Protect your business and people with

# LIBRACYBER

## La piattaforma human-centric più affidabile in Europa per prevenire, rilevare e proteggere dal rischio cyber.

**Vittorio Bitteleri** – Country Manager Italia

www.libracyber.com

Made in Europe

# LibraCyber

**> 150**
Dipendenti

**> 3.500**
Clienti attivi

**> 13 Milioni**
Simulazioni effettuate

**> 500**
Partner

**> 0.7 Miliardi**
Messaggi analizzati al mese

**> 1.5 Milioni**
Utenti attivi

**> 300**
MSSP

**> 140.000**
Domini clienti gestiti

**> 6.5 Milioni**
Lezioni fruite

## **CLIENTS** of any size and vertical

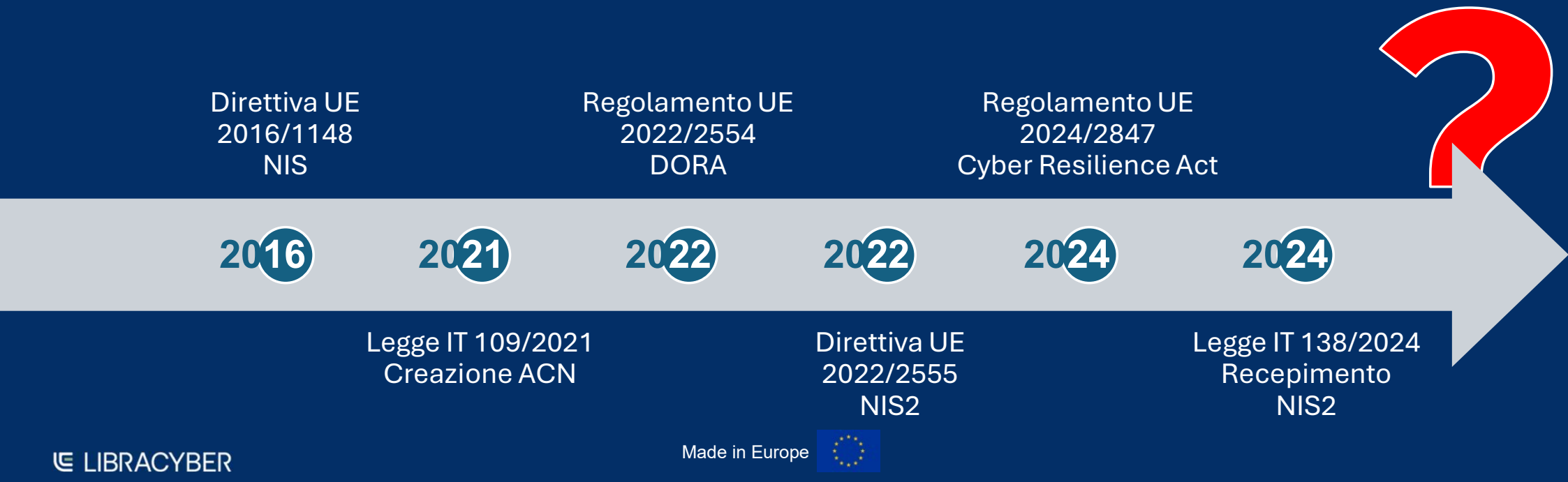
Manufacturing – Luxury & Fashion – Public Administration – Education – Power & Energy – Healthcare – IT Services – Banking & Insurance – Retail – Telco & Media – Transportation & Logistics – Food & Beverage – Charity & Non-Profit – Pharma

LIBRACYBER

Made in Europe

# Un percorso normativo sempre più articolato e stringente.

## In quale direzione stiamo andando?




LIBRACYBER

Made in Europe

# Un percorso normativo sempre più articolato e stringente.
## In quale direzione stiamo andando?

La cyber security non è più solamente una questione interna all'organizzazione

Le norme assegnano agli organi di gestione aziendale la responsabilità diretta del governo della cyber security

Il mancato rispetto delle norme può comportare sanzioni economiche e penali rilevanti per l'organizzazione e per il manager

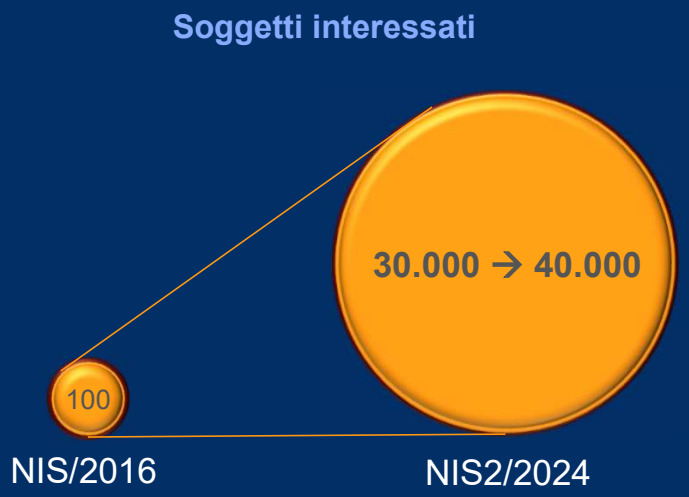
# NIS2 (Network and Information Security Directive 2)

## In sintesi

La direttiva NIS2 introduce nuove regole e obblighi di conformità che devono essere seguiti da tutte le organizzazioni interessate:

- La direttiva si applica a soggetti **ESSENZIALI** e **IMPORTANTI** di medie e grandi imprese, compresa la **Supply Chain**, anche con le **PMI**
- Estende notevolmente i **settori merceologici** interessati
- Assegna agli organi di gestione aziendale la **responsabilità** del governo della cyber security
- **Sanzioni economiche e penali** rilevanti (2% - 1,4%)

Fatturato da 10M€ * 1,4% = 140.000 €



# NIS2

## Settori Essenziali e Importanti

★ Già incluse nel perimetro NIS


LIBRACYBER

Made in Europe

# NIS2

## La rivoluzione nella governance

La Direttiva NIS2 assegna agli organi di gestione aziendale la responsabilità del governo della cybersecurity.

La normativa prevede che gli organi di gestione aziendale possano essere ritenuti responsabili in caso di violazioni, sottolineando così l'importanza del loro ruolo nella prevenzione e gestione dei rischi.

Gli organi di gestione sono, ora, chiamati a

- **Approvazione** delle misure per la gestione del rischio cyber.
- **Supervisione** dell'implementazione di tali misure.
- **Partecipazione** a formazione specifica su temi cyber anche allo scopo di poter valutare l'efficacia e l'adeguatezza delle misure di sicurezza adottate.
- **Promozione** di un'offerta periodica di formazione cyber per i dipendenti.
- **Essere informati** su base periodica o, se opportuno, tempestivamente, degli incidenti e delle relative notifiche.

La filosofia su cui si basa la Direttiva NIS2, quindi, afferma che la cybersecurity è una questione che riguarda l'intera organizzazione e non solo le funzioni tecnologiche.

# NIS2

## Riferimenti normativi (DL 138/2024, recepimento Direttiva UE 2022/2555)

Art. **23** – Organi di amministrazione e direttivi

[…]

2. Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti:
   a) sono **tenuti a seguire una formazione** in materia di sicurezza informatica;
   b) promuovono **l'offerta periodica di una formazione** coerente a quella di cui alla lettera a) ai loro dipendenti, per favorire l'acquisizione di conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi per la sicurezza informatica e il loro impatto sulle attività del soggetto e sui servizi offerti.

   […]

Art. **24** - Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica

[…]

2. Le misure di cui al comma 1 sono basate su un approccio multi-rischio, volto a proteggere i sistemi informativi e di rete nonché il loro ambiente fisico da incidenti, e **comprendono almeno** i seguenti elementi:

   […]

   g) pratiche di igiene di base e di **formazione in materia di sicurezza informatica**;

   […]

# Chi deve fare formazione cyber per la NIS2

**La formazione in cyber security richiesta dalla NIS2 rappresenta un tassello fondamentale per la sicurezza delle organizzazioni e coinvolge:**

## ORGANI DIRETTIVI

### BOARD TRAINING NIS2

La formazione, pensata per amministratori e dirigenti aziendali, rappresenta uno strumento essenziale per sviluppare la piena consapevolezza delle responsabilità specifiche previste dalla Direttiva NIS2 e per affrontare con competenza le sfide della sicurezza digitale.

## DIPENDENTI E COLLABORATORI

### SECURITY AWARENESS TRAINING

La piattaforma, con i suoi tre programmi formativi, è in grado di incidere concretamente ed efficacemente sul comportamento degli utenti e sviluppare in loro le tre principali caratteristiche difensive: la conoscenza, la percezione del pericolo, la prontezza.

# Board Training NIS2

## La risposta agli obblighi formativi

Il percorso formativo sulla Direttiva UE NIS2 è progettato per sviluppare le competenze manageriali essenziali alla gestione del rischio cyber, fornendo strumenti pratici per essere in grado di:

Leggere il contesto strategico generale della cyber security;

- Analizzare l’evoluzione degli scenari nazionali e internazionali;
- Comprendere i rischi di cyber security della propria organizzazione;
- Valutare e approvare strategie, piani, policy e procedure volti alla loro mitigazione;
- Valutare le azioni di mitigazione (procedurali, organizzative e tecniche) più opportune.


LIBRACYBER

Made in Europe


LIBRACYBER
Q&A
Grazie!
www.libracyber.com
Made in Europe