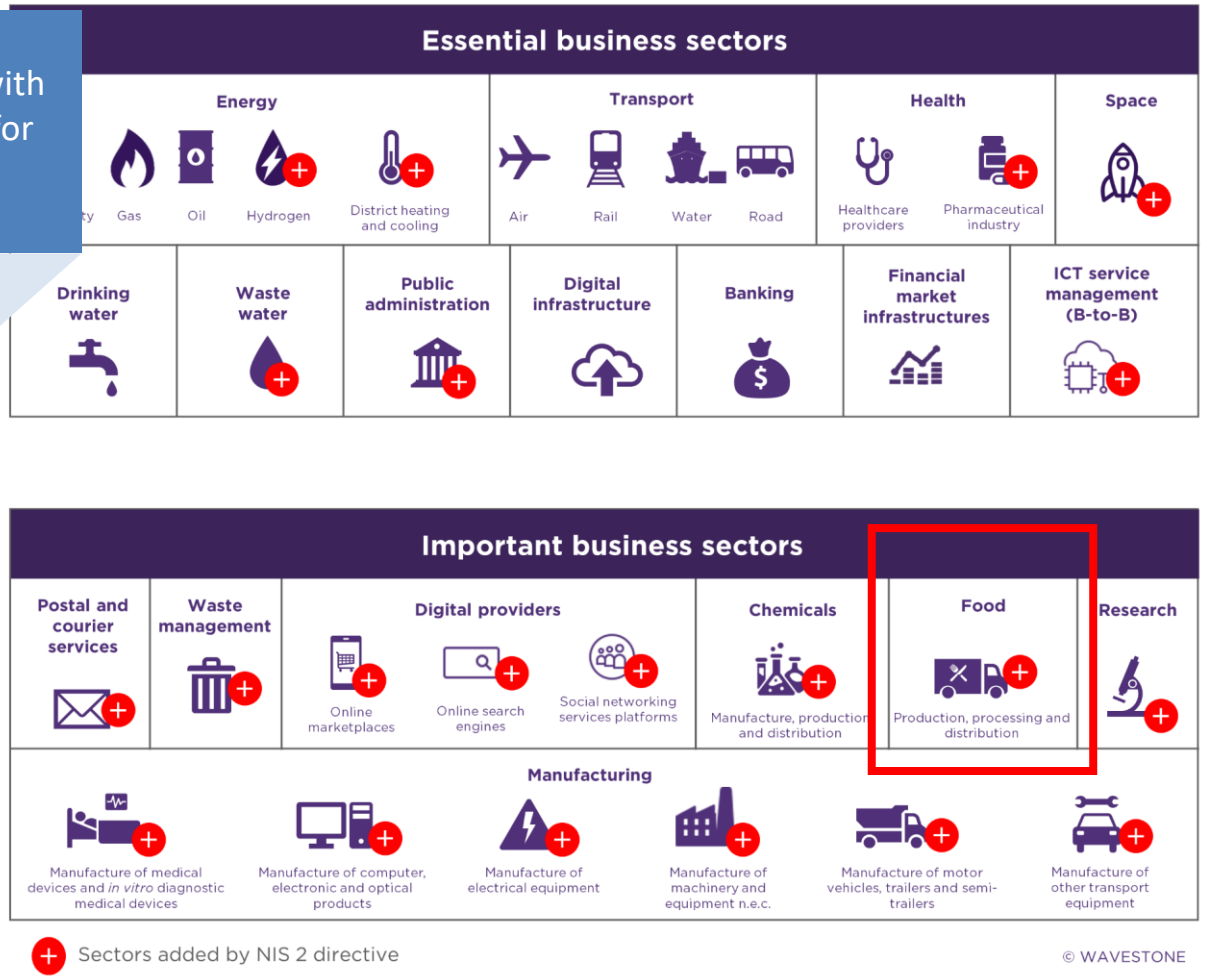
NIS 2 EU Directive
Objectives and impacted sectors

The **NIS2 Directive** is the evolution of the EU NIS directive (implemented in Italy with Legislative Decree no. 65/2018) and establishes the minimum-security measures for a common level of security of networks and information systems in the EU

The NIS2 Directive sets some objectives such as **increasing the resilience and incident response capabilities** of the interested parties, providing more specific indications in the field of Cybersecurity and the protection of Critical Infrastructures

Compared to the previous legislation (NIS) **additional obligations and provisions** have been defined and included.

The **number of subjects involved has increased**.



The Barilla Cyber way

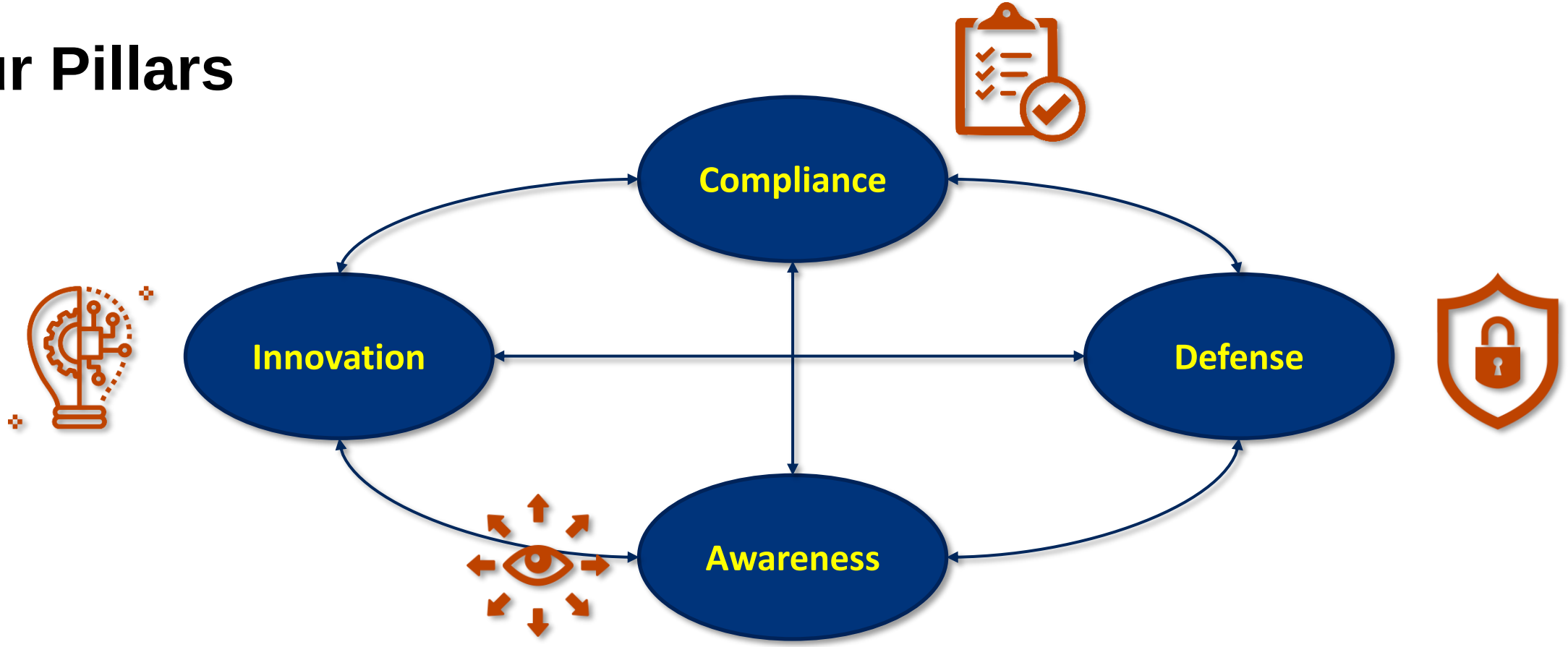
Our **Mission**

01. Protect Barilla digital assets, identities and information through **proactive and reactive cybersecurity technologies and processes**, in **continuous improvement**

02. Promote a **culture of cybersecurity awareness** and **cooperation** to mitigate risks and ensure trust and confidence in Barilla operations, **through people**

Barilla
The Italian Food Company. Since 1877.

Our Pillars



Security by design, embedded in project management

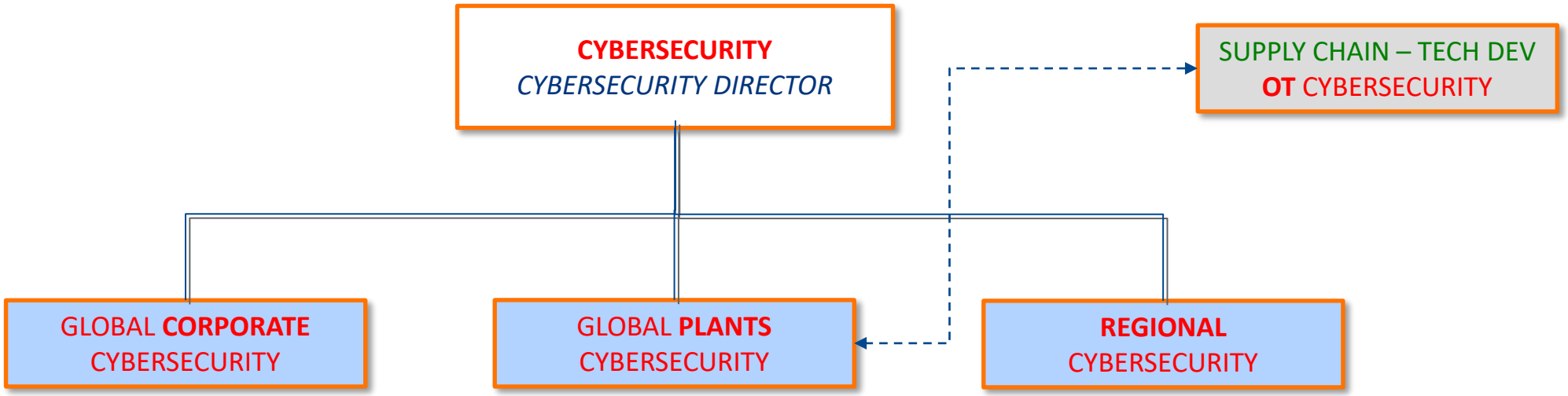
✓ Strategic **attention by top management** to **cyber security** as **key for business success**

✓ Extensive **cooperation** with relevant **external stakeholders** (business peers, networks, institutions, …)

Cross-functional cooperation : IT, Privacy, Compliance, Audit, HR, ERM, Supply Chain, Crisis Team.

The Barilla Cybersecurity Team

Cybersecurity team is part of Infrastructure, Architecture & Cybersecurity unit within Barilla "Group Digital & Business Technology", ultimately reporting to CFO



- An extremely **lean organization** with **multiple services** and tasks, supported by a few **trusted external partners**.
- Ability to act as «**one team**» with strong cooperation in all areas and loose boundaries if needed.

Cross-Functional Cooperation

Cyber protect together

Cross-functional cooperation is the cornerstone of Barilla cybersecurity strategy, as we recognize the critical importance of **working seamlessly across departments and with external stakeholders** to fortify our defenses against evolving cyber threats

- **Group Digital & Business Technology**

To ensure that security measures are integrated into every Barilla digital project in a ***security by design*** fashion.

- **Internal Audit**

To **review and address security gaps**, promote **continuous improvement**, and manage organizational risks effectively.

- **Legal and Compliance**

To guarantee **regulatory compliance** and **data privacy** wherever we operate

- **Human Resources**

To deliver and **enforce cybersecurity culture** across all Barilla people and **ensure organizational fit**.

- **Enterprise Risk Management**

To **include and harmonize cyber risk** into Barilla risk management practice.

- **Supply Chain – Technical Development**

Partnering with the dedicated "OT Cybersecurity" team in SC, to design, manage and operate **cyber protection for our plants**.

- **Corporate Crisis Team**

To **get ready in case of company crisis** originated from a cyber incident and orchestrate a **business-wise response**.

- **External entities**

To create and nurture relationships with **authorities**, public **institutions**, **law enforcement**, **universities**, technological **partners** and other **peers**, for an active network of information exchange and prompt support.

- ***… and ALL Business stakeholders***

*To **identify** and anticipate cyber risks, **protect** business information assets and provide a joint **reaction** to cyber events.*

Barilla ISO 27001

In 2018, Barilla has decided to undertake the **ISO 27001 certification process** of its **Information Security Management Systems** (**ISMS**), following a strategic **progressive path** guided by **three main drivers/benefits**

The certification of the Information Security Management System (ISMS):

1. requires a strengthening of the processes for the management of information security, guaranteeing **secure and reliable services to the business and the whole company** – ***Internal Environment***;
2. supports **compliance with** the requirements expressed by **contracts, laws and regulations** (GDPR, NIS2, etc.) – ***Compliance requirements***
3. offers an **impartial view of the ISMS**, facilitating and encouraging **relationships with the external market** about continuity of production, product integrity, intellectual property etc. – ***External market***.

Current scope

Planning, Design, Implementation, Operation and Support provided for Barilla worldwide by Group Digital & Business Technology Units for the following services:

- ***IT Security***
- ***Workstation & Mobility***
- ***Network & Communication***
- ***System Architecture & Governance***
- ***Resiliency***
- ***Application Development***
- ***Consumer Digital Technologies***

Certified locations

(where audited services are based)

- Parma (HQ)
- Western Europe
- Northern Europe

Upcoming (2024)…

- Central Europe
- Eastern Europe
- …

Barilla Cyber Context

Barilla Point-of-View

Barilla contends with a myriad of **cyber threats on a daily basis**. From phishing attempts aimed at getting people's credentials and compromising sensitive data, to sophisticated social engineering schemes targeting key employees, the company navigates a complex cyber landscape. Here are some examples:

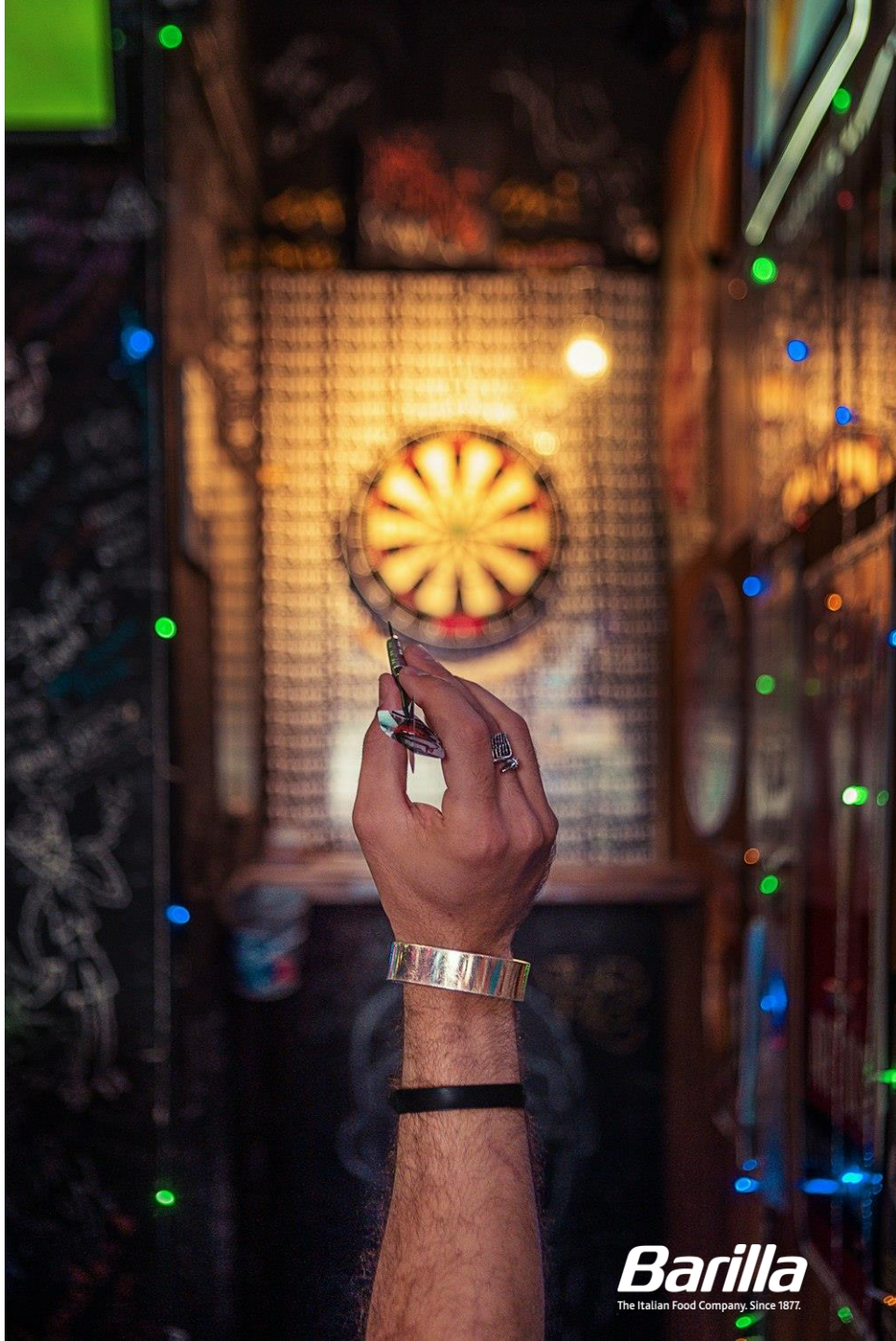
Brute-force Attacks
Brute-force attacks on credentials are on the rise, targeting users' accounts

Phishing
Relevant increase in phishing attempts and malicious mail

Supply Chain Attacks
More and more key suppliers and third parties attacked all over the world

Social Engineering
Rise in social engineering attacks, strategically crafted to manipulate individuals within the company.

Network Attacks
Barilla is experiencing continued pressure on border protection and intrusion attempts from outside



Cyber Security
The Barilla figures

ISO 27001 certified since 2018

More than

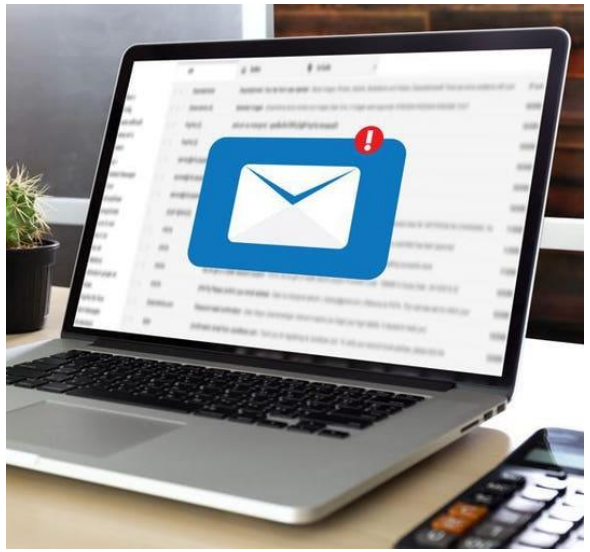
30

Cybersecurity tools and solution for protection

More than

6.000

Cybersecurity relevant **events** yearly managed



More than

36 Million

malicious inbound mail messages yearly blocked

More than

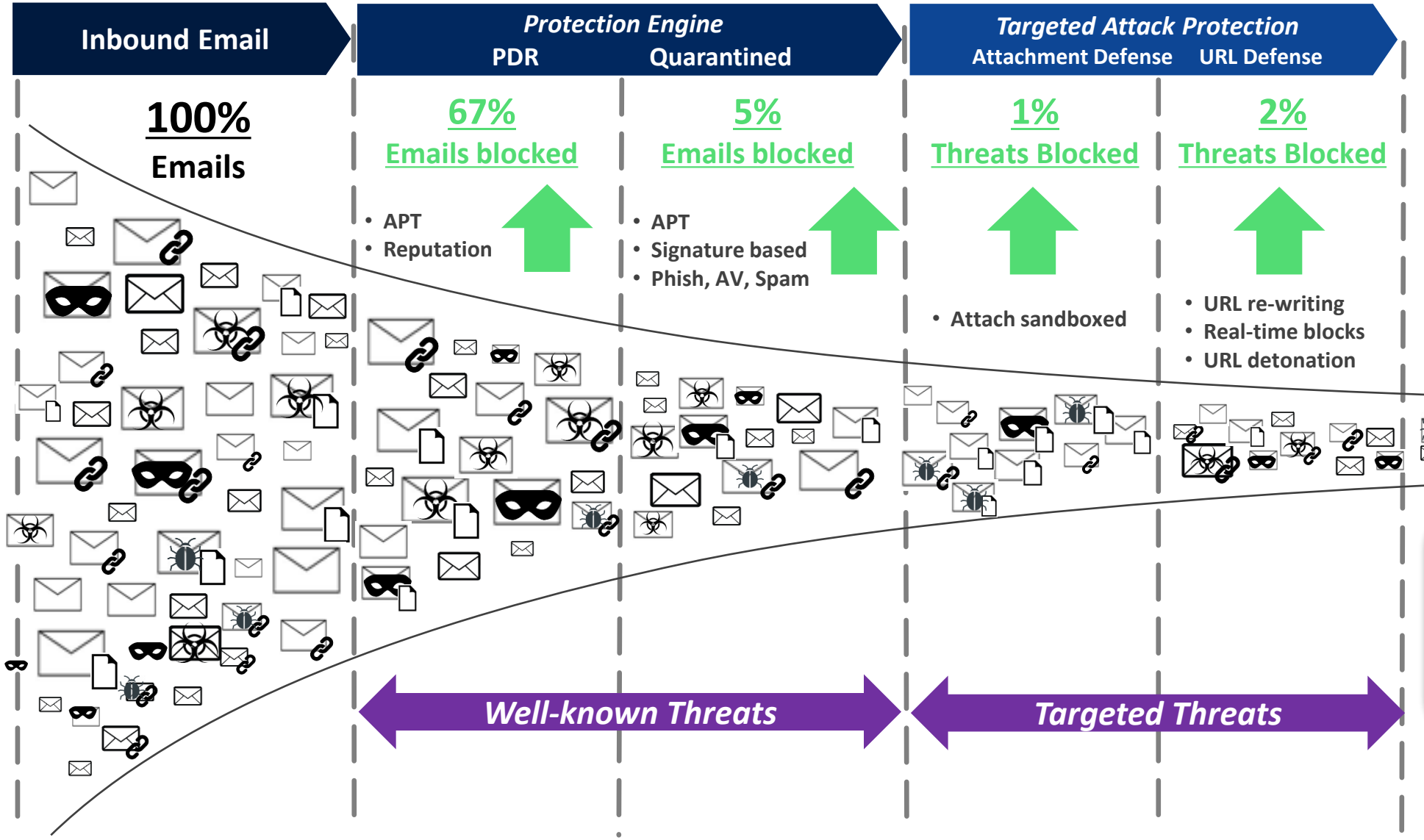
55.000

Cybersecurity vulnerabilities remediated during last year

The Italian Food Company. Since 1877.

Cyber Context
Mail Protection

In a **typical month**, most inbound e-mails to @barilla.com recipients (**millions!**) are **filtered out** due to **threats**.



25%
Emails delivered to final recipients

Increasing trend of blocked threats:
both generic (widespread) and targeted (aimed at Barilla people)

Barilla
The Italian Food Company. Since 1877.

Context & Drivers for ISMS (and related cybersecurity projects)

All components are **equally crucial in project prioritization**.

ISMS Fundamentals
- Objectives from ISMS Manual + yearly add-ons
- Monitoring

ISMS Risk Treatment Plan (RTP)
- Yearly RTP

Barilla IT Fundamentals
- Project Portfolio
- Digital Architecture

Cyber governance enhancements
- Incident/Crisis Response
- Special Programs

Context
- Business
- Cybersecurity (trends, threats, incidents, …)
- Regulatory compliance
- Authorities & Law Enforcement

Audit
- Auditors' recos

Goal: to achieve full and continuous consistency of **security projects portfolio** vs **risk evaluation**, **Barilla assets & priorities** and **changing context**.

Barilla
The Italian Food Company. Since 1877.

Hot topics

ISO 27001 geographical extension

Security by design

Plant/Regional cyber enforcement

Third-party cyber risk/incidents

Cyber Incident/Crisis management

Improve security of (multi)cloud services

Global Identity and Access Protection

Fight against vulnerabilities and obsolescence

Getting ready for NIS 2 Directive…

Cybersecurity Awareness

We **all** are responsible **for the security of Barilla**, by adopting correct behaviors and actions

OneLearning Courses

Mandatory cybersecurity courses are available on eLearning platform.

These courses help to recognize and deal with main security threats

Phishing Simulation

Test the ability of users to spot a phishing e-mail, providing an immediate and targeted training moment

Cybersecurity Warnings

Broadcast security warnings sent to all Barilla people, whenever needed, about emerging or widespread threats.

Mini animated Series

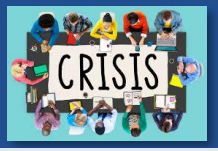
Cybersecurity and Privacy teams together launched animated series (also available as eLearning)

Town Hall Attendance

Cybersecurity team participates to town halls to spread cyber awareness where business people usually meet

Cybersecurity Newsletters

The Cybersecurity Chronicles provide a fresh view on major cyber risks that may affect us and the best practices to be followed



Incident Response Exercises

Table-top exercises to simulate a cyber incident or cyber crisis, with technical and business audiences

Barilla
The Italian Food Company. Since 1877.

OT Cybersecurity

Barilla plant cybersecurity approach is based on a "*defense-in-depth*" approach with interventions at different levels:

Perimeter

- Next Generation Firewalls
- MFA for VPNs connections
- Secure Remote Access

OT Network

- Revamping of OT networks
- OT Threat Detection

Systems on the OT Network

- Asset discovery/inventory
- Device hardening
- Endpoint Protection

Users

- Specific cyber security training
- General awareness campaigns

Security by design

- Partnering with Technical Development team in Supply Chain, define and apply secure design principles for new automation projects

Barilla
The Italian Food Company. Since 1877.

Regional Cybersecurity

The Regional Cybersecurity Team is dedicated to the management and mitigation of cybersecurity risks in all **Barilla's regions**, with the aim of improving each region's cybersecurity posture. In line with Barilla corporate strategy of decentralization, each region is closely followed and supported by a **dedicated Regional Cybersecurity Professional**, in order to **maximize support** to local IT and users in the region.

Every year, the Team develops a **Cybersecurity Program** composed by a set of projects and activities tailored to each region, which is periodically reviewed and updated by each Regional Cybersecurity Professional. This program takes into account different local contexts: **organizational**, **technical** and of **processes.**

In line with the **Information Security Management System** adopted for the management of HQ IT services in the ISO27001 scope, a **proper governance** of all local IT services and processes and a **security-by-design approach** is promoted (e.g., through the definition of policies, standards, procedures and guidelines). Furthermore, each region is also supported in the extension of the ISO27001 certification when required.

The Regional Cybersecurity Team is committed to support Local ITs by providing each region the necessary **cybersecurity guidance**. Moreover, a specific focus is given to **cybersecurity incident management** preparation and response activities and to **spreading cybersecurity awareness** across regions (e.g., through phishing simulations, newsletters, training sessions, etc..).

Supplier Cyber Risk Management

In such a complex and evolving context, we are working to

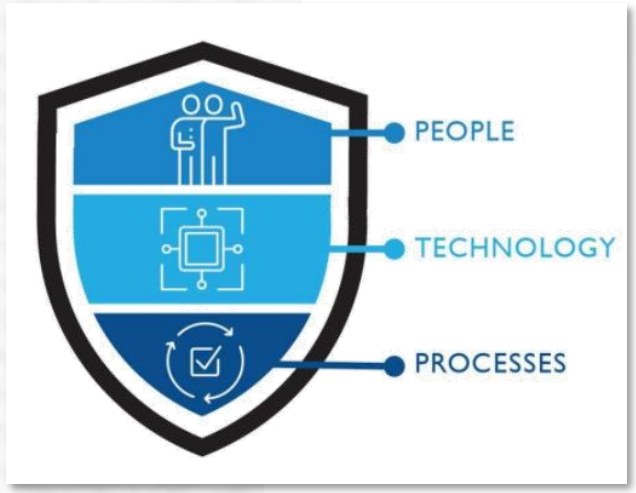
Establish a governance framework for supplier cyber risk

Promote a culture of cyber security in our supplier base

Barilla
The Italian Food Company. Since 1877.

CONOSCERE E *STRUTTURARE* L'ORGANIZZAZIONE

- Quali **rischi**?
- Quali **punti deboli**?
- Quali **informazioni pregiate**?
- Quali **possibili attaccanti**?
- Quali **vincoli normativi**?



Dotarsi di **ruoli interni deputati** (e possibilmente dedicati) alla gestione della *cybersecurity*

Gli ***standard*** di riferimento: guida "pronta all'uso", opportunità di crescita, non mero adempimento formale

ISO 27001

CIS Center for Internet Security®

NIS2 Directive

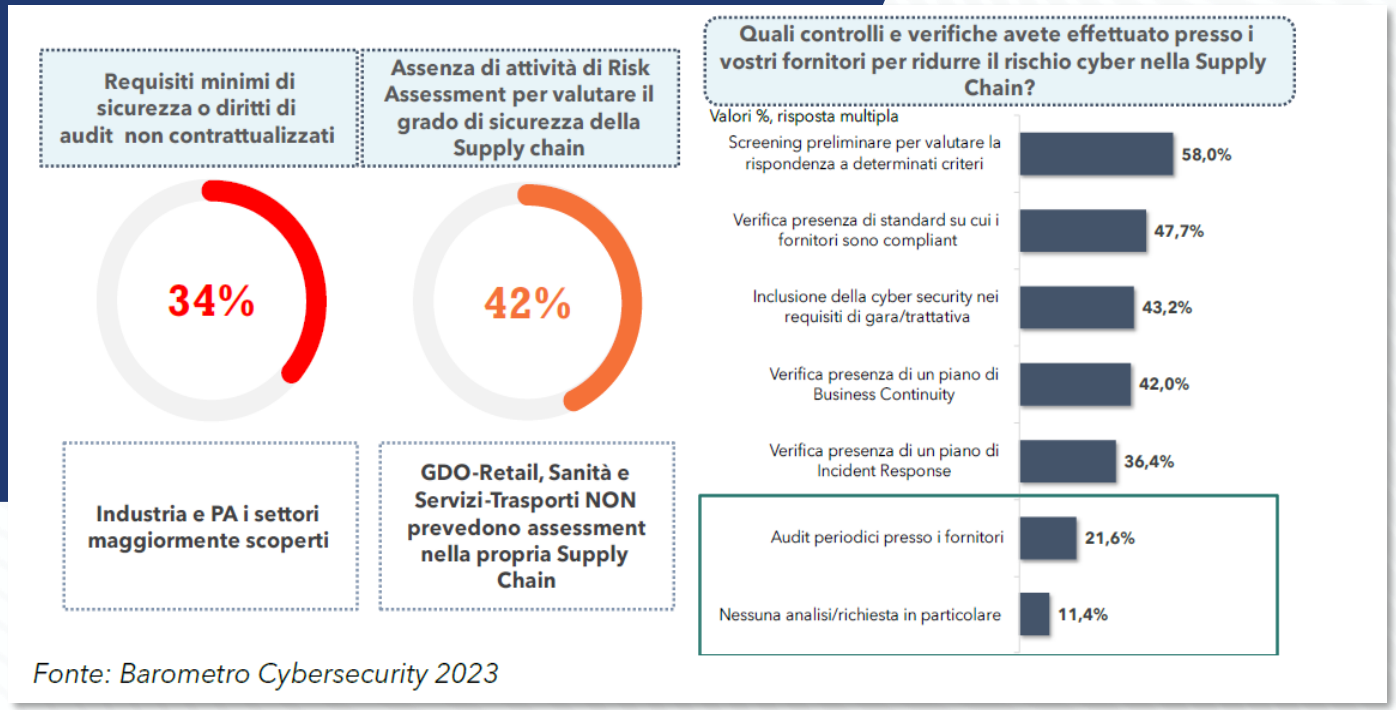
NIST CSF

ISA IEC 62443

Nuove **normative di ambito** come elemento di **coerenza sistemica**

La *cybersecurity* come **sfida continua e collettiva**: IT, Risorse Umane, Legale, Finanza/*Risk*, Produzione, … , Alta Direzione

CONOSCERE E *RAFFORZARE* LE PROPRIE FILIERE



Fonte: Barometro Cybersecurity 2023

- Quali i ***partner*** **vitali** per la continuità operativa?
- Quali gli "**anelli deboli**" nelle catene di approvvigionamento e distribuzione?
- Verso quali soggetti la <u>mia</u> organizzazione può essere **veicolo d'attacco**?

Obblighi contrattuali di:
- valutazione del rischio
- requisiti tecnico-organizzativi
- facoltà di *audit*
- notifica di incidenti *cyber*

Standard di riferimento, ma soprattutto promozione di una **cultura partecipata** del rischio *cyber* di filiera

Opportunità di "**effetto traino**" positivo nel settore agroalimentare

TECNOLOGIA “QUANTO BASTA”

Addizione di tecnologie di protezione non adeguatamente gestite
→ Falso senso di sicurezza

Equilibrio tra presìdi tecnologici e capacità di gestirli e mantenerli in efficienza
→ Rischio vulnerabilità “*boomerang*”

Le minacce *cyber* sono persistenti e dinamiche
→ Importanza di un monitoraggio continuo e professionale dei sistemi di difesa e di strategie organizzate di risposta

La tecnologia da sola NON è la soluzione, nemmeno per le organizzazioni più piccole

Un eccesso di tecnologie non coordinate può trasformarsi in minaccia

LE *PERSONE AL CENTRO*

Le persone sono sempre la prima e l'ultima linea di difesa dagli attacchi *cyber* → il "*firewall* umano"

Nel valutare la propria esposizione e risposta alle minacce *cyber*, da ricordare che anche gli attaccanti sono persone ed operano secondo schemi, finalità e tattiche criminali "profondamente umane": inganno, pressione psicologica, massimo profitto con minimo sforzo, …

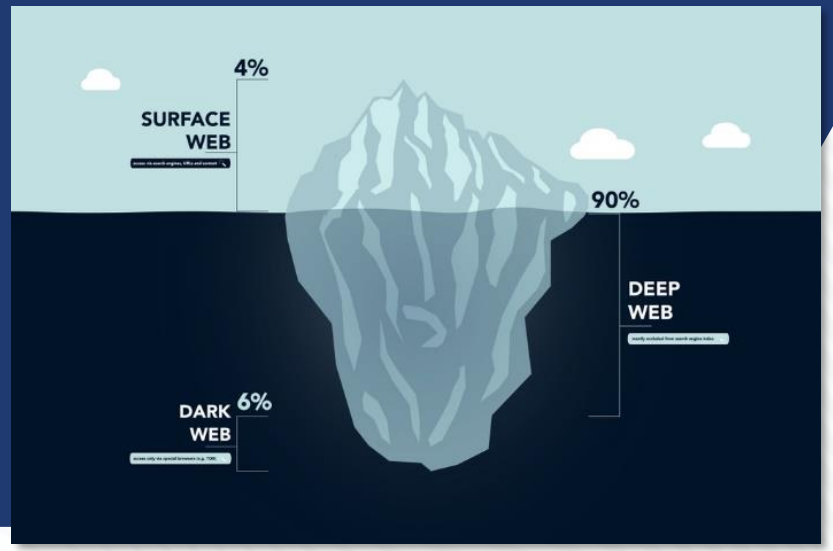
Sensibilizzare e formare continuamente dipendenti e collaboratori su come riconoscere ed evitare le minacce *cyber*

Predisporre e testare procedure di risposta agli incidenti *cyber*:

- **cosa fare in caso di sistemi bloccati?**
- **come garantire la continuità operativa minima?**
- **chi guida la gestione della crisi?**
- **cosa comunicare ai partner, al pubblico e alle Autorità?**

Promuovere una mentalità in cui il *cyber* è parte del quotidiano e richiede comportamenti consapevoli, attenti e prudenti

CYBER INTELLIGENCE



In *cybersecurity*, molta partita si gioca nella capacità di prevedere e anticipare le minacce

Tutte le organizzazioni, anche le più piccole, possono beneficiare di informazioni aggiornate su

- **presenza di propri fattori di esposizione (credenziali rubate, sistemi esposti su Internet, informazioni riservate circolanti, …)**
- **indicatori sugli attacchi più frequenti ed emergenti**

- ✓ **Risorse informative pubbliche, anche gratuite**
- ✓ **Servizi specializzati di *Cyber Threat Intelligence***
- ✓ **Circolarità informativa proattiva con**
  - **enti specializzati, pubblici e privati**
  - **esperti di settore**
  - **altre aziende**
  - ***partner* chiave nella propria filiera**
  - **associazioni di categoria/ambito**
  - **Autorità competenti**

Grazie

Bedankt

Ευχαριστούμε

Спасибо

Teşekkürler

Gracias

Thank you

Merci

Danke

The Italian Food Company. Since 1877.

www.barillagroup.com

@BarillaGroup @barillapeople @BarillaGroup