CYBER SECURITY

A C-LEVEL & BOARD TOPIC

JAN DE BLAUWE

MAY 25TH, 2021

BNP PARIBAS FORTIS

The bank for a changing world

AGENDA

Questions to be asked by the Board:

Question 1
Why is cyber security a point of concern?

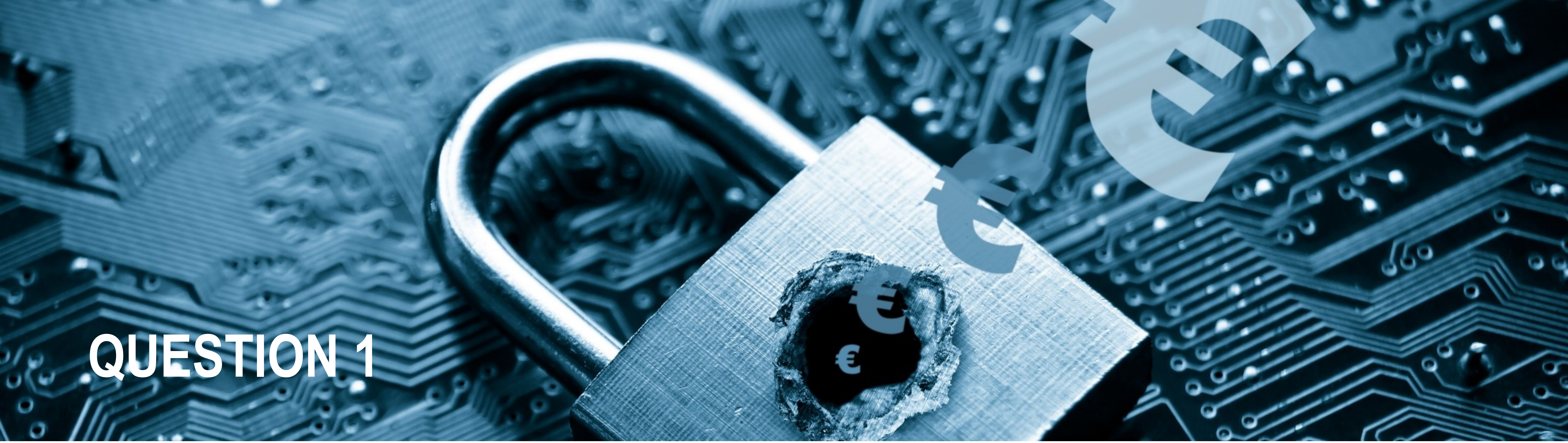
Question 2
Why is it so difficult to solve?

Question 3
How are we organized?

Question 4
Where do we stand?

Question 5
What’s next?

Conclusions



QUESTION 1

WHY IS CYBER SECURITY A POINT OF CONCERN?

WORLD ECONOMIC FORUM RAISING ‘CYBER’

As one of the Top 5 risks

Top 5 Global Risks in Terms of Likelihood

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
1st	Asset price collapse	Asset price collapse	Storms and cyclones	Severe income disparity	Severe income disparity	Income disparity	Interstate conflict with regional consequences	Large-scale involuntary migration	Extreme weather events	Extreme weather events	Extreme weather events
2nd	Slowing Chinese economy (<6%)	Slowing Chinese economy (<6%)	Flooding	Chronic fiscal imbalances	Chronic fiscal imbalances	Extreme weather events	Extreme weather events	Extreme weather events	Large-scale involuntary migration	Natural disasters	Failure of climate-change mitigation and adaptation
3rd	Chronic disease	Chronic disease	Corruption	Rising greenhouse gas emissions	Rising greenhouse gas emissions	Unemployment and underemployment	Failure of national governance	Failure of climate-change mitigation and adaptation	Major natural disasters	**Cyber-attacks**	Natural disasters
4th	Global governance gaps	Fiscal crises	Biodiversity loss	**Cyber-attacks**	Water supply crises	Climate change	State collapse or crisis	Interstate conflict with regional consequences	Large-scale terrorist attacks	**Data fraud or theft**	**Data fraud or theft**
5th	Retrenchment from globalization	Global governance gaps	Climate change	Water supply crises	Mismanagement of population	**Cyber-attacks**	High structural unemployment or underemployment	Major natural catastrophes	**Massive incident of data fraud/theft**	Failure of climate-change mitigation and adaptation	**Cyber-attacks**

World Economic Forum, “The Global Risks Report 2019” 14th Edition

Concerns about data fraud and cyber-attacks were prominent again:

- Massive data breaches in 2018
- New hardware weaknesses revealed
- Exploitation of AI to engineer more forceful cyberattacks

WORLD ECONOMIC FORUM RAISING ‘CYBER’

As one of the Top 5 risks

Top 5 Global Risks in Terms of Likelihood

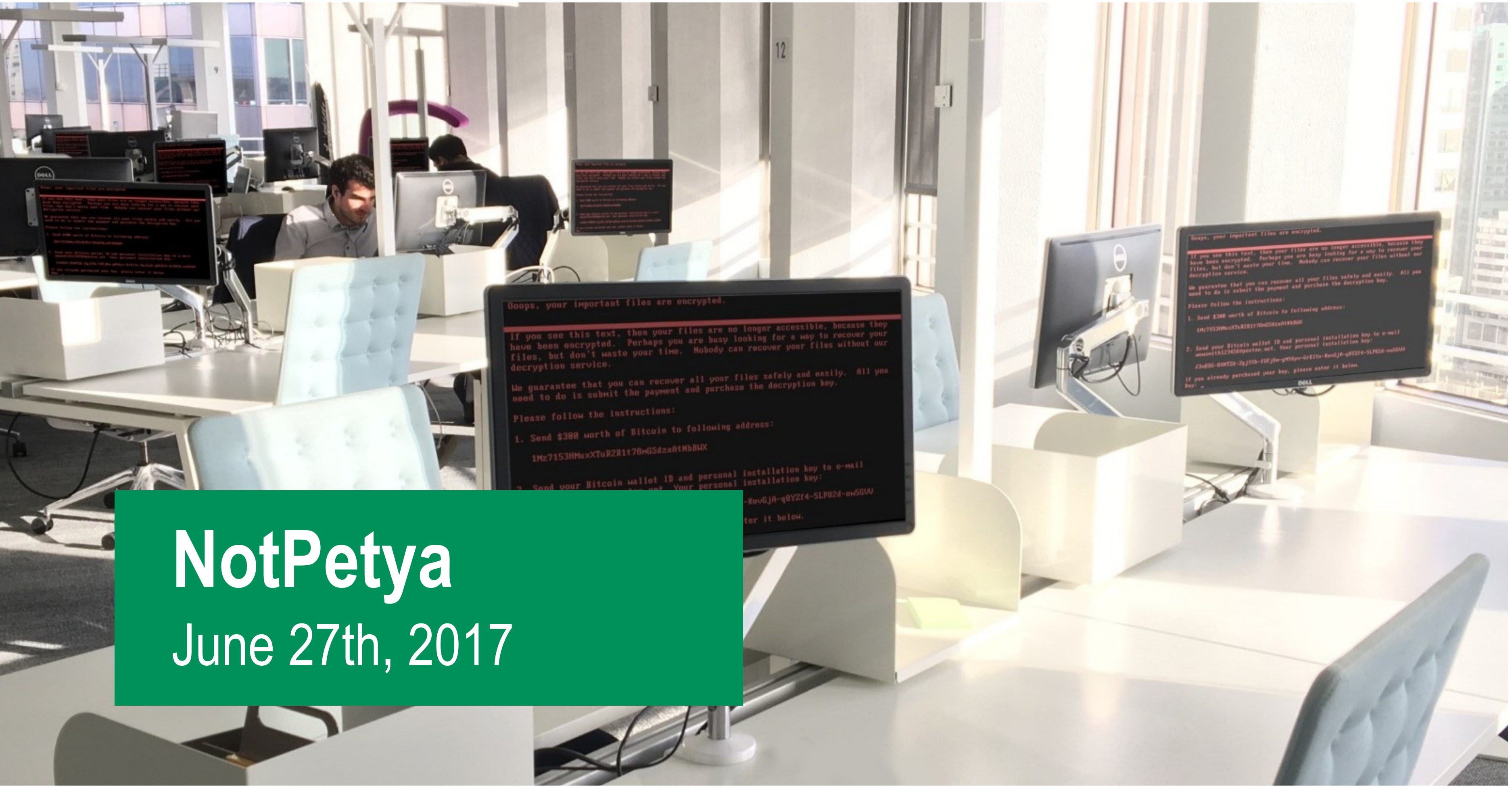
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
1st	Asset price collapse	Asset price collapse	Storms and cyclones	Severe income disparity	Severe income disparity	Income disparity	Interstate conflict with regional consequences	Large-scale involuntary migration	Extreme weather events	Extreme weather events	Extreme weather events
2nd	Slowing Chinese economy (<6%)	Slowing Chinese economy (<6%)	Flooding	Chronic fiscal imbalances	Chronic fiscal imbalances	Extreme weather events	Extreme weather events	Extreme weather events	Large-scale involuntary migration	Natural disasters	Failure of climate-change mitigation and adaptation
3rd	Chronic disease	Chronic disease	Corruption	Rising greenhouse gas emissions	Rising greenhouse gas emissions	Unemployment and underemployment	Failure of national governance	Failure of climate-change mitigation and adaptation	Major natural disasters	**Cyber-attacks**	Natural disasters
4th	Global governance gaps	Fiscal crises	Biodiversity loss	**Cyber-attacks**	Water supply crises	Climate change	State collapse or crisis	Interstate conflict with regional consequences	Large-scale terrorist attacks	**Data fraud or theft**	**Data fraud or theft**
5th	Retrenchment from globalization	Global governance gaps	Climate change	Water supply crises	Mismanagement of population	**Cyber-attacks**	High structural unemployment or underemployment	Major natural catastrophes	**Massive incident of data fraud/theft**	Failure of climate-change mitigation and adaptation	**Cyber-attacks**

World Economic Forum, “The Global Risks Report 2019” 14th Edition

Concerns about data fraud and cyber-attacks were prominent again:

- Massive data breaches in 2018
- New hardware weaknesses revealed
- Exploitation of AI to engineer more forceful cyberattacks

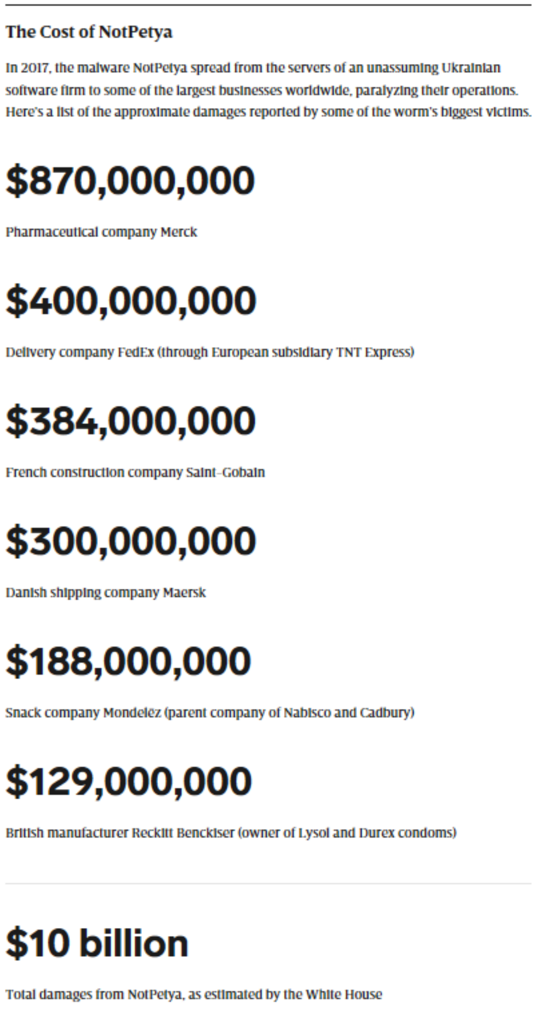
FEARS OF SYSTEMIC RISKS



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail
                                    Your personal installation key:
                                 -KevGjA-q8YZf4-5LP82d-ew5GVV
                               ter it below.
```

NotPetya

June 27th, 2017



The Cost of NotPetya

In 2017, the malware NotPetya spread from the servers of an unassuming Ukrainian software firm to some of the largest businesses worldwide, paralyzing their operations. Here's a list of the approximate damages reported by some of the worm's biggest victims.

$870,000,000	Pharmaceutical company Merck
$400,000,000	Delivery company FedEx (through European subsidiary TNT Express)
$384,000,000	French construction company Saint-Gobain
$300,000,000	Danish shipping company Maersk
$188,000,000	Snack company Mondelēz (parent company of Nabisco and Cadbury)
$129,000,000	British manufacturer Reckitt Benckiser (owner of Lysol and Durex condoms)
$10 billion	Total damages from NotPetya, as estimated by the White House

INCREASED REGULATORY ATTENTION …

… and fines

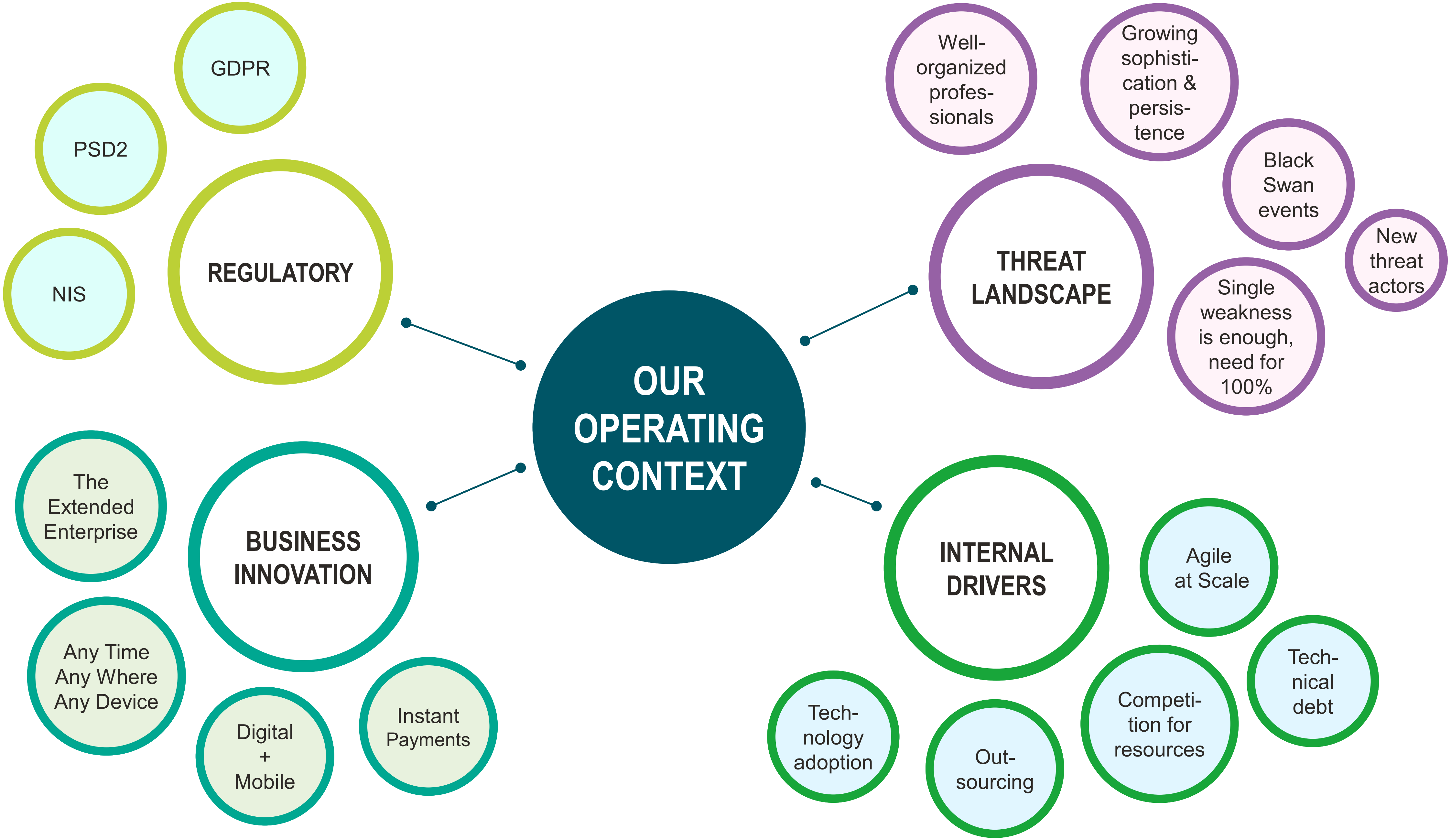
> ” British Airways’s fine
> of 230 Mn US Dollar fine
> (500€ per record) over GDPR
> breach as they ‘simply’ used
> bad javascripts

QUESTION 2

WHY IS IT SO DIFFICULT TO SOLVE?

“We regularly read / hear about incidents in the press”

“We are worried that we are investing in an endless pit”



OUR OPERATING CONTEXT

REGULATORY
- GDPR
- PSD2
- NIS

THREAT LANDSCAPE
- Well-organized professionals
- Growing sophistication & persistence
- Black Swan events
- New threat actors
- Single weakness is enough, need for 100%

BUSINESS INNOVATION
- The Extended Enterprise
- Any Time Any Where Any Device
- Digital + Mobile
- Instant Payments

INTERNAL DRIVERS
- Agile at Scale
- Technical debt
- Competition for resources
- Outsourcing
- Technology adoption

QUESTION 3

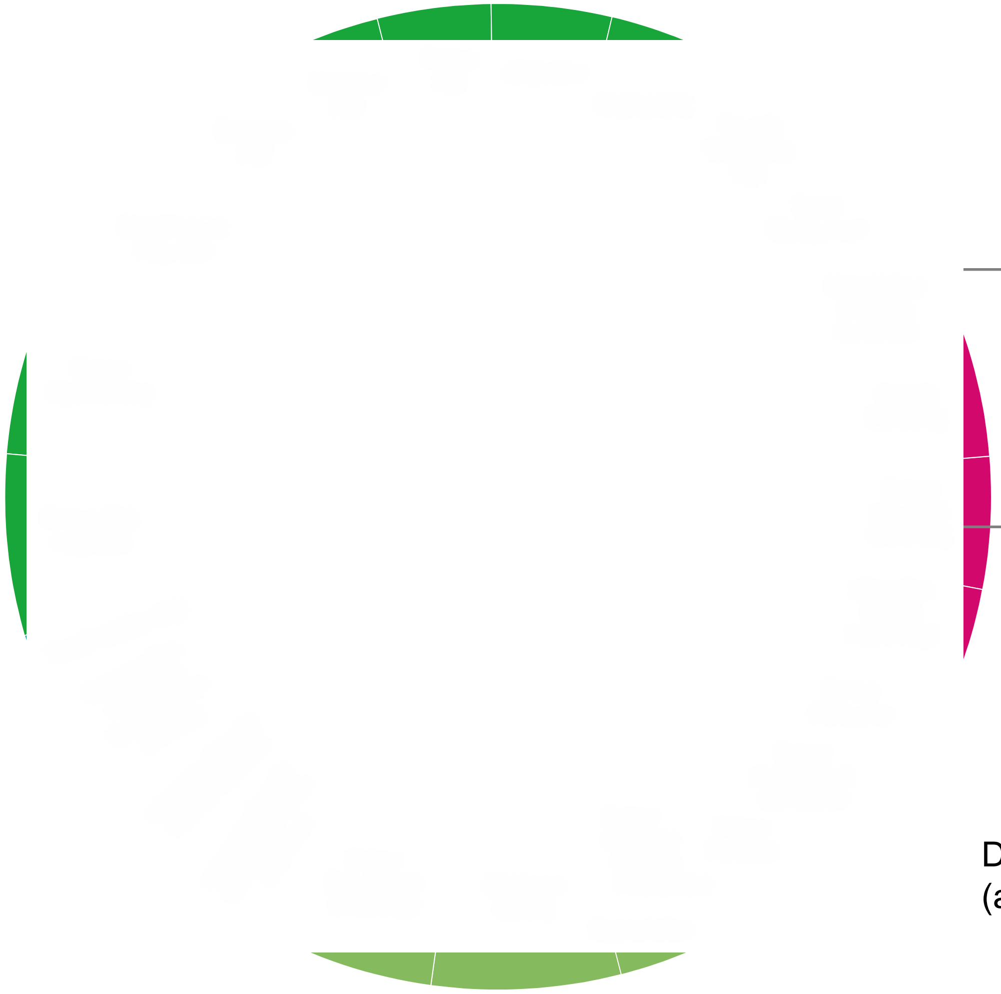
HOW ARE WE ORGANIZED?

“As board member, I need to get assurance that this topic is managed in an adequate and structured manner.”

“I need to understand the organization, processes, and decision making structures that are in place.”

1ST LINE OF DEFENCE

INFORMATION SECURITY MANAGEMENT SYSTEM



Dedicated cyber governance, risk and compliance monitoring

Structural embedment of security in a number of key ‘change processes’

Day-to-day security services (aka. ‘capability set’)

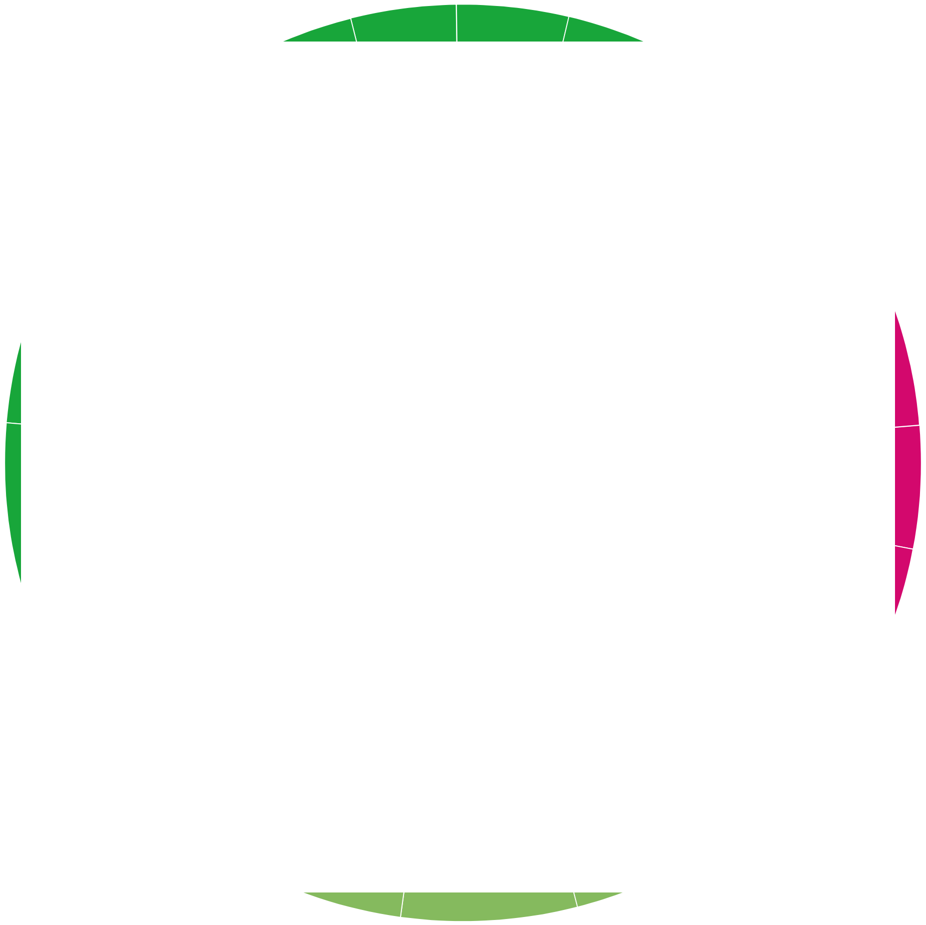
Project & Architecture Governance:
Projects are systematically supported by an information security architect i.o. to assess the presence of security weaknesses and to adapt the design to avoid them.

New Activity Committee (NAC):
All major changes and new activities are subject to a risk review (incl. cyber) governed by the New Activity Committee (NAC).

Procurement:
Third parties are subject to pre-contractual security checks (including a Data Privacy Impact Assessment); and subject to contractual clauses re. to security, privacy, business continuity, and the right to audit.

Ad hoc risk assessments:
Performed either on demand of an internal client, or at the initiative of the security function.

INFORMATION SECURITY MANAGEMENT SYSTEM



TOP RISKS

→

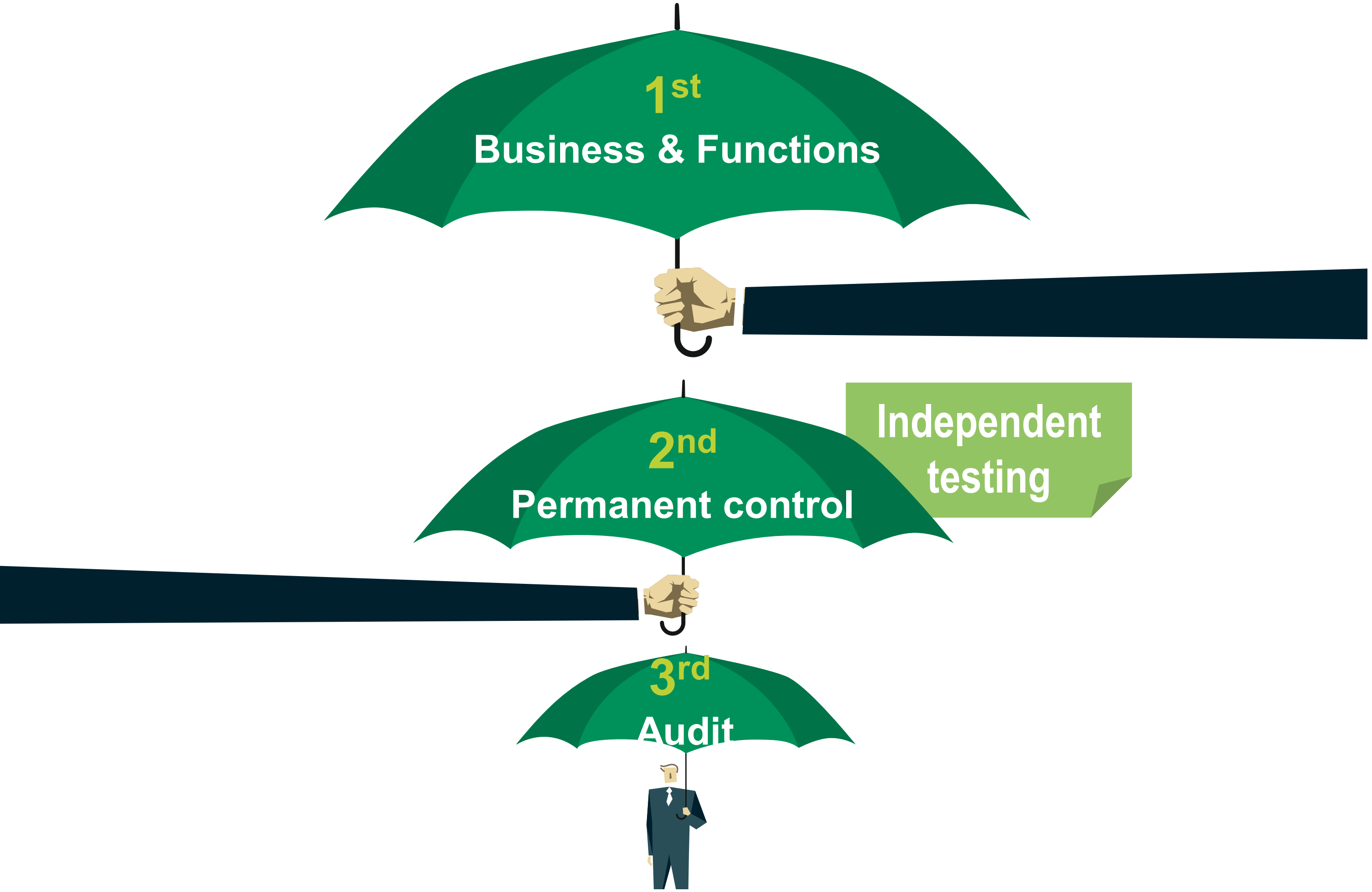
INCIDENTS

CYBER MATURITY PROGRAM

Note: maturity data is for illustrative purposes only, not indicative of actuals

3 LINES OF DEFENCE

3 LINES OF DEFENSE



DEFENSE IN DEPTH, ALSO APPLIED AT ORGANISATIONAL LEVEL

FIRST LINE IS COMPLEMENTED BY:

- Permanent Control (= 2nd line of defence)
  Provides additional assurance, e.g. by performing independent testing (for ex. red-teaming tests, review of cyber capabilities, …). And intervenes in New Activity validation process with a risk opinion.
- Audit (= 3rd line of defence)
  Performs punctual missions to check the resilience and adequacy of our systems and processes against the risk of cyber threats.
- ExCo and Board
  Act as a ‘4th line of defence’; in particular by having a good mastery of the topic, conveying its importance (‘Tone at the Top’), and ensuring that sufficient means are dedicated to the topic

QUESTION 4

WHERE DO WE STAND?

“As board member, I need to understand the major risks we face, the incidents we suffered, and the actions we take to address them.”

“I need to understand whether the budgets are in place to implement those actions.”

RISK BASED APPROACH

DATA LEAKAGE

Data leakage is the unauthorized transmission of data from within an organization to an external destination or recipient. The term can be used to describe data that is transferred electronically or physically (web, email, etc.)

EXTERNAL INSTRUSION & SPYING

External attack coming from outside the organization network and leading to compromise a computer system by breaking the security of such a system or causing it to enter into an insecure state

CYBER FRAUD

Cyber fraud refers to any type of deliberate deception for unfair or unlawful gain that occurs online.

SABOTAGE

Unavailability is the situation when an item does not operate correctly at a given time and under specified conditions. A total unavailability will prevent some or all of the users from receiving business services.

MANAGE OPEN WORLD

A set of evolving topics due to new threats resulting from the opening of the traditional IT scope. This includes: Cloud, Mobile, Big Data,…

Key Challenges

Business
Threats
Budget
Resourc es

Pursue digital transformation whilst ensuring cybersecurity is not left behind (opportunity cost vs cost of incidents)

Further build/advance existing capabilities **in a challenging cost environment**

Stay ahead of (perpetual) adversaries
The intensity of cyber threats continues to grow.

Resource crunch
Demand for cyber skills far outstrips supply

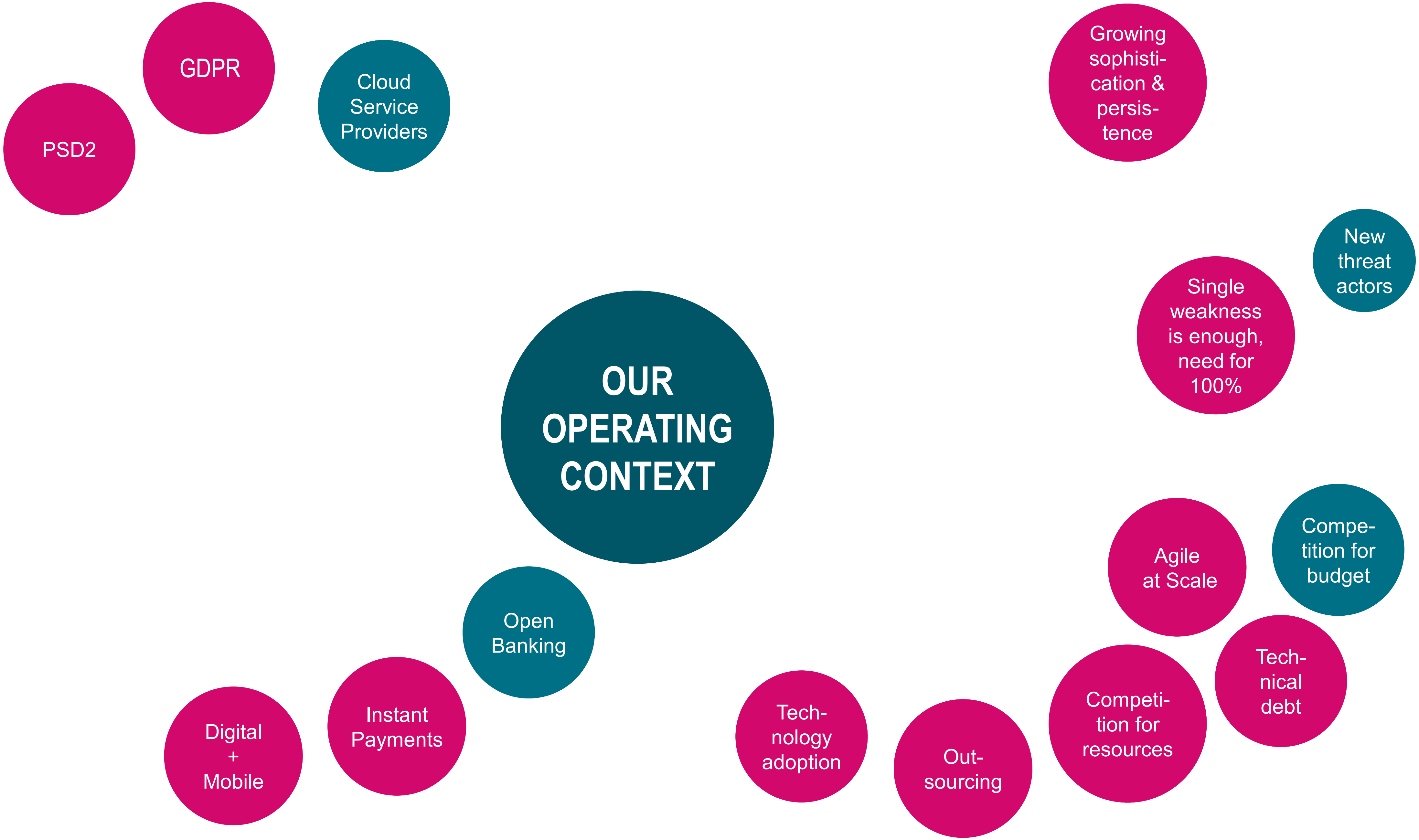
QUESTION 5

WHAT’S NEXT?

“As board member, I need to understand whether we are prepared for the future”

“… whether structures, actions, means, etc are in place such that our exposure to cyber risks will improve (or stay at the same level)”

RAINY OUTLOOK



OUR OPERATING CONTEXT

GDPR

PSD2

Cloud Service Providers

Growing sophistication & persistence

New threat actors

Single weakness is enough, need for 100%

Agile at Scale

Competition for budget

Technical debt

Competition for resources

Outsourcing

Technology adoption

Open Banking

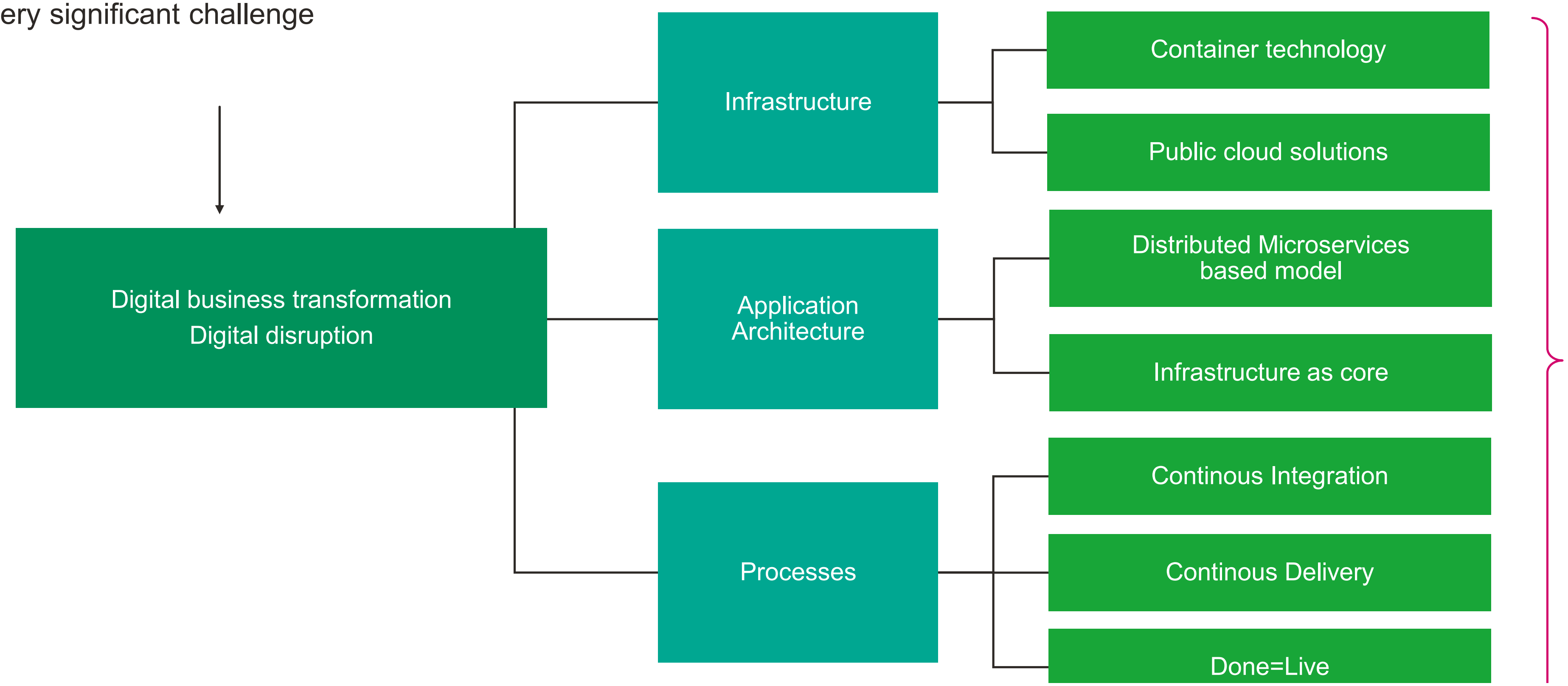
Instant Payments

Digital + Mobile

EXAMPLE: # SECDEVOPS

Drivers: reduce time-to-market, keep costs under control and deliver new capabilities and features in an **agile way** to customers.

These imperatives, **combined with major and broad-ranging technology innovation** not seen before, represent
a very significant challenge



Digital business transformation
Digital disruption

Infrastructure

Container technology

Public cloud solutions

Application Architecture

Distributed Microservices based model

Infrastructure as core

Processes

Continous Integration

Continous Delivery

Done=Live

INNOVATION IN ALL 3 AREAS AT THE SAME TIME

YOUR ROLE AS A BOARD MEMBER

As a Board member, you ...

1 Embody that cybersecurity is an **enterprise-wide** risk issue

2 nderstand the **legal nplications** of cyber risks

3 Request and obtain access to **cybersecurity expertise**

4 Ensure that management establishes an enterprise-wide risk management **framework with adequate staffing and budget**

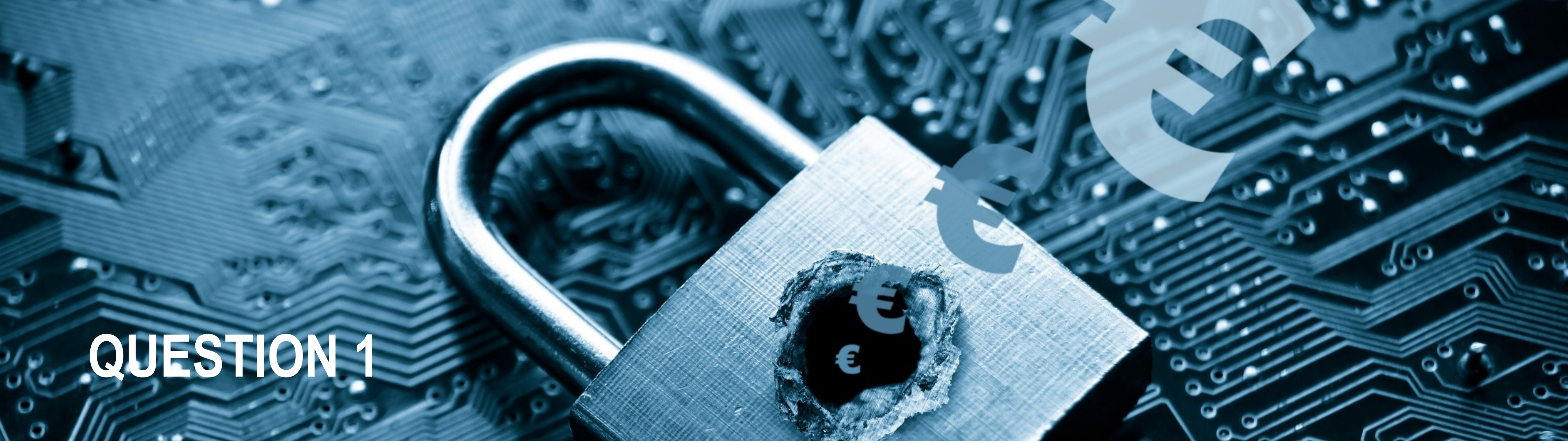
5 Challenge senior management on which **risks to avoid, accept, mitigate or transfer**

6 Insist on the timely **nplementation of the cyber ecurity strategy**

7 ead by **example**

Guiding principles *based on the National Association of Corporate Directors in corporation with the American International Group*

CONCLUSIONS



QUESTION 1

WHY IS CYBER SECURITY A POINT OF CONCERN?

The intensity of cyber threats continues to grow. Expected losses are estimated to increase, driven by tail risks.

QUESTION 2

WHY IS IT SO DIFFICULT TO SOLVE?

- “We regularly read / hear about incidents in the press”
- “We are worried that we are investing in an endless pit”

Security is intrinsically a very complex business problem to solve. It involves the whole organization, requires strong top management support, and needs a holistic approach.

QUESTION 3

HOW ARE WE ORGANIZED?

- “As board member, I need to get assurance that this topic is managed in an adequate and structured manner.”
- “I need to understand the organization, processes, and decision making structures that are in place.”

Put a strong expert team in place, with C-level reporting line.

Security is integrated in the change processes of the organization (‘security by design’), and regularly tested.

Define cyber maturity objectives; measure maturity; and make means available to strengthen areas that are not yet at target level.

QUESTION 4

WHERE DO WE STAND?

- "As board member, I need to understand the major risks that we face, the incidents that we suffered, and the actions we take to address them."
- "I need to understand whether the budgets are in place to implement those actions."

Measure progress against stated maturity targets.

Revise the maturity model and capability set at least once per year.

QUESTION 5

WHAT'S NEXT?

"As board member, I need to understand whether we are prepared for the future; whether structures, actions, means, etc are in place such that our exposure to cyber risks will improve (or stay at the same level)"

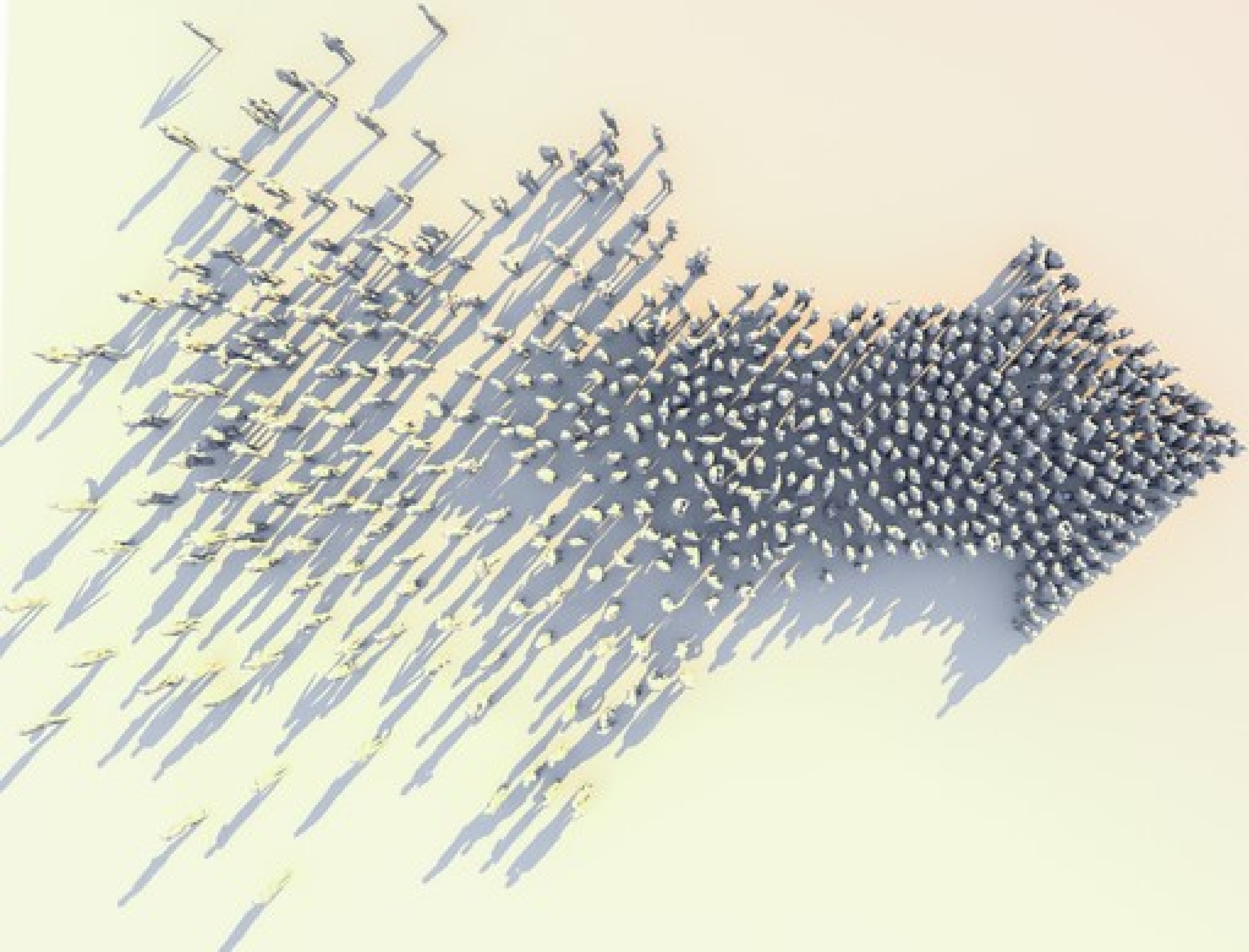
Your risk outlook is probably 'rainy'

- Significant security investments are needed to accompany business transformation (digital customer journeys; Agile; supply chains; etc)
- Talent shortages on the job market compound budget reductions

There is no room for complacency

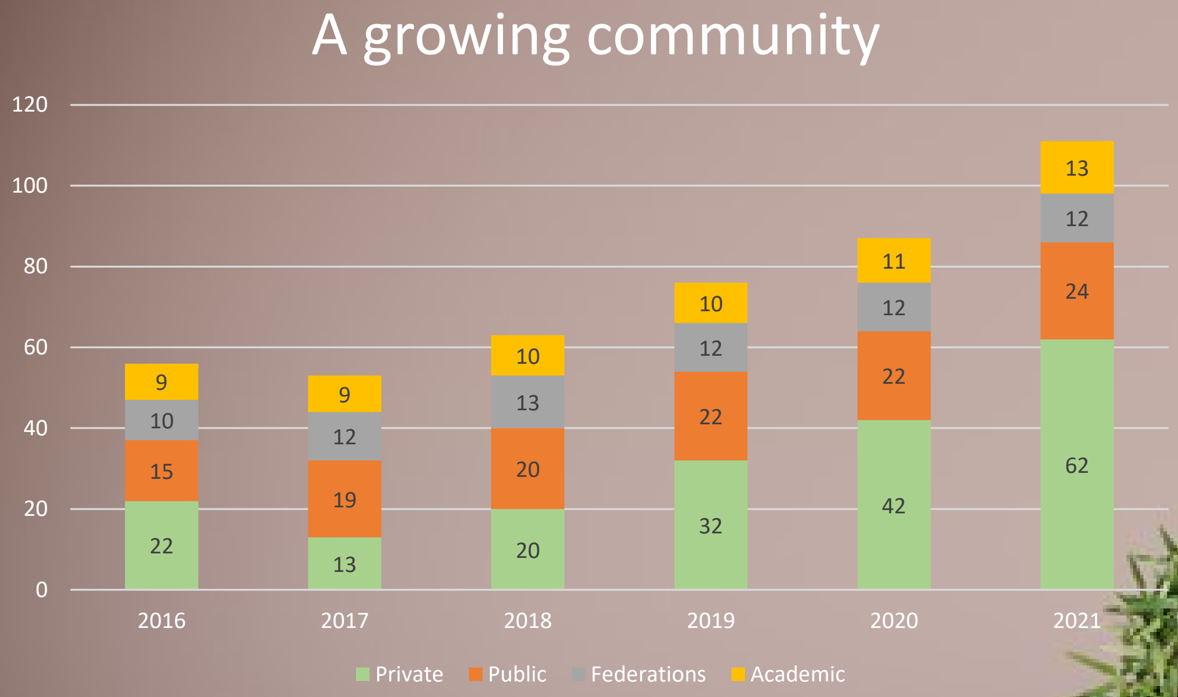
Cyber weaknesses will be exploited; cyber incidents are uncompromising and may be very consequential.

CYBER SECURITY
COALITION.be



Our mission ***is to bolster Belgium's cyber security resilience by building a strong cyber security ecosystem at national level.***

CYBER SECURITY COALITION.be



- 107 member organizations
- from Private, Public and Academic sectors
- 4 associate members
- Community self-governance

Experience sharing

Operational collaboration

Awareness raising

Policy recommendations

bringing together experts & peers

cooperation is key in the fight against cybercrime

CYBER SECURITY COALITION.be

Experience Sharing

- Connect & build the trust network through events
- Shared capability building & mutual aid
- Sharing information & best practices
- Cyber Security Awareness & Culture Manager training

CYBER SECURITY COALITION

Operational Collaboration

Peer-to-peer discussions in a trusted platform

- 10 focus groups
- Bringing together experts & peers across sectors
- Focused exchange
- Common actions/ projects

CYBER SECURITY COALITION.be

Focus Groups

- Tap into a ‘virtual team’
- Experts connect with peers
- Reliable references
- Threat intelligence shared by allies
- Sharing of ‘common’ assets

- CSIRT-SOC (2016)
- Awareness (2016)
- Privacy (2017)
- NIS (2017)
- Cloud Security (2018)
- Crypto (2018)
- Enterprise Security Architecture (2019)
- GRC (2019)
- EU Cybersecurity Act (2019)
- OT/ICS Security (2021)

CYBER SECURITY COALITION.be

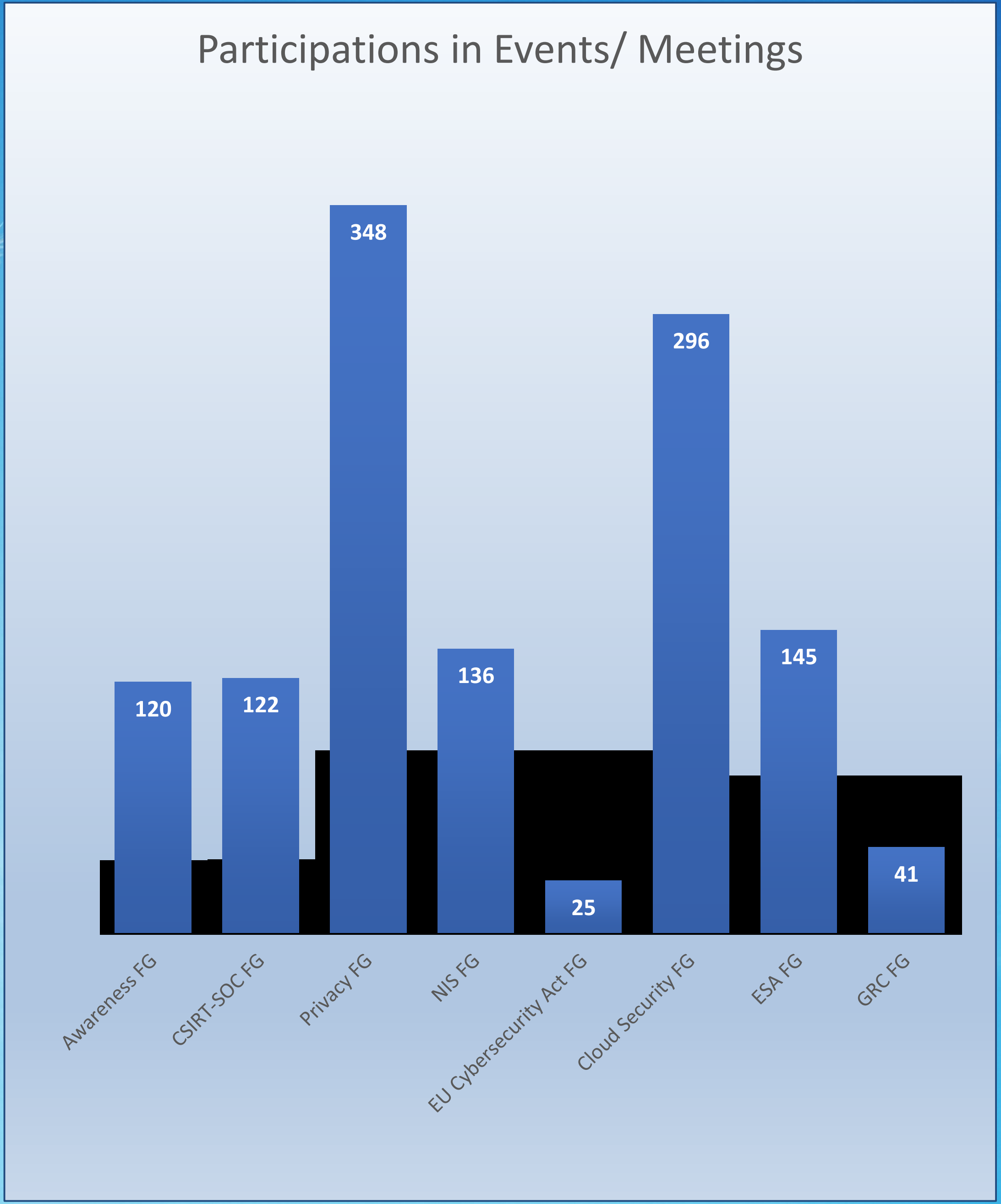
Focus Groups

35 activities

1,233 participations

in events / meetings

(2020)


Participations in Events/ Meetings

Awareness Raising

Passwords are a thing of the past
Protect your online accounts with two-factor-authentication
Kn1ght123

- Strategic partnership with Centre for Cyber Security Belgium (CCB)
- Preparing 7th national awareness campaign (2021)

The impact of a joint awareness campaign is greater than an individual member's efforts

CYBER SECURITY COALITION.be

Classification : Internal

Awareness Raising

Interactive Cyber Security E-Learning via Kahoot

Cyber Security Basics for Starters

Cyber Security KIT

SME Security Scan

- Focus on weakest link in the chain: **SME segment**
- Freely available guidelines/ tools

- Sponsoring cyber security tournaments for students (skills gap in the labour market)

CYBER SECURITY COALITION

Policy Recommendations

- Coalition is a sounding board for public authorities
- Exchange of implementation practices
- Actions to put cyber security higher on the list of priorities at all governmental levels.

Members: Public & Academic Sector

Belnet
dedicated connectivity

CENTRE FOR CYBER SECURITY BELGIUM

CERT.be

Service Public Fédéral FINANCES
Federale Overheidsdienst FINANCIEN
WWW.FIN.BELGIUM.BE

Solvay Brussels School
Economics & Management

ULB

CPVP
Commission de la protection de la vie privée

BOSA

BELV

FCCU

Federale Politie

PXL

KU LEUVEN

UCL
Université catholique de Louvain

ibz

Vlaamse overheid

howest
De Hogeschool West-Vlaanderen
Lid van de Associatie Universiteit Gent

UNIVERSITÉ DE NAMUR

digital wallonia .be

ADIV-SGRS

I B P T

PARLEMENT DE WALLONIE

DEFENCE

GHENT UNIVERSITY

eurometropolitan ecampus

KINGDOM OF BELGIUM
Foreign Affairs,
Foreign Trade and
Development Cooperation

VSSE
veiligheid van de staat
sûreté de l'état

cirb.brussels
you

DPA
Data Protection Authority

THOMAS MORE

ICHEC
BRUSSELS MANAGEMENT SCHOOL

VUB

economie
FOD Economie, K.M.O., Middenstand en Energie

B

MIVB STIB

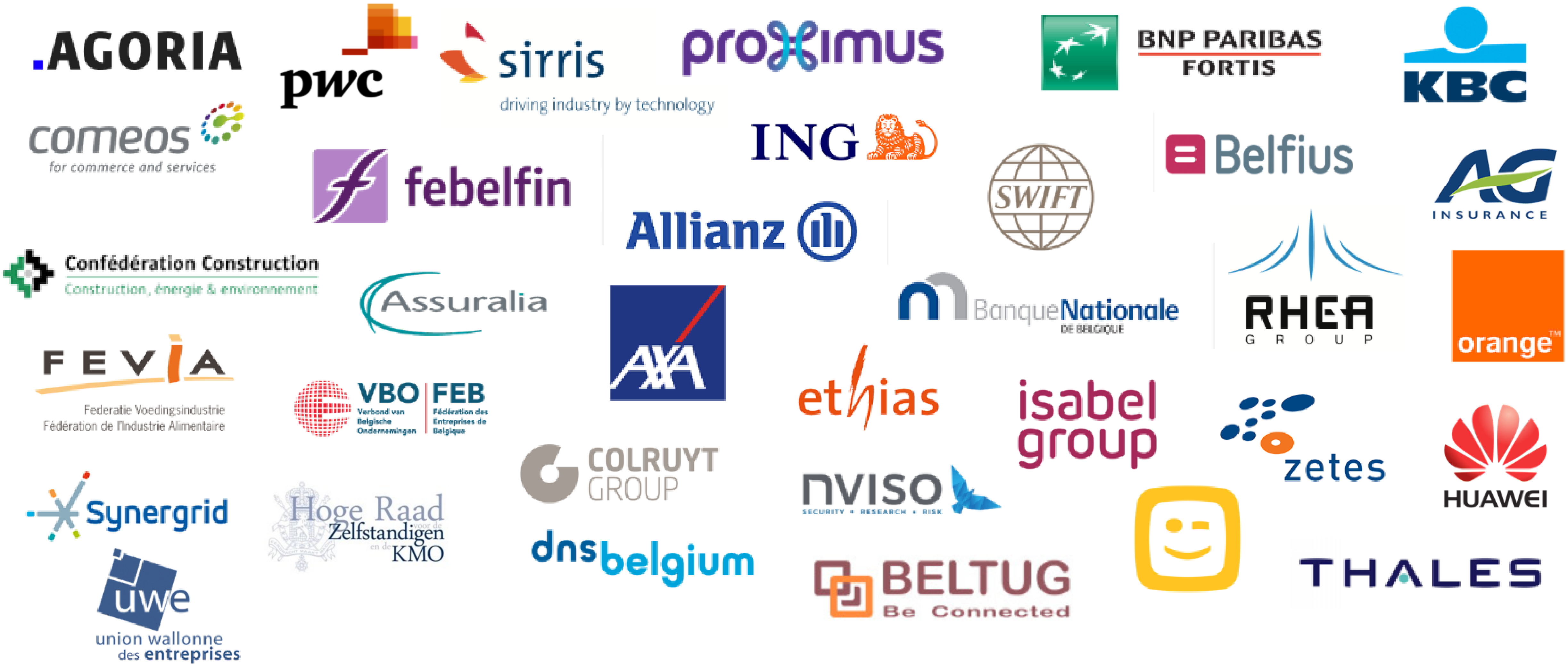
European Commission

CERT-EU

Service public fédéral
Santé publique, Sécurité de la Chaîne alimentaire et Environnement
Federale Overheidsdienst
Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu

vives
hogeschool

Members: Private Sector


.AGORIA
pwc
sirris
driving industry by technology
proximus
BNP PARIBAS
FORTIS
KBC
comeos
for commerce and services
febelfin
ING
SWIFT
Belfius
AG
INSURANCE
Allianz
Confédération Construction
Construction, énergie & environnement
Assuralia
AXA
BanqueNationale
DE BELGIQUE
RHEA
GROUP
orange™
FEVIA
Federatie Voedingsindustrie
Fédération de l'Industrie Alimentaire
VBO
Verbond van Belgische Ondernemingen
FEB
Fédération des Entreprises de Belgique
ethias
isabel group
zetes
HUAWEI
COLRUYT
GROUP
nviso
SECURITY • RESEARCH • RISK
Synergrid
Hoge Raad voor de Zelfstandigen en de KMO
dnsbelgium
BELTUG
Be Connected
THALES
uwe
union wallonne
des entreprises

Members: Private Sector

TOREON
Your coach in digital security

synergics
CLOUD CHANGE AGENT

Secutec

INNOCOM.

EASI

dilaco

BEKAERT
better together

SOCIALware

SENIOR LIVING GROUP
In caring hands

Orange
Cyberdefense

expertware

CHU | UVC BRUGMANN

APPROACH

sopra steria

DKV

Microsoft

EXCELLIUM
Your first call when it comes to cybersecurity and privacy

Hôpital Universitaire des Enfants Reine Fabiola
Universitair Kinderziekenhuis Koningin Fabiola

ALLEN & OVERY

nextAuth
Best in mobile user authentication

LINEAS
YOUR FREIGHT FORCE

INTIGRITI
ETHICAL HACKING PLATFORM

CRANIUM

ARGENTA

vanbreda
RISK & BENEFITS

olv
Top in Zorg.

KPMG

JUNIPer NETWORKS | Engineering Simplicity

GHdC
asbl

euroclear

DIGITRIBE

UNISYS | Securing Your Tomorrow®

SAI
studiecentrum voor automatische informatieverwerking vzw

YZ
Jan Yperman Ziekenhuis

Hôpitaux Iris Sud | HIS
Iris Ziekenhuizen Zuid | IZZ

.eu
Powered by EURid

LSEC
LEADERS IN SECURITY

4 Associate Members

www.cybersecuritycoalition.be

CYBER SECURITY
COALITION.be

Contact:
info@cybersecuritycoalition.be

Q&A