CENTRE FOR
CYBERSECURITY
BELGIUM

Will the NIS2 make us more secure

Made in Belgium

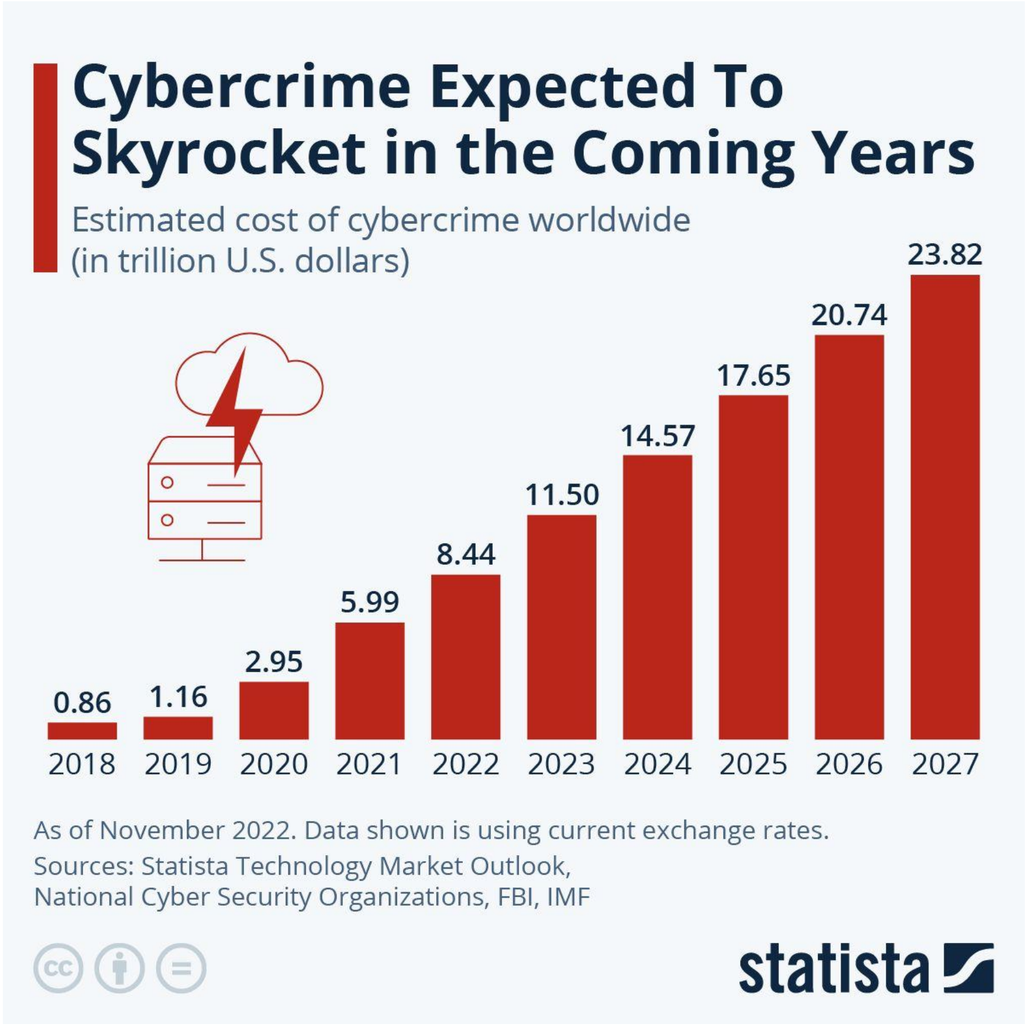
Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

CENTRE FOR CYBERSECURITY BELGIUM

Why a Cybersecurity Law?

Most important Cyber threats

- **RANSOMWARE**
  - 57.8% increase year over year
- **ONLINE FRAUD**
  - Doubled last year
- **DDOS**
  - On average 10/month in BE
- **ESPIONAGE**
- **NEW TECHNOLGIES**
  - Artificial Intelligence



Why this increasing threat?

CENTRE FOR CYBERSECURITY BELGIUM

- **Poor government governance**
  - As many models as countries in the EU
- **Open and free anonymous internet**
  - No public space in cyber space & no security by design
- **Basic security measures not installed**
  - “Security is a burden, a cost”
  - 80% of incidents could have been prevented with 2FA

CENTRE FOR CYBERSECURITY BELGIUM

BE-NIS2:

A new way of thinking …

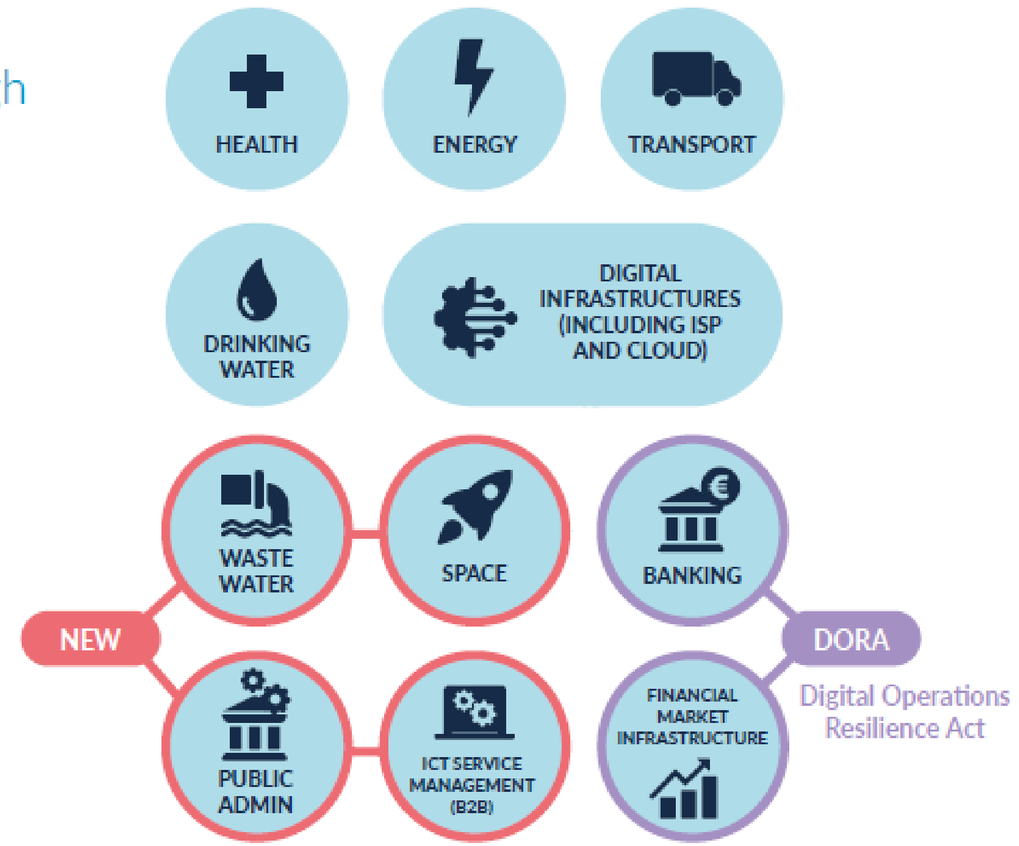
New opportunities

- Common framework for all sectors
  - *Common sense & minimal baseline*
- Early Warning system integration
- Fast Vulnerability Scan
- Supply chain
- Gov support
  - *Gov reporting & support (situational awareness)*

Sectors in scope

CENTRE FOR CYBERSECURITY BELGIUM

Annex 1 - Sectors of High Criticality



Essential or **Important** Entities

Annex 2 - Other Critical Sectors

Important Entities

Entities in scope

CENTRE FOR CYBERSECURITY BELGIUM

Annex I: Sectors of high criticality
Entity type + size-cap*

Large size
(at least 250 FTE or > €50M annual turnover/€43M balance sheet)

Medium size
(at least 50 FTE or > €10M annual turnover/balance sheet)

CERTIFICATION

Essential entities

Important entities

Annex II: Others critical sectors
Entity type + size-cap

Large size
(at least 250 FTE or > €50M annual turnover/€43M balance sheet)

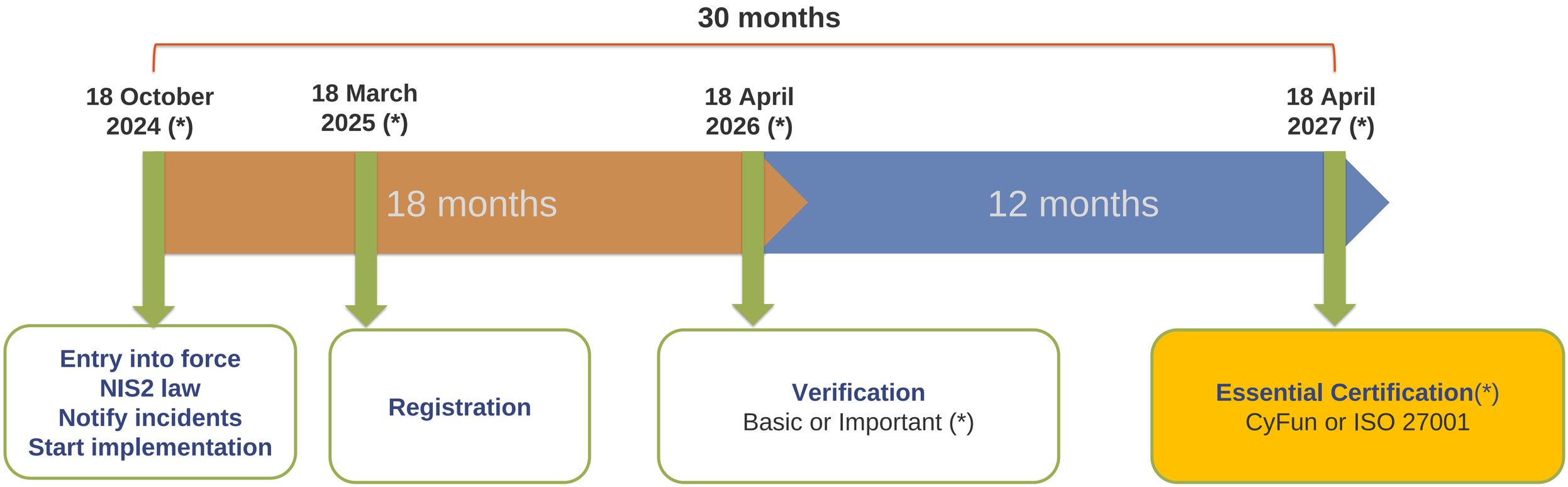
Medium size
(at least 50 FTE or > €10M annual turnover/balance sheet)

Important entities

Important entities

(*) There are some exceptions where the size-cap doesn't apply

Specific timeline for regular conformity assessment



*(in case of formal identification, the timing starts from the notification of the administrative decision)

CENTRE FOR CYBERSECURITY BELGIUM

NIS2 The Belgian Way

Unity makes strength

NIS2 made in Belgium

CENTRE FOR CYBERSECURITY BELGIUM

- NIS 2 Quickstart Guide – implementing NIS2 in 7 steps
  1. Am I affected by NIS2?
  2. Register your NIS2 entity ASAP
  3. Report significant incidents
  4. **Determine your CyberFundamentals (CyFun®) level**
  5. Plan cybersecurity training
  6. Implement the security measures
  7. Have your security reviewed

https://atwork.safeonweb.be/tools-resources/nis-2-quickstart-guide

CCB Standard Risk Assessment

CENTRE FOR CYBERSECURITY BELGIUM

Default Risk Assessment per Sector & Size ➔ appropriate Cyber Fundamentals Level

Energy			Common skills		Common skills		Common skills		Extended Skills		Extended Skills	
Organization Size (L/M/S = 3/2/1)	3	Threat Actor Type	Competitors		Ideologues Hactivists		Terrorist		Cyber Criminals		Nation State actor	
Cyber Attack Category	Global or Targetted	Impact	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score
Sabotage/ Disruption (DDOS,…)	2	High	Low	0	Low	0	Med	30	Med	30	High	60
Information Theft (espionage, …)	2	High	Low	0	Low	0	Low	0	High	60	High	60
Crime (Ransom attacks)	1	High	Low	0	Low	0	Low	0	High	30	Low	0
Hactivism (Subversion, defacement…)	1	Med	Low	0	Med	7,5	Low	0	Low	0	Med	7,5
Disinformation (political influencing)	1	Low	Low	0	Med	0	Low	0	Low	0	Low	0
	Total	Total		0		7,5		30		120		127,5

Score	CyFun Level
285	**ESSENTIAL**

Cyber Fundamentals Framework

Approval

Accreditation

Certificate or Label

Conformity Assessment Body

Advantages

- Low-cost Risk Assessment and Security Plan
- One system to maintain for all sectors and entities
- Supply chain cyber security level can be easily and uniformly assessed (Ripple-through)
- Effective and efficient supervision (CAB)
- There is a recognized method for executive & board member responsibilities
- Cross-sector education, training and exercises
- International recognition ➔ cross-border (partially but growing)

CENTRE FOR CYBERSECURITY BELGIUM

Wrap-up

YES, NIS2 will make a difference !

- 2500 Important & Essential Entities will improve their Security Level
- CCB services will reduce national vulnerability
- More incident reporting & effective response
- Change in mentality :

Cybersecurity as a routine

Based on a common

Cyber Fundamentals Framework

One thing to remember

Two/Multi-factor authentication

On ALL

External connections

CENTRE FOR CYBERSECURITY BELGIUM

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Rue de la Loi / Wetstraat 18 - 1000 Brussels

www.ccb.belgium.be

nis@ccb.belgium.be