BENELUX

CompTIA®
COMMUNITY

Welcome

CompTIA Community – Benelux Meeting

8 February 2024, Antwerp

Antitrust, Diversity, and Anti-Harassment

- Antitrust
  You must not engage in discussions that could result in an unreasonable restraint of trade.
  https://connect.comptia.org/about-us/antitrust-statement

- Diversity
  We promote an inclusive environment that respects and values all individuals.
  https://connect.comptia.org/about-us/dei-policy

- Anti-Harassment
  This is a respectful and safe environment for all. Any verbal, physical, or psychological harassment will not be tolerated.
  https://www.comptia.org/contact-us/harassment-complaint

Please report any violation of the above policies to CompTIA staff immediately.
Violators will be removed from the event or meeting.

WE ARE THE CompTIA COMMUNITY

Katrin Giza
CompTIA

Leanne Johnson
CompTIA

WE ARE THE CompTIA COMMUNITY

Leanne Johnson
CompTIA

MJ Shoer
CompTIA

Kris Nagamootoo
CompTIA

Luke Barton
CompTIA

CompTIA COMMUNITY

08:30 - 9:00	**Registration and Breakfast**
9:00 - 09:15	**CompTIA Welcome** **Leanne Johnson**, CompTIA
09:15 - 9:25	**Community Introduction** **Daniëlle Meulenberg,** Sophos **and Steven Tytgat,** Tyneso
09:25 - 09:45	**CompTIA Community Updates** **MJ Shoer,** CompTIA
09:45 - 11:00	**Keynote: Navigating the NIS2 Directive: Legal Responsibilities and Potential Penalties** **Maarten Verhaghe**, TRUST Advocaten
11:00 – 11:10	**Break**
11:10 - 11:20	**Keynote: Attracting Women to Tech: Strategies and Respect in the Workplace** **Lieve Van der Voorde,** Kyocera **Sibyl Jacob,** Kingston
11:20 - 12:00	**Respect: The Key to Empowerment in Tech** **Steff Vanhaverbeke**, The House of Coaching
12:00 - 13:00	**Lunch**
13:00 - 14:00	**Keynote: Future-Proofing Your Company: Embracing New Management Styles** **Patrick Steenssens**, TD SYNNEX

CompTIA COMMUNITY

14:00-15:00	**Decoding NIS2: A Comprehensive Look at Technology and Insurance Aspects** **Mario Casier**, Software & Security Copaco Belgium **Vicky Vandergeeten**, Vanbreda Risk & Benefits, **Tom Van Britsom**, Vanbreda Risk & Benefits	
15:00-15:30	**Break**	
15:30 – 16:30	**Insights from the CompTIA Community – UK & I Cybersecurity Interest Group** **Greg Jones,** Kaseya / Datto	**Interactive Session: Ask the experts about any questions on Cyberinsurance or NIS2 legal aspects** **Vicky Vandergeeten**, Vanbreda Risk & Benefits **Tom Van Britsom**, Vanbreda Risk & Benefits **Maarten Verhaghe**, TRUST Advocaten **Mario Casier**, Software & Security Copaco
16:30 -16:45	**Cybersecurity Interest Group for Benelux** **Pierre Kleine Schaars,** Quality Cyber Solutions **Tycho Löke,** PeopleRock	
16:45 – 17:00	**End of Day Recap** **Steven Tytgat**, Tyneso **Daniëlle Meulenberg**, Sophos	
17:00-19:30	**Networking Buffet Dinner & Drinks**	

Insights from the CompTIA Community UK&I Room: MEIR, 2nd floor

CompTIA COMMUNITY

CompTIA®

Networking

Member-led communities, councils and events that help tens of thousands of executives and professionals learn and collaborate with peers.

Education

Vendor-neutral education, business standards, technical content and career advice to help drive company and professional growth.

Thought Leadership

Highly regarded research and subject-matter expertise covering workforce developments, emerging technologies and business trends.

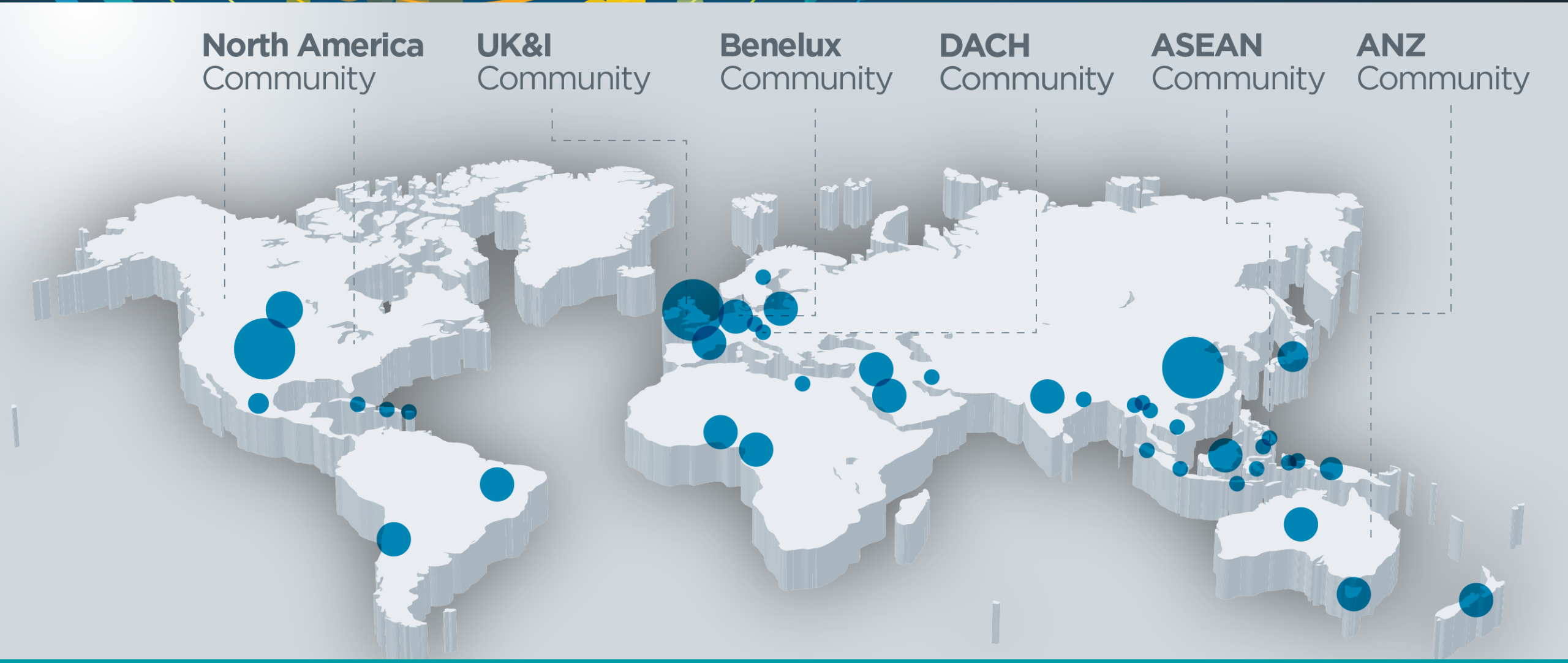
Certification

Vendor-neutral certifications that help millions of IT professionals around the world validate their skills and advance in their careers.

Philanthropy

Help for those who are under-represented in IT and those who lack economic opportunity to prepare for, secure and succeed in IT careers.

CompTIA COMMUNITY



Global Reach of Our Member Community

CompTIA
Estelle Johannes COMMUNITY

North America Community
UK&I Community
Benelux Community
DACH Community
ASEAN Community
ANZ Community


Adam Proulx


Brianna White


Sam Ross


Leanne Johnson


Katrin Giza


Rose Stamell

Regional Groups

Interest Groups in Benelux

CompTIA®
COMMUNITY

Advancing Women in Technology (AWIT)

Meeting Member Needs: Our members have voiced an interest in seeing more women in IT, highlighting the importance of this issue. Their requests are a driving force behind our commitment to this cause.

Enhancing Industry Growth: By developing and executing initiatives that promote the advancement of women in IT, we are not only supporting gender diversity but also contributing to the overall progress and innovation in the industry.

Pioneering Global Change: Our efforts will initially focus on North America and Benelux, setting the stage for a broader global impact. These regions will be the starting point for our initiatives, with plans to extend our reach globally.

CompTIA COMMUNITY

We welcome you to join us.

Join the Group

CompTIA COMMUNITY

Start the conversation

Interest Group Chat

CompTIA COMMUNITY BENELUX

CompTIA Community Benelux Advancing Women in Tech Interest Group

19 February 1-2pm CET

https://connect.comptia.org/events/view/comptia-community-benelux-advancing-women-in-tech-interest-group

CompTIA COMMUNITY BENELUX

CompTIA Community Benelux Cybersecurity Interest Group

13 February 11am-12noon CET

https://connect.comptia.org/events/view/comptia-community-benelux-cybersecurity-interest-group

CompTIA Community Benelux MSP Interest Group

3 Part Marketing Lunch and Learn Series

A series of webinars on digital marketing for MSPs looking to either begin or enhance their digital marketing efforts

20 March 12.15-1pm CET: Content Marketing for MSPs – Unlock the Power of Your Brand

17 April 12.15-1pm CET: Social Media Mastery for MSPs – Connecting With Your Audience

15 May 12.15-1pm CET: SEO Strategies for MSPs – Boost Your Online Visibility

CompTIA COMMUNITY BENELUX

CompTIA Community Benelux MSP Interest Group

3 Part Marketing Lunch and Learn Series

https://connect.comptia.org/events/view/comptia-community-benelux-msp-interest-group---marketing-lunch-and-learns-(3-part-series)

CompTIA COMMUNITY BENELUX

CompTIA Community Benelux Emerging Technology Interest Group

https://forms.office.com/r/3Y37yZHqaj

Highlights

CompTIA COMMUNITY

October 2023

EMEAMember & Partner Conference – Benelux, DACH, UK&I EC

Spotlight Awards – ANZ Community

Mentor | Mentee Programme – NA Region

MSP and Cyber GuideBook – NA Region

*State of Cybersecurity**

December 2023

Year End Planning Meeting in New Orleans

From Member Journey to Women in Tech

60 leaders input & guidance for 2024/5 strategy

*IT Industry Outlook (Benelux)**

November 2023

New EC Members elected – ANZ, Benelux, North America and UK&I

Seeheim Meeting - DACH Community

Eindhoven - Benelux Community

Global Task Force

January 2024

Cybersecurity Interest Group Meeting in Birmingham UK&I

**research reports*

RESEARCH REPORT | SEPTEMBER 2023

STATE OF CYBERSECURITY 2024

DOWNLOAD THE FULL REPORT

People

Product

Methodology

About CompTIA

Trends to Watch 2024

Policy
Risk management is the driving force behind cybersecurity

People
Talent pipelines get stronger as firms build skill resilience

Process
Cybersecurity processes drive a wide range of decision-making

Product
AI drives the cybersecurity product set to new heights

INTERNATIONAL BRIEFS

ANZ

ASEAN

Benelux

DACH

UKI

https://connect.comptia.org/content/research/cybersecurity-trends-research

CompTIA COMMUNITY

CompTIA Gives Back: 2023 Community Philanthropy Recipients

$120,000 donated to tech-focused charitable organizations

Accelerating Aotearoa Inc. $5,000

Apps for Good $5,000

The Cyber Helpline $10,000

i.c.stars $30,000

Ignite Worldwide $5,000

Innocent Lives Foundation $30,000

KiKa $10,000

Project Tomorrow $5,000

The Smith Family $5,000

Teen Tech Charity $5,000

Women in Tech $10,000

CHARITY SUGGESTIONS FOR THE BENELUX REGION

We'd love your charity suggestions for the Benelux region 2024. Please send to kgiza@comptia.org or use the form by 16 February

WE ARE THE
CompTIA
COMMUNITY

Sam Ross

CompTIA

SRoss@comptia.org

Copyright© 2023 CompTIA, Inc. All Rights Reserved. | Connect.CompTIA.org

Executive Council

CompTIA COMMUNITY

BENELUX

Timon Bergsma
Pax8

Jef Bogaerts
Zomentum

Jos Hageman
Scale-up

Sibyl Jacob
Kingston
Technology Belux

Pierre Kleine Schaars
ICT
Cyber Security

Daniëlle
Meulenberg
Sophos
Chair CompTIA
Community Benelux

Ashley Schut
ESET Nederland

Steven Tytgat
Tyneso
Vice Chair CompTIA
Community

Lieve Van De Voorde
KYOCERA

Valérie Vernout
Data Wise Consultancy

08:30 – 09:00	Registration, Breakfast and Networking
09:00 – 09:15	CompTIA Welcome
09:15 – 09:25	***Community Introduction***
09:25 – 09:45	CompTIA Community Updates
09:45 – 11:00	Keynote: Navigating the NIS2 Directive: Legal Responsibilities and Potential Penalties
11:00 – 11:10	Break

WE ARE THE CompTIA COMMUNITY

Daniëlle Meulenberg
Sophos

Chair CompTIA Benelux Community

Steven Tytgat
Tyneso

Vice Chair CompTIA Benelux Community

08:30 – 09:00 Registration, Breakfast and Networking

09:00 – 09:15 CompTIA Welcome

09:15 – 09:25 Community Introduction

09:25 – 09:45 ***CompTIA Community Updates***

09:45 – 11:00 Keynote: Navigating the NIS2 Directive: Legal Responsibilities and Potential Penalties

11:00 – 11:10 Break

WE ARE THE CompTIA COMMUNITY

MJ Shoer

Chief Community Officer, CompTIA

CEO, CompTIA Spark

WE ARE THE
CompTIA
COMMUNITY

Brand Streamlining & New Naming Convention Guidelines

WORDMARK	BRAND NAME
CompTIA® COMMUNITY	CompTIA Community

We are one community.

The word community and the slogan We are the CompTIA Community refers to **all regional membership** groups as a whole (and never one individual group of any kind).

WE ARE THE CompTIA COMMUNITY

REGIONAL GROUPS: WORDMARKS

CompTIA COMMUNITY ANZ

CompTIA COMMUNITY DACH

CompTIA COMMUNITY ASEAN

CompTIA COMMUNITY North America

CompTIA COMMUNITY Benelux

CompTIA COMMUNITY UK & Ireland

NAMING CONVENTION UPDATES

CompTIA COMMUNITY

PREVIOUS	NEW TERM / USAGE
committees	**interest groups**
forums	**online discussion groups**
registered user	**non-member subscriber / subscriber**

CompTIA Community interest groups:

- **DEI Interest Group**
- **Managed Services Interest Group**
- **Cybersecurity Interest Group**
- **Emerging Technology Interest Group**
- **Advancing Women in Tech Interest Group**

CompTIA COMMUNITY

CompTIA CYBERSECURITY Information Sharing and Analysis Organization

Connecting to an incredibly powerful network of more than 1,000 tech vendors, MSPs/solution providers, and business technology consultants on the front lines of cybersecurity.

Gain allies who are working together to share information about the latest cybersecurity risks.

Thwarting the malicious attacks that threaten our businesses, our customers, and the credibility of our industry.

Enhancing your reputation and thought leadership in the tech and security industries.

Demonstrating social and cybersecurity responsibility.

CompTIA COMMUNITY

CompTIA ISAO Cyber Forum

94 MJ Shoer 117 Search...

- Home
- CyberWeekly Podcast
- Breaking News! Podc...
- Cyber Risk Rating
- Forums
- News Feeds
- Resources
- Sophos X-Ops Intelix
- Threat Reports
- TruSTAR Login
- Members
- My.CompTIA
- Help Documents
- Preference Center

Forum list | Threads | Latest activity 10+ | Posts | Questions | Resources | Create

1 2 3 ... 146 Next › | Set default

INFORMATIONAL TLP:GREEN Zero-Days in Edge Devices Become China's Cyber Warfare Tactic of Choice
Cariza Schiavone · Yesterday at 3:03 PM · Threat Intelligence
China's Cyber Warfare Tactics
0 ratings Updated: Yesterday at 3:03 PM

ACTIONABLE Severity: Medium TLP:GREEN LockBit Ransomware Exploits Citrix Bleed in Attacks, 10K Servers Exposed
Asim Subedi · Yesterday at 2:36 PM · Threat Intelligence
Ransomware Attack
0 ratings Updated: Yesterday at 2:36 PM

INFORMATIONAL TLP:GREEN 82% of Attacks Show Cyber-Criminals Targeting Telemetry Data
Asim Subedi · Yesterday at 2:35 PM · Vendor Reports
82% of Attacks Show Cyber-Criminals Targeting Telemetry Data
0 ratings Updated: Yesterday at 2:35 PM

INFORMATIONAL Severity: Medium TLP:GREEN BlackCat Ransomware Gang Targets Businesses Via Google Ads
Jonathan Braley · Yesterday at 10:34 AM · Threat Intelligence
Ransomware
0 ratings Updated: Yesterday at 10:34 AM

INFORMATIONAL Severity: Low TLP:GREEN DDoS Attacks Underscore the Vulnerability of Public Systems
Asim Subedi · Tuesday at 4:53 PM · Threat Intelligence
DDoS Attack
0 ratings Updated: Tuesday at 4:53 PM

Filter

In category:
- Cyber Forum Policies
- Cyber Genius Videos
- Help Documents
- Member Resources
- Threat Reports

- Watched resources
- Watched categories
- All
- People you follow
- People that follow you

Save

- CompTIA ISAO - FREE to ALL MSP/solution provider members
  - Cyber Forum – online forum, safe space for discussion and collaboration
  - Informational and Actionable Threat Reports
    - Easy to understand, with threat analysts comment
    - Access to Splunk / TruStar Threat Intelligence Management
  - Access to Sophos X-Ops Intelix
  - Access to Cyber Risk Rating powered by Security Scorecard
  - Monthly Member Meetups every 3rd Wednesday, 2 sessions for our global members
  - Access CompTIA ISAO Cyber Forum from my.CompTIA.org

CompTIA CYBERSECURITY Emergency Response Team

- MSP911.org
- Launched in North America March 2023
- Free assistance to any MSP/solution provider experiencing a cybersecurity incident
- Launched by victims of the July 2022 Kaseya attack
- This is NOT incident response
- Provides a coach to help you through the critical initial hours/days
- Live call center 24/7

CompTIA COMMUNITY

CompTIA CYBERSECURITY Trustmark

- Organizational Accreditation designed specifically for MSPs/solution providers to establish a foundational security program for their organization
- Based on industry accepted best practices across varying controls from globally recognized frameworks
- Includes access to a GRC Platform
- Participant discussion in the CompTIA ISAO Cyber Forum (private group)
- Weekly calls with Platform Partners, FortMesa and Cybersecurity Program Team members to help you succeed
- Join over 900 companies from 27 countries!

08:30 – 09:00 Registration, Breakfast and Networking

09:00 – 09:15 CompTIA Welcome

09:15 – 09:25 Community Introduction

09:25 – 09:45 CompTIA Community Updates

09:45 – 11:00 ***Keynote: Navigating the NIS2 Directive: Legal Responsibilities and Potential Penalties***

11:00 – 11:10 Break

WE ARE THE

CompTIA®

COMMUNITY

Maarten Verhaghe

Trust Advocaten

COMPTIA 08.02.2024, Antwerp – NIS 2.0


Attorney - Partner
Certified DPO
Guest Lecturer
Author
Mr. Maarten Verhaghe


IT
IP
Data Protection
Cybersecurity

01

EU Cyber Strategy

EU Cyber Strategy 2013

"An Open, Safe and Secure Cyberspace"

- EU statement
- Brussels dd. 7 February 2013
- Resilient digital information systems
- User awareness
- Improved coordination between::
  - Member States
  - Legal and enforcement agencies
  - Public and private stakeholders
- Strengthening cybersecurity and defence policy in the EU

- ➔ NIS Directive and Cybersecurity Regulation

EU Cyber Strategy 2020

"Integrate cybersecurity into every element of the supply chain and bring further together EU's activities and resources across the four communities of cybersecurity – internal market, law enforcement, diplomacy and defence"

- EU statement
- Brussels dd. 16 December 2020

EU Cyber Strategy 2020

- Increasing cyber and physical resilience
  - Adaptation of legislative framework after review
    - Update NIS Directive
    - New directive for resilience of critical entities (extension directive 2008)
  - Cybersecurity of Internet of Things (IoT)
  - Cybersecurity shield in the EU
    - Establishment of Security Operations Centres
    - Powered by AI
    - Early detection of cyber-attacks and enabling proactive attacks
    - Avoiding damage
  - Responding to major attacks
  - Global collaboration to ensure security and stability in cyberspace

  ➔ NIS 2.0 Directive and Cyber Resilience Regulation

02

Current Legal Framework

Current Legal Framework?

- Various Regulations and Directives
  - E-Commerce Directive (2000)
  - E-Privacy Directive (2002)
  - Eletronic Identification and Trust Services Regulation - eIDAS (2014)
  - General Data Protection Regulation - GDPR (2016)
  - Belgian Framework Law on the Processing of Personal Data (2018)
  - Network Information Security Directive – NIS (2016)
  - Law Establishing a Framework for the Security of Network and Information Systems of Vital Importance for Public Safety (2019)
  - Cybersecurity Regulation (2019)

New Legal Framework?

- Recently approved:
  - Data Act
    - Access to data of consumers and businesses generated through products/devices
    - New legal provisions to strengthen the negotiating position of Small and Medium-sized Enterprises (SMEs)
    - Prevention of contractual imbalances
  - Cyber Resilience Act
    - Security of products (both software and hardware) with digital elements
    - Obligations for manufacturers (conformity declarations and CE marking)
    - Administrative fines up to €15,000,000 for market participants
  - AI Act
    - Regulation of artificial intelligence
    - Classification of AI systems + prescriptions
    - Risk assessments, data management, and cybersecurity

03

NIS2 Directive

Material Scope of Application

- **Measures aimed at achieving a high common level of cybersecurity in the EU.**
- **Security of network and information systems (art. 6.1 en 6.2 NIS2 Directive):**

‘network and information system’:

*a) an **electronic communications network** as defined in Article 2, point (1), of Directive (EU) 2018/1972;*

*b) any **device or group of interconnected or related devices**, one or more of which, pursuant to a programme, carry out automatic **processing of digital data**; or,*

*c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and **maintenance**;*

‘security of network and information systems’:

*The ability of network and information systems to resist, at a given level of confidence, any event that may compromise the **availability, authenticity, integrity or confidentiality** of stored, transmitted or **processed data** or of the services offered by, or accessible via, those network and information systems,*

Personal Scope of Application

- **Expansion of the scope of NIS1**
  - New sectors included under the scope
  - Based on NACEBEL-Codes – registration in the CBE (KBO)
    - Postal and courier services
    - Waste management
    - Production en distribution of chemical substances/food products
    - Manufacturing of medical devices, ICT products, electrical equipment, etc.
    - Public authorities (including local and education, if decided by the Belgian legislator)
    - Critical infrastructures in accordance with Directive 2022/2557
    - ICT manager and ICT security manager
  - Entities with more than 50 employees or an annual turnover (or annual balance sheet total) exceeding 10 million euros

Scope Art. 2 and 3 NIS2 Directive

Sector	Subsector	Jurisdiction	NIS-1 & CER entities (+ equivalent)	Large entities (more than 250 employees or more than 50 million revenue)	Medium (more than 50 employees or more than 10million revenue)	Small & Micro
Annex I: Sectors of high criticality						
1. **Energy**	Electricity; district Heating &cooling; Gas; Hydrogen; oil;	The Member State(s) where it is established	Essential	Essential	Important, except if identified as essential by Member State	Not in Scope, except if identified as essential or important by national authorities due to sole service, significant impact, essential to society
2. **Transport**	Air; Water; Rail; Road					
	Special case: Public Transport: **only** if identified as CER					
3. **Banking**	Credit institutions **(attention: DORA lex specialis)**					
4. **Financial Market Infrastructure**	Trading venues, central counterparties **(attention: DORA lex specialis)**					
5. **Health**	Healthcare providers; EU reference laboratories; R&D of medicinal products; manufacturing basic pharma products and preparations; manufacturing of medical devices critical during public health emergency					
	Special case: entities holding a distribution authorization for medicinal products: **only** if identified as CER					
6. **Drinking Water**						
7. Waste Water	(only if it is an essential part of their general activity)					
8. **Digital Infrastructure**	Qualified trust service providers			Essential		
	DNS service providers (excluding root name servers)	**One stop**: Only the MS where they have their main establishment				
	TLD name registries					
	Providers of public electronic communications networks	Member State in which they **provide their services**		Essential		Important, except if identified as essential based on National risk assessment
	Non-qualified trust service providers	The Member State(s) where it is established				
	Internet Exchange Point providers		Essential	Essential	Important, except if identified as essential by Member State	Not in Scope, except if identified as essential or important
	Cloud computing service providers	**One stop**: Only the MS where they have their main establishment				
	Data centre service providers					
	Content delivery network providers					
8a. ICT-service management	Managed (Security) Service Providers					
9. Public Administration entities	Of central governments (excluding judiciary, parliaments, central banks; defence, national or public security).	MS that established them		Essential		
	Of regional governments: risk based. (Optional for Member States: of local governments)			Important, except if identified as essential by Member State		
10. Space	Operators of ground-based infrastructure (by MS)	The Member State(s) where it is established		Essential	Important, except if identified as essential by Member State	Not in Scope, except if identified as essential or important
Annex II: other critical sectors						
1. Postal and courier services		The Member State(s) where it is established	Essential	Important, except if identified as essential by Member State		Not in Scope, except if identified as essential or important by national authorities due to sole service, significant impact, essential to society
2. Waste Management	(only if principal economic activity)					
3. Chemicals	Manufacture, production, distribution					
4. Food	Production, processing and distribution					
5. Manufacturing	(in vitro diagnostic) medical devices; computer, electronic, optical products; electrical equipment; machinery; motor vehicles, trailers, semi-trailers; other transport equipment (NACE C 26-30)					
6. Digital providers	online marketplaces, search engines, social networking	**One stop**: Only the MS where they have Main establishment				
7. Research	Research organisations **(excluding education institutions)**	Member State(s) where established				
Entities providing domain name registration services		**One stop**: Only the MS where they have Main establishment	*All sizes, but only subject to Article 3(3) and Article 28*			

Designation by the legislator?

- **NIS2 Bill provides for the possibility of identification**
  - Designation of new NIS2 entities
  - Designation new NIS2 sectors
  - Expansion of existing sectors using NACEBEL-codes

- **Evaluation of identification**
  - Biannual

How to determine whether a company falls under the scope?

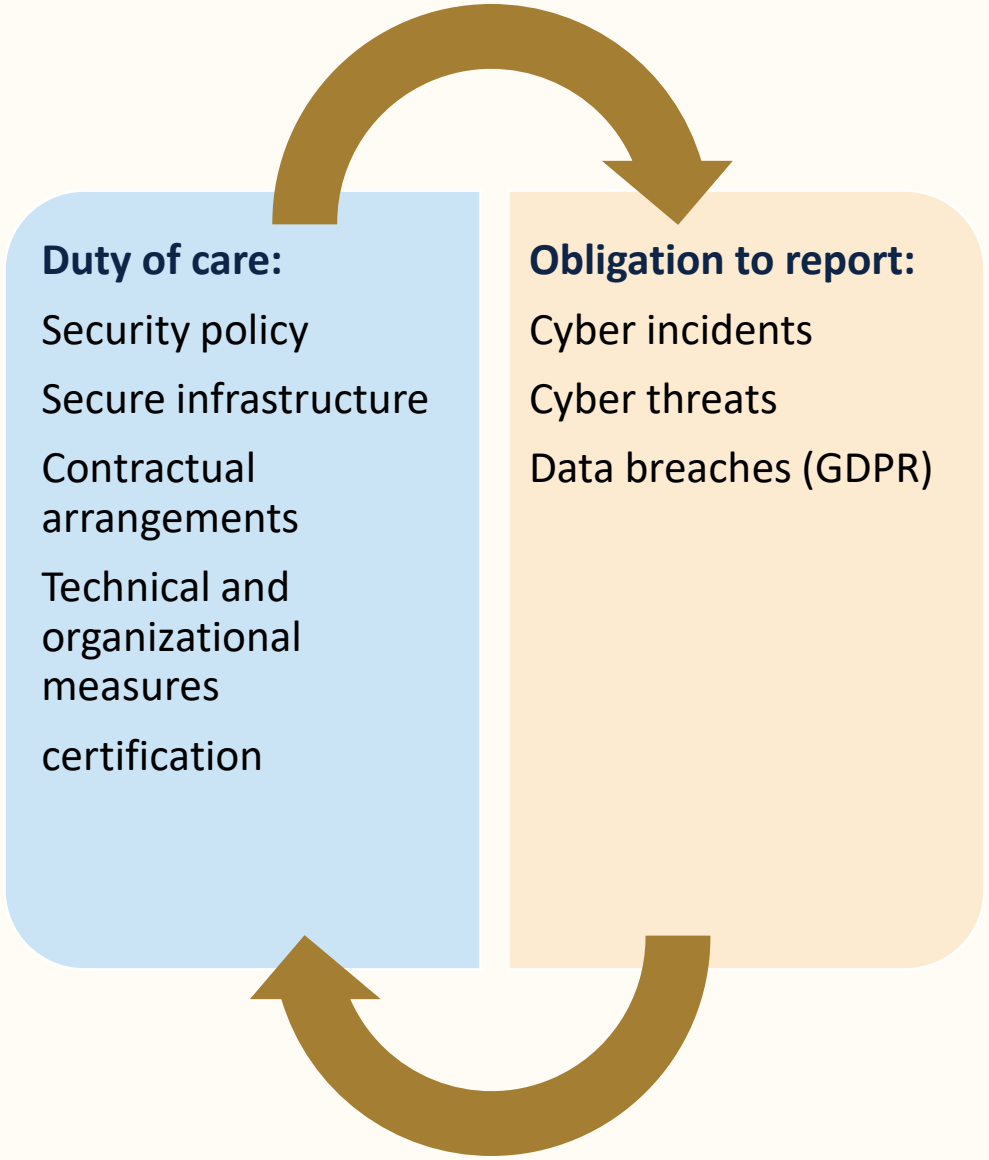
- **Audit (legal)**
  - Review of the company's current activities and NACEBEL-code
  - Screening of the company's future activities
  - Analysis of turnover and employees
  - Desgination by the legislator

- **Know Your Customer → Supply chain security**
  - Direct NIS2 customers
  - Indirect NIS2 customers (sub-suppliers)

04

NIS2 - Obligations

NIS 2.0



“Ongoing obligation of means”

Obligation to continuously evaluate and update measures

Governance: Art. 20 NIS2 Directive

- **Awareness and liability**
  - Obligation to supervise the implementation of cybersecurity measures
  - Governing bodies responsible for non-compliance with the obligations as specified in article 21 et seq. of the NIS2 Directive
  - Regularly attend specific training courses to acquire sufficient knowledge and skills to identify and assess risks and management practices in the field of cybersecurity and their impact on the entity's activities.
  - Similar training for employees to enable them to identify risks and assess their consequences.

Measures for Cyber Risks: Art. 21 NIS2 Directive

- Adoption of appropriate, proportionate technical and organizational measures: broad formulation
  - Taking into account the state of the art
  - Measures tailored to the risk, but at least the following:
    - Policy for risk analysis and security of information systems
    - Incident handling
    - Business continuity (backup management, emergency provision, and crisis management)
    - Security of the supply chain (Art. 24 NIS2 Directive)
    - Security in the acquisition, development, and maintenance of network and information systems
    - Policy and procedures for encryption
    - Policy and procedures to assess the effectiveness of measures
    - Security aspects concerning personnel, access policies
    - Multi-factor authentication

Risk Management Measures: Art. 21 NIS2 Directive

- **Specific measures or guidelines?**
  - By the 17th of October 2024, the EU Commission will propose implementing acts for:
    - DNS service providers
    - Cloud computing
    - Data centers
    - Hosting
    - ICT manager and ICT security manager
    - Online marketplaces
    - Social media
    - Trust services

Risk Management Measures: NIS2 Bill

- **Security policy?**
  - A physical or digital document
    - Creation of a risk analysis considering all hazards.
      - Network and IT systems
      - Physical environment of Network and IT systems
    - Protection and safety measures
    - At least include everything stated in Article 21 of the NIS2 Directive

  - Ontbreken beveiligingsbeleid
    - Na vaststelling, onmiddellijk corrigerende maatregelen nemen

Supply Chain Security

- **Legal obligation?**
  - Article 7 and 21.3 of the NIS2 Directive:
    - Member States shall establish policies on cybersecurity in the supply chain for ICT products and services used by entities to provide their services
      - The procurement options for NIS2 entities will be limited.
      - Suppliers will have to conform to NIS2 and meet a high level of cybersecurity.
      - Contractual arrangement for cybersecurity (for suppliers).
      - Also with regards to suppliers outside the scope of NIS2.

Supply Chain Security

Consideration 85 NIS2 Directive:

"Essential and important entities should therefore assess and take into account the overall quality and resilience of products and services, the ***cybersecurity risk-management*** *measures embedded in them, and the* ***cybersecurity practices of their suppliers and service providers****, including their secure development procedures.*

Essential and important entities should in particular be encouraged to incorporate ***cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers****. Those entities could consider risks stemming from other levels of suppliers and service providers."*

Supply Chain Security

- **Supplier Assessment?**
  - Article 21.3 NIS2 Directive:
    - Screening of (sub-)suppliers and service providers
      - *Taking into account specific vulnerabilities.*
      - *General quality of cybersecurity practices of products.*
      - *Secure development procedures for products and services.*
    - *Similar to "vendor-assessment" under the GDPR (art. 28.1 GDPR)*

"…, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures…"

Supply Chain Security: NIS 2 Bill

- **Screening sub-suppliers confirmed?**

"When essential and significant entities consider which measures referred to in paragraph 3(4) are appropriate, they shall take into account the specific vulnerabilities of each direct supplier and service provider and the overall quality of the products and cybersecurity practices of their suppliers and service providers, including their secure development procedures."

- Obligation under Belgian Bill
- Analysis of vulnerabilities
- Security measures
- Contractual guarantee

Supply Chain Security

- **Contractual addition?**
  - Article 21.3 and recital 85 NIS2 Directive:
    - Double obligation:
      - Contractual arrangement (pay attention: B2B law and new CC)
        - Risk assessment information security policy
        - Audit regulation
        - Procedures regarding incident report
        - Emergency recovery and measures
        - Warranties and declarations of conformity
        - State of the art security measures
        - ISO 27001 and 27002 as a minimum
      - Declaration of conformity: regarding suppliers / customers
    - Drafting supplier evaluation

Conformity assessment: Bill NIS2

- **Regular conformity assessment?**
  - Essential entities
    - 2 possibilities:
      - Assessment by a Conformity assessment body designated by CCB
        - Assessment against CCB reference framework
        - ISO 27001
      - Check by inspection service CCB
        - Retribution fixed in draft RD

NIS2 compliance? : Bill NIS2

- **Regular conformity check by assessment body**
- **Presumption of compliance**
  - Until proven otherwise
    - Essential entities:
    - Important entities, on a voluntary basis
      - ISO 27001 is a minimum

Duty to report: Art. 23 NIS2 Directive

- **Essential and important entities:**
  - Reporting significant incident and threats (where applicable) to their customers (art. 23.1 and 2 NIS 2 Directive)
  - Reporting of significant incidents (art. 23.3 NIS 2 Directive)

> *"(a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;*
>
> *(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage."*

- The EU Commission will only specify on October 17, 2024 the cases in which an incident should be considered "significant" for ICT service providers (service providers as security service operators).

Duty to report: Art. 23 NIS2 Directive

- **Current framework NIS1 Directive**
  - **NIS 1 assessment:** *the availability, confidentiality, integrity or authenticity of the network and information systems on which the essential service or services it provides depend*
  - **Or:**

Duration of the incident *Unavailability for more than 5,000,000 user hours*	▪ The term *'duration'* refers to the time span from the moment the service no longer functions properly in terms of availability, authenticity, integrity, or confidentiality, to the moment of full restoration of the service; ▪ The term *'user hour'* refers to the number of users in the European Union affected for a time span of twenty minutes.	**Nature of the impact** *Risk to public security* *or* *Risk to public safety* *or* *Has led to a risk of loss of human life*	▪ The DSP can determine the nature of the impact based on indicators such as the nature of its contractual involvement with the client or, if applicable, the potential number of affected users
Number of users *More than 100,000 affected users*	▪ Included in the '*users*' of digital services are all natural persons and legal entities who are customers or subscribers to an online marketplace or cloud computing service, or who perform searches on the website of an online search engine by entering search terms.	**Material damage** *Caused damage > €1,000,000*	▪ The incident causes >€1,000,000 damage to at least one user in the European Union

Duty to report: Art. 23 NIS2 Directive

- **Essential and important entities:**
  - **Incident reporting**

    - To the CSIRT or competent authority
    - Without delay and at the latest within 24 hours in case of suspicion of malicious intent or cross-border impact
    - Update without delay and at the latest within 72 hours
    - Draft interim reports and a final report no later than one month after notification
    - Communication to the public by CSIRT or competent authority or concerned entity

Presumption of compliance: Art. 24 NIS2 Directive

- **Cybersecurity certification (art. 24 NIS2 Directive)**

- Presumption of compliance with security obligation
- **Member States may impose specific certification**
- Cybersecurity Regulation
- Distinction with NIS1 ➔ ISO 27001 presumption of compliance with AED (not DDV)

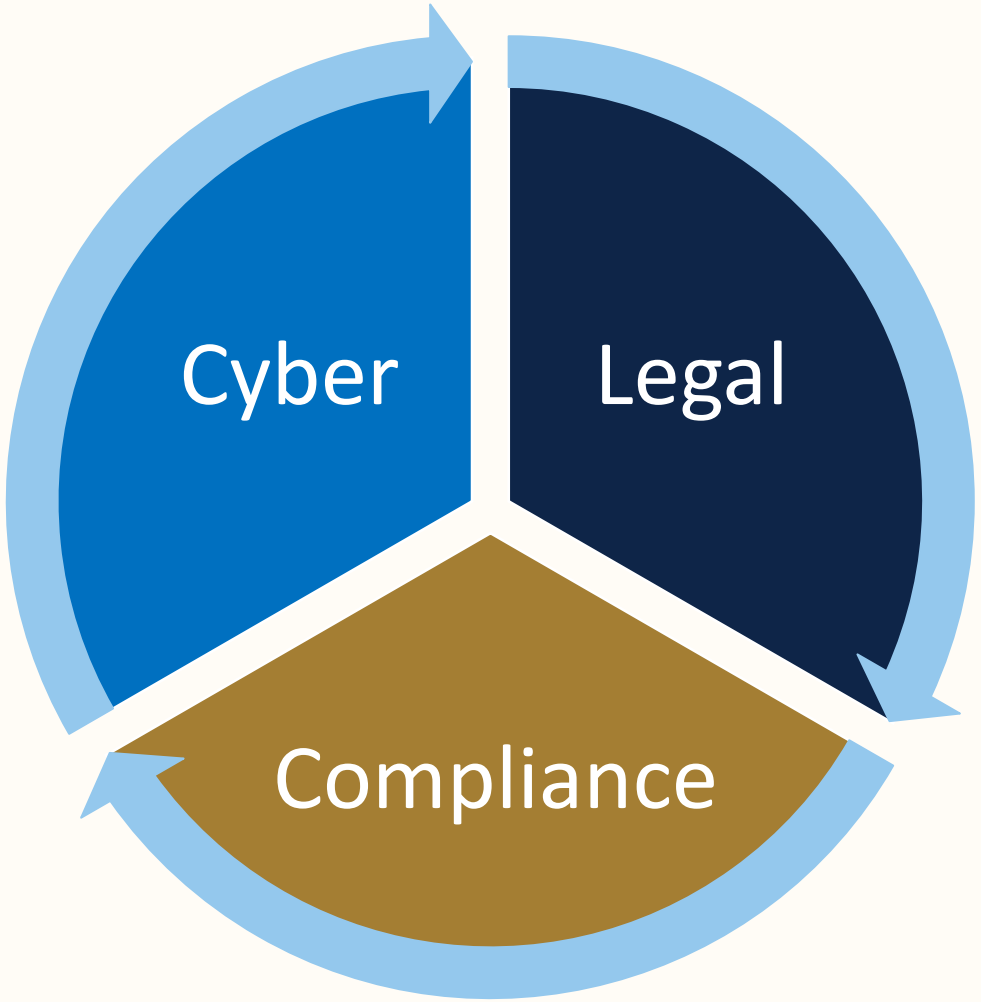
- Cf. combination with supply chain security (art. 21 NIS2 Directive).

Beware: NIS2 on public procurement?

- **Local authorities may be governed by NIS2 (art. 2.5 NIS2 Directive)**
  - National legislator decides at the end of 2024

- Cybersecurity requirements for ICT products and ICT services
  - Tendering procedures
  - Specific requirements
  - Certification
  - Encryption
  - Use of open source

How to be NIS 2 compliant?



- **Cybersecurity audit**
  - Analyse security
  - Determining crown jewels
- **Legal audit**
  - Know your customer
  - Risk assessment suppliers + suppliers' chain
  - Assessment of existing contract (own + suppliers)
- **Drafting contractual framework**
  - Vendor assessment
  - Contractual provisions regarding notification, audit, guarantees, security measures …
- **Compliance**
  - ISO 27001 and 27002
  - Incident Response Plan and Business Continuity plan
  - Security policy
  - Awareness sessions

05

NIS2 Enforcement

Monitoring and enforcement: Art. 31 - 33 NIS2 Directive

- Competent authorities + cooperation with DPA
  - Inspections on-site
  - Audits
  - Security scans
  - Information requests
  - Requests for access / data / documents / information
  - Request proof of cybersecurity policy

Corrective measures: Art. 32 -33 NIS2 Directive

- Supervisory authority has extensive capabilities:
  - Imposing corrective measures → periodic penalty payment?
  - Ordering: only purchasing ICT products / services / processes if subject to certification
  - Ordering: only developing certified ICT products / services / processes

Sanctions: Art. 32 and 33 NIS2 Directive

- Competent authorities + cooperations with DPA
  - Issuing warnings
  - Adopt binding instructions
  - Order to cease conduct
  - Designate monitoring officer for a determined period of time
  - Making public and publication
  - Administrative fine of at least EUR 10.000.000 / 2% worldwide turnover
  - Administrative fine of at least EUR 7.000.000 / 1,4% worldwide turnover
  - Suspend certifications

Liability: Art. 32 and 33 NIS2 Directive

*"Member States shall ensure that **any natural person** responsible for or **acting as a legal representative** of an essential entity on the basis of the power to represent it, **the authority to take decisions on its behalf or the authority to exercise control of it has the power to ensure its compliance with this Directive**. Member States shall ensure that it is possible to hold such natural persons liable for breach of their duties to ensure compliance with this Directive."*

- Also, important entities (art. 33 NIS 2 Directive)
- Directors
- Board members (CFO, CISO …)

Confirmed in Bill NIS 2

Sanctions: criminal sanctions?

- Recital 131 foresees possibility of criminal sanctions

  “Member States should be able to lay down the rules on criminal penalties for infringements of the national rules transposing this Directive. However, the imposition of criminal penalties for infringements of such national rules and of related administrative penalties should not lead to a breach of the principle of ne bis in idem, as interpreted by the Court of Justice of the European Union.”

- Similar to NIS1

Criminal sanctions under NIS1?

- **Monitoring and findings (Art. 48 – 55 NIS Act)**
  - Official report by inspection authorities
  - Competent sectoral government
    - Notifying public prosecutor (Art. 54 NIS Act)
      - Decision on criminal charges within 2 months
    - If no prosecution, administrative procedure
      - Imposing administrative fine (art. 57 NIS Act)
      - Appeal at Market Court (Brussels Court of Appeal) (art. 57 NIS Act)
  - **Similar regime is expected under NIS2**

Criminal sanctions under NIS1?

Violation	Criminal Sanction ▪ for each offense ▪ In case of a recurrence of the same actions within a period of 3 years, the fine shall be doubled, and the offender shall be subject to imprisonment for a period of 15 days to 3 years.	Administrative Sanction ▪ for each offense ▪ In case of a recurrence of the same actions within a period of 3 years, the administrative fine shall be doubled.
Provide all relevant information to the NIS authorities upon their request.	Imprisonment from 8 days to 1 year and a criminal fine of €208 (€26x8) to €400,000 (€50,000*8), or one of these two penalties	Fine ranging from 500 to 125,000 EUR
Implement technical and organizational measures for the security of the network and information systems on which the provided services depend.	Imprisonment from 8 days to 1 year and a criminal fine of €208 (€26x8) to €240,000 (€30,000*8), or one of these two penalties	Fine ranging from 500 to 100,000 EUR
Report incidents that compromise the security of the network and information systems upon which the provided services depend.	Imprisonment from 8 days to 1 year and a criminal fine of €208 (€26x8) to €160,000 (€20,000*8), or one of these two penalties	Fine ranging from 500 to 75,000 EUR
Ensure the confidentiality/professional secrecy of the information processed in the context of the NIS law. + subcontractors	Imprisonment from 1 year to 3 years and a criminal fine of €800 (€100x8) to €8,000 (€1,000*8), or one of these two penalties (cf. art. 458 Sw.)	
Intentional obstruction of the execution of an inspection by a member of the inspection service, refusal to provide information requested during an inspection, or intentional disclosure of incorrect or incomplete information.	Imprisonment from 8 days to 2 years and a criminal fine of €208 (€26x8) to €600,000 (€75,000*8), or one of these two penalties	Fine ranging from 500 to 200,000 EUR

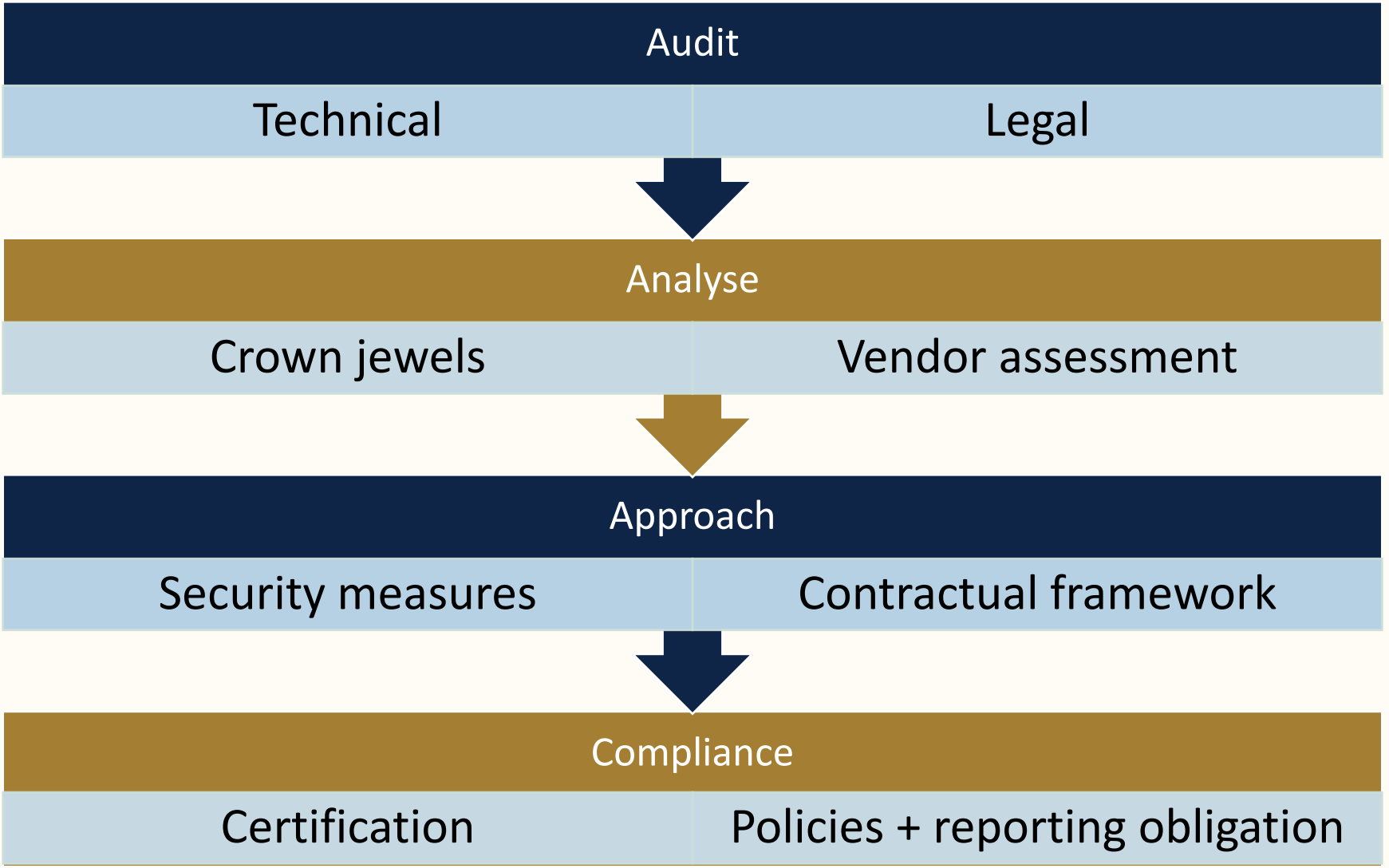
Possibilities to file a complaint?

- **No legal framework foreseen in NIS2 Directive**
  - **But!**
  - Directive: minimum harmonisation
    - Complaint likely possible at Inspection Services
      - Health care: FPS Public health
      - Energy: FPS Economy
      - ICT/digital services: FPS Economy
      - Other important sectors: FPS Economy
  - Bill NIS2
    - Notification of potential security risks to CSIRT
    - Anonymously by natural or legal person

06

Can you prepare?

How to prepare?



Concerns:

- **Security policy + measures**
- **Supply chain security**
  - Certification
  - Contractual securities
- **Incident management**
  - Technical / legally
  - Reporting obligations + methodology (NIS + GDPR)
  - Incident response plan
- **Business continuity**
- **Best practice: ISO 27001 and 27002**

Deadline?

- **Temporal scope:**

- Approved by EU Parliament: November 10th 2022
- Conversion to Belgian law: 18 months ➔ October 2024
- Minimum harmonisation

TRUST
ADVOCATEN

0468 410 690

maarten@trustadvocaten.be

www.trustadvocaten.be

08:30 – 09:00 Registration, Breakfast and Networking

09:00 – 09:15 CompTIA Welcome

09:15 – 09:25 Community Introduction

09:25 – 09:45 CompTIA Community Updates

09:45 – 11:00 Keynote: Navigating the NIS2 Directive: Legal Responsibilities and Potential Penalties

11:00 – 11:10 ***Break***

11:10 – 11:20	***Attracting Women to Tech***
11:20 – 12:00	Respect: The Key to Empowerment
12:00 – 13:00	Lunch
13:00 – 14:00	Keynote: Future-Proofing your Company
14:00 – 15:00	Decoding NIS2
15:00 – 15:30	Break
15:30 – 16:30	Insights from CompTIA Community UK&I / Ask The Experts on NIS2

WE ARE THE

CompTIA®

COMMUNITY

Sibyl Jacob

Kingston

Lieve Van De Voorde

Kyocera

CompTIA COMMUNITY BENELUX

CompTIA Community Benelux Advancing Women in Tech Interest Group

19 February 1-2pm CET

https://connect.comptia.org/events/view/comptia-community-benelux-advancing-women-in-tech-interest-group

11:10 – 11:20 Attracting Women to Tech

11:20 – 12:00 ***Respect: The Key to Empowerment***

12:00 – 13:00 Lunch

13:00 – 14:00 Keynote: Future-Proofing your Company

14:00 – 15:00 Decoding NIS2

15:00 – 15:30 Break

15:30 – 16:30 Insights from CompTIA Community UK&I / Ask The Experts on NIS2

WE ARE THE

CompTIA®

COMMUNITY

Steff Vanhaverbeke

The House of Coaching

11:10 – 11:20 Attracting Women to Tech

11:20 – 12:00 Respect: The Key to Empowerment

12:00 – 13:00 ***Lunch***

13:00 – 14:00 Keynote: Future-Proofing your Company

14:00 – 15:00 Decoding NIS2

15:00 – 15:30 Break

15:30 – 16:30 Insights from CompTIA Community UK&I / Ask The Experts on NIS2

11:10 – 11:20 Attracting Women to Tech

11:20 – 12:00 Respect: The Key to Empowerment

12:00 – 13:00 Lunch

13:00 – 14:00 ***Keynote: Future-Proofing your Company***

14:00 – 15:00 Decoding NIS2

15:00 – 15:30 Break

15:30 – 16:30 Insights from CompTIA Community UK&I / Ask The Experts on NIS2

WE ARE THE

CompTIA®

COMMUNITY

Patrick Steenssens

TD SYNNEX

Are we future proof?

Patrick Steenssens

p.steenssens@tdsynnex.com
+32 486 439 474

Date	Author	Version
08/02/2024	Patrick Steenssens	Rev 0

ARE WE

FUTURE PROOF?

Agenda

- some market trends
- evolution of the IT ecosystem
- are we ready as leaders

2023

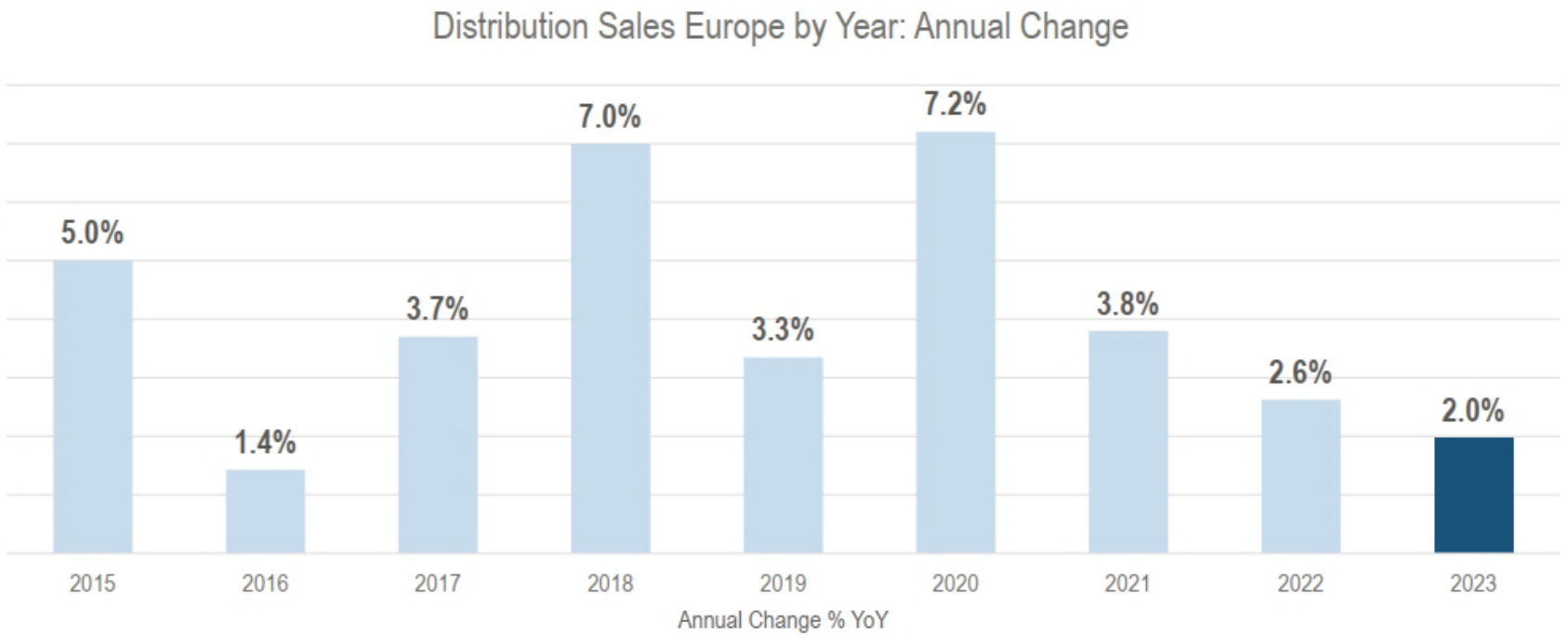
what a year...

2023

Forecast evolution 2023

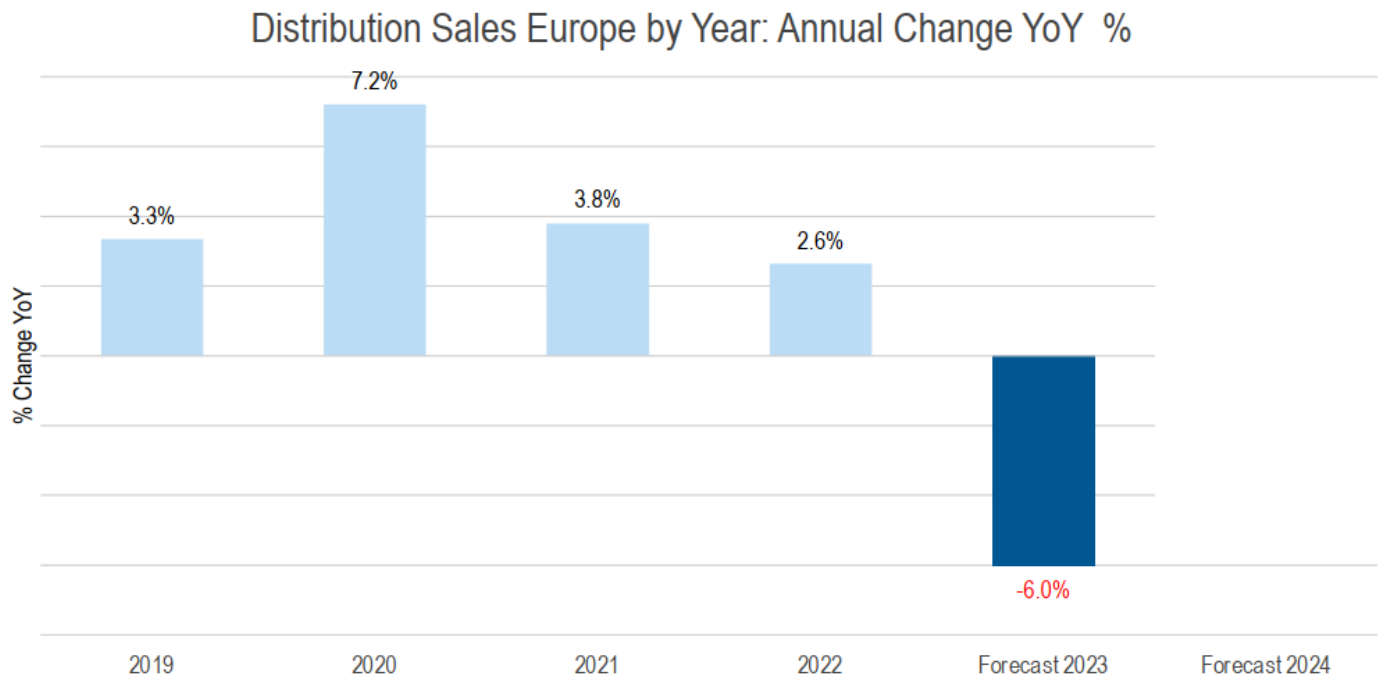
Planning & Outlook January 2023

THE CONTEXT 2023 FORECAST IS FOR SUSTAINED BUT MUTED GROWTH



Revised Outlook after Q3 result

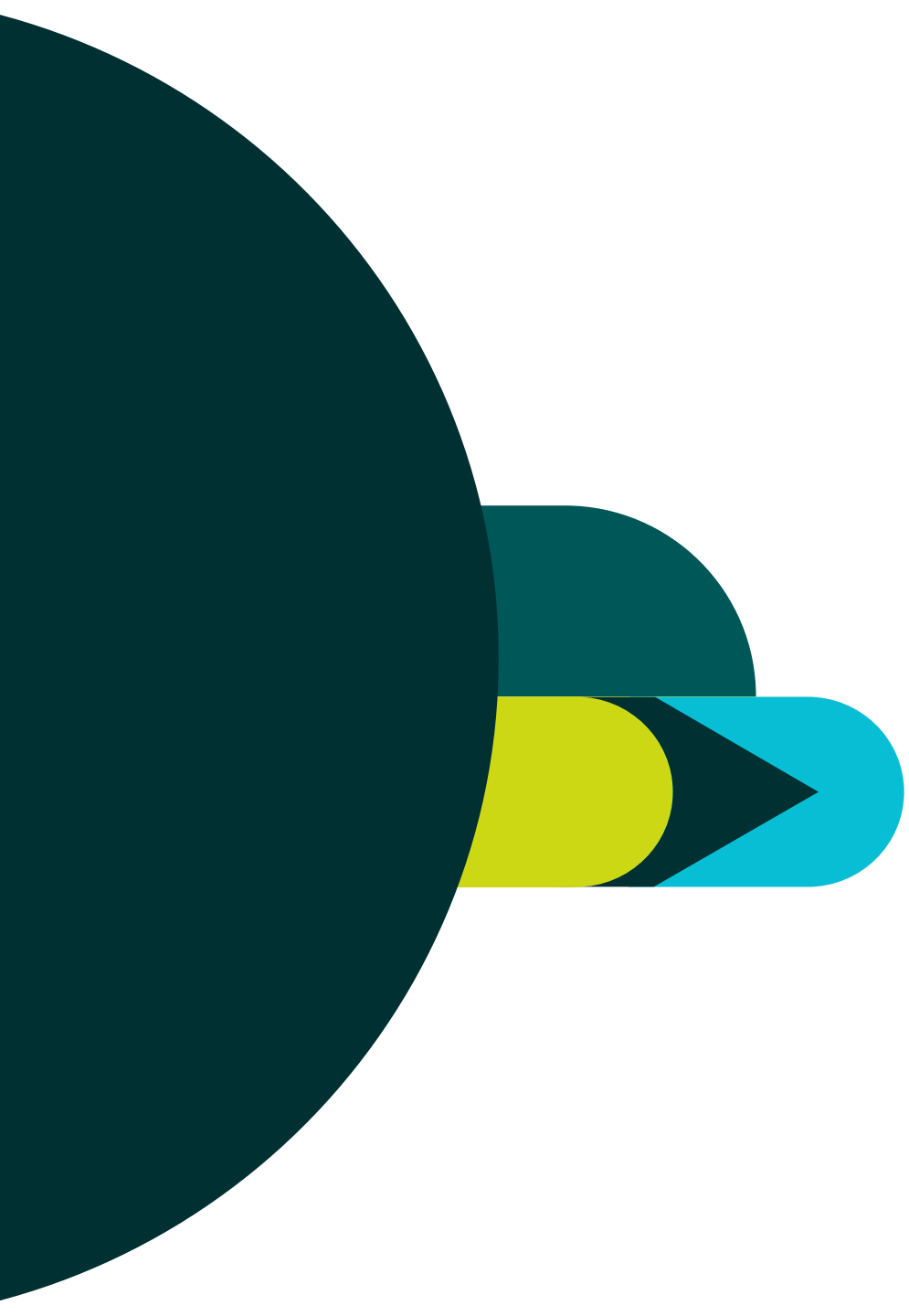
FOLLOWING Q3 RESULTS, WE ARE REVISING OUR FORECAST FOR 2023 DOWN



2023 forecast range from -4.5% to -8.0%

Distribution sales translated at fixed € exchange rate and Panel Europe includes:
Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Ireland, Italy, Latvia, Lithuania, Netherlands, Norway, Poland, Portugal, Slovakia, Spain, Sweden, Switzerland, UK.

Source CONTEXT SalesWatch © 2023 CONTEXT CONFIDENTIAL
// Not to be reproduced or disseminated without permission // Data not adjusted for trading days // Revenue based on fixed FX rates



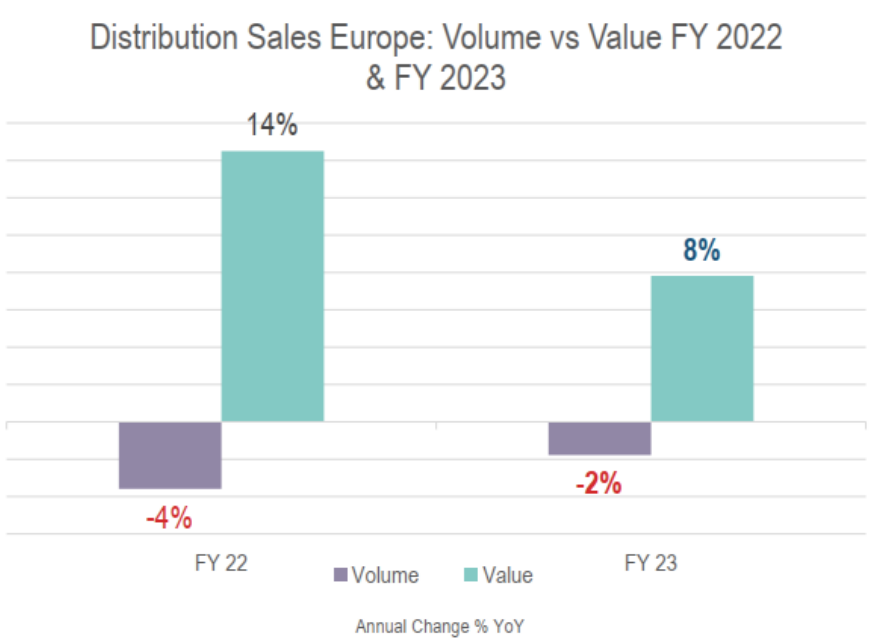
Most volatile year in 20 years

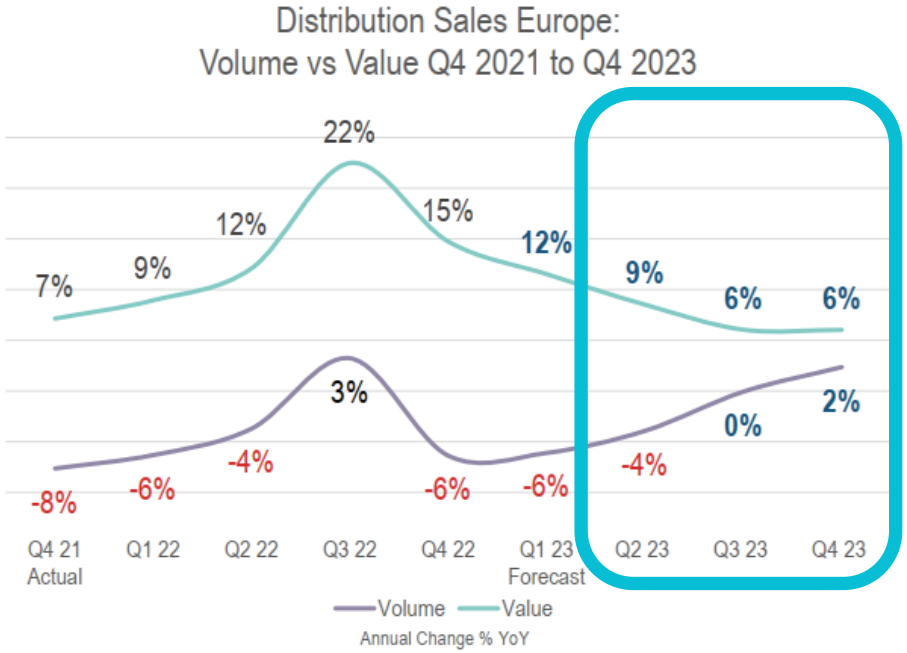
What happened?

Volume vs Value January Forecast

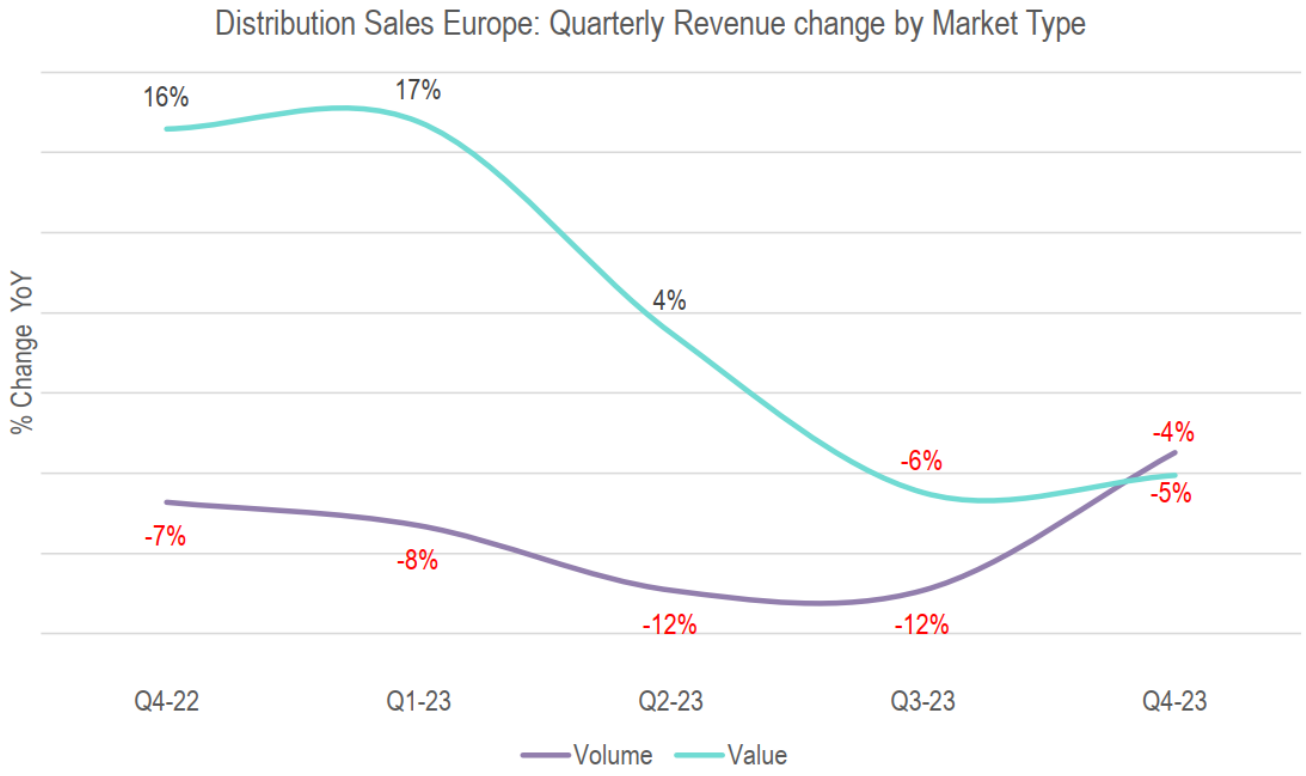
WITH STRONG VALUE GROWTH, AND VOLUME RECOVERS IN H2

CONTEXT





Volume overtakes Value in Q4 2023



CONTEXT

-6%

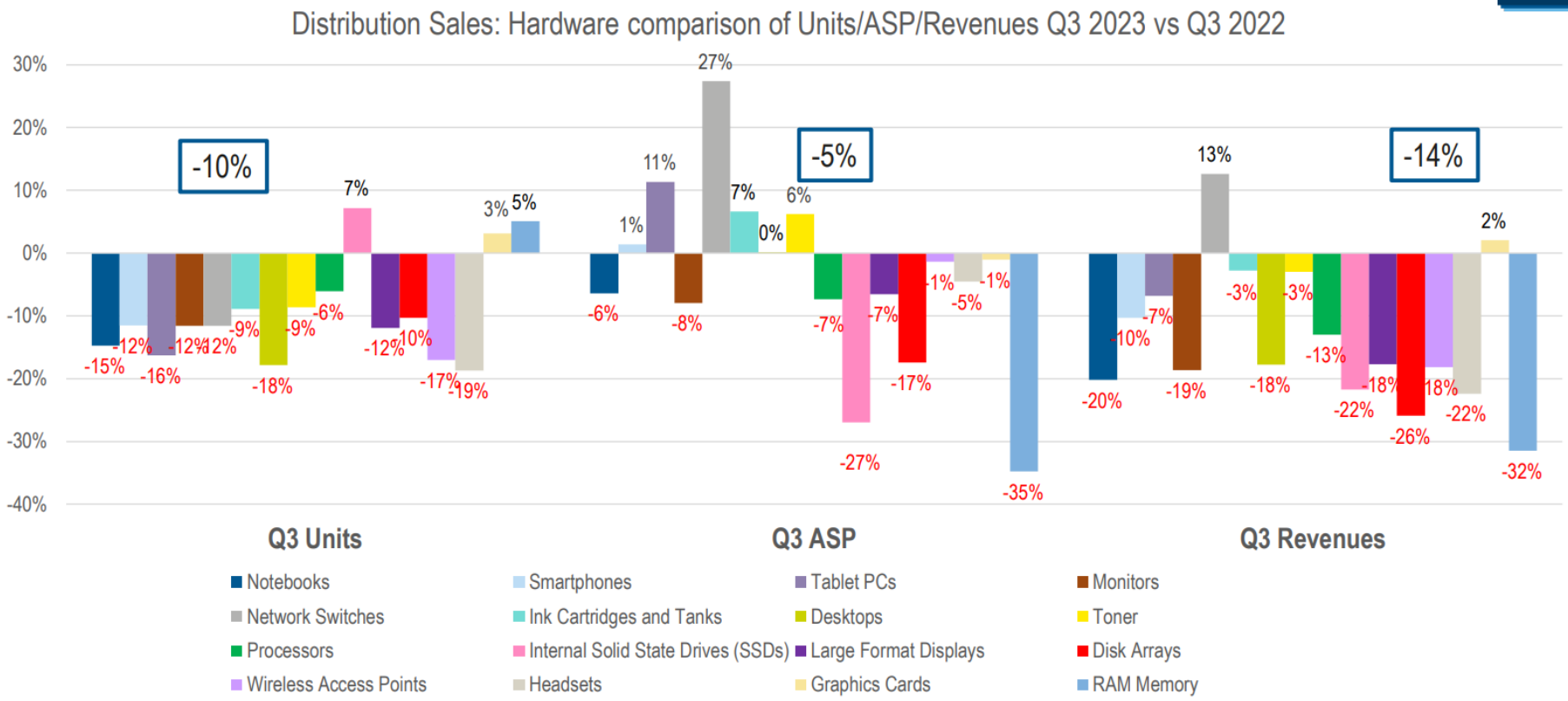
Forecast value "Central Scenario"

-9%

Forecast volume "Central Scenario"

Units decline no longer compensated by ASP increases

ASP CONTINUES TO DECLINE - FROM -1% IN Q2 TO -5%

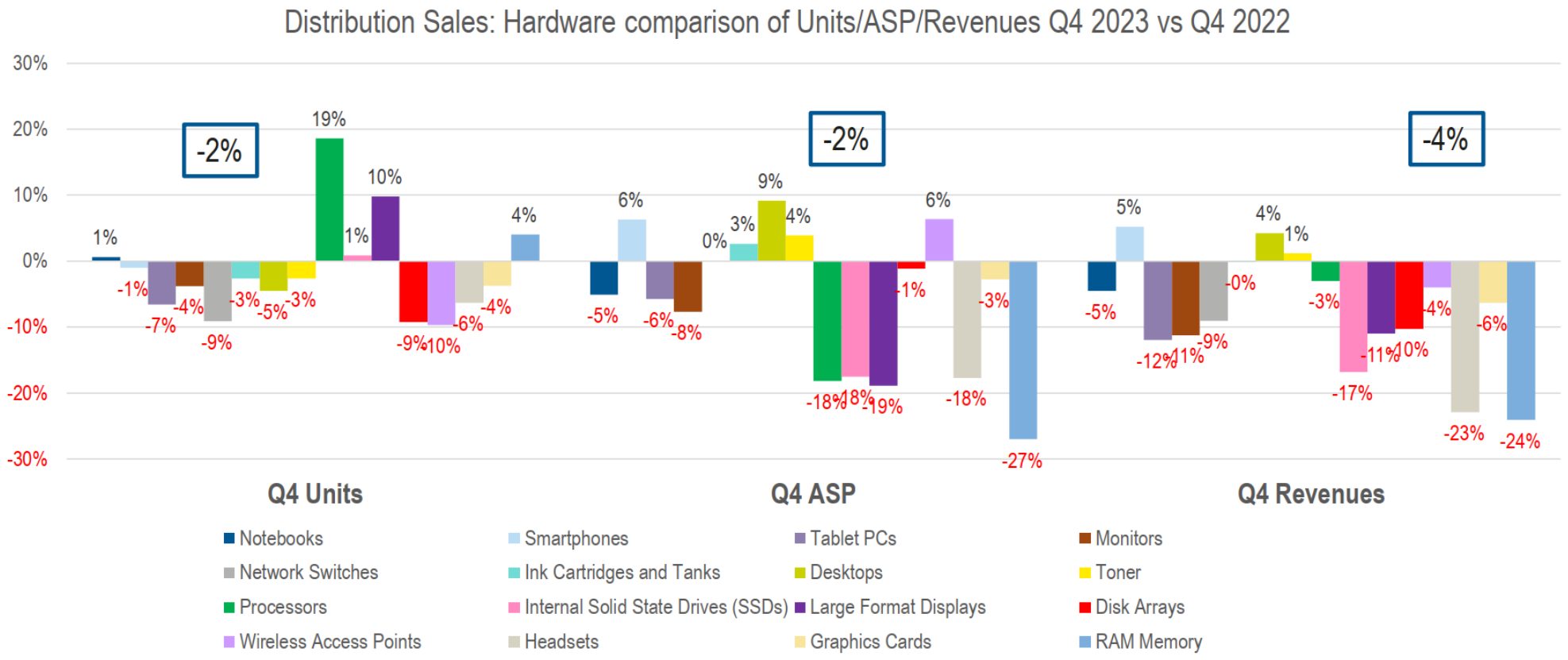


Distribution sales translated at fixed € exchange rate and Panel Europe includes: Austria, Baltics, Belgium, Czech Republic, Denmark, Finland, France, Germany, Italy, Netherlands, Norway, Poland, Portugal, Slovakia, Spain, Sweden, Switzerland and UKI

© 2023 CONTEXT CONFIDENTIAL // Not to be reproduced or disseminated without permission

Finally stabilizing in Q4 2023

PRICE DECREASE SLOWS DOWN

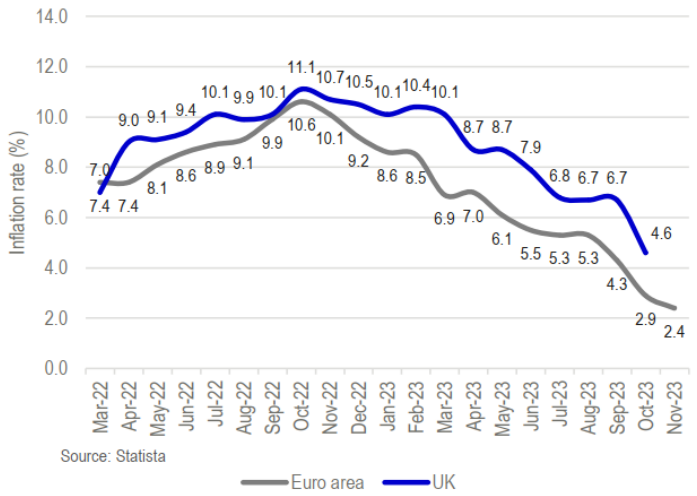


Outlook 2024

Inflation down Interest still there…

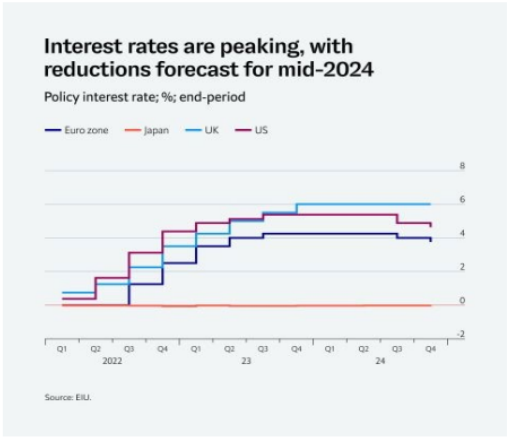
OUTLOOK: INFLATION DOWN, BUT NEAR-TERM GDP IMPACTED BY INTEREST RATES

Inflation rates (%)



Inflation easing but far from reversing. New upside risk: conflict in Middle East

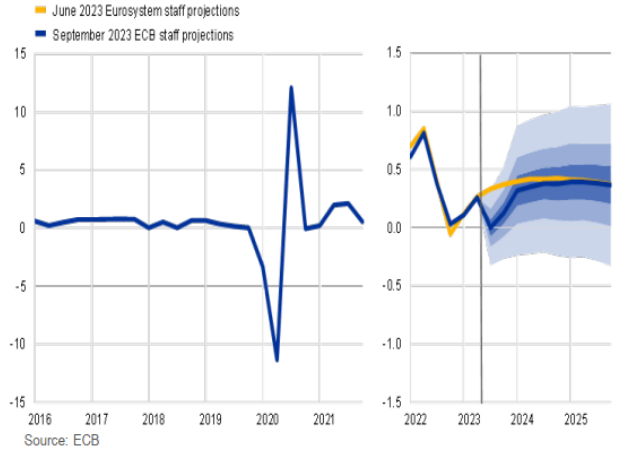
Interest rates (%), current and forecast (EIU projections)



Source: EIU

Monetary tightening likely to have ended, but Central Banks will be cautious on loosening => credits will remain expensive

Euro Area GDP, current and forecast (ECB projections)



Source: ECB

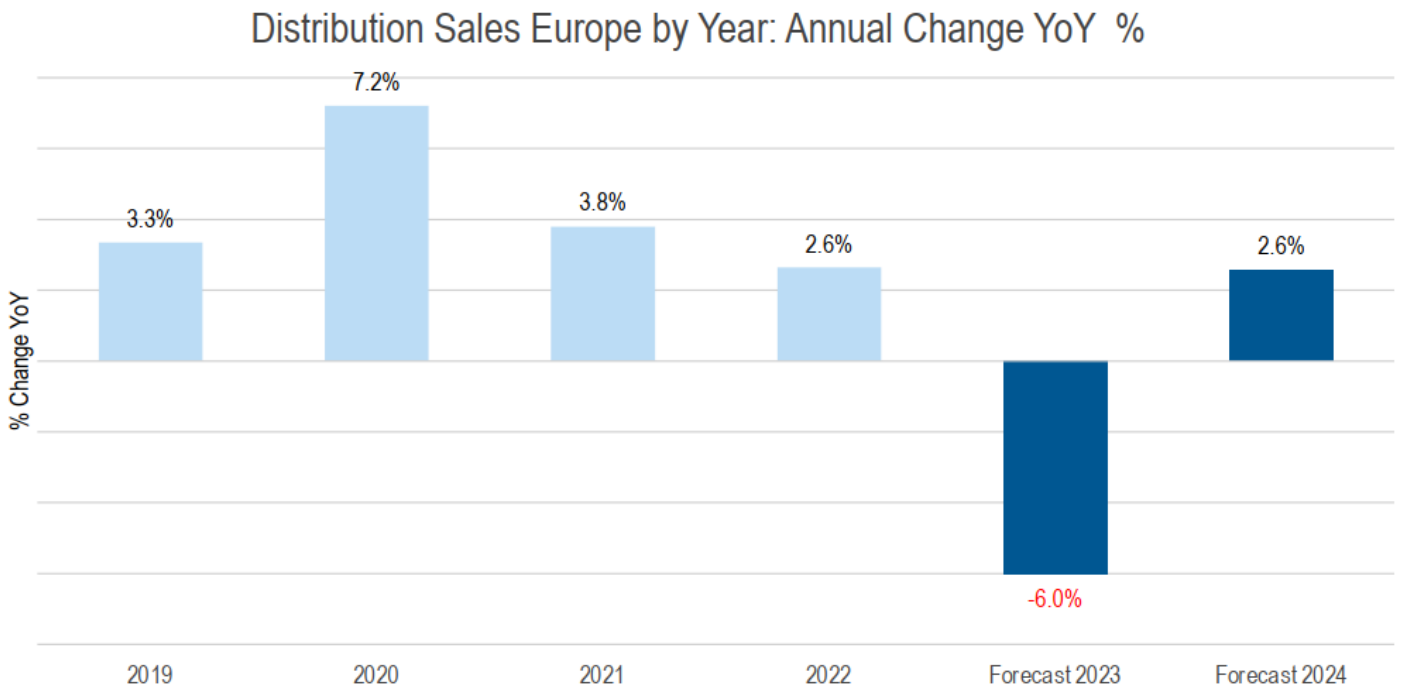
ECB: near-term economic outlook weak (2023-Q4 and 2024 GDP revised down in September), improvements in 2024-H2

Distribution sales translated at fixed € exchange rate and Panel Europe includes: Austria, Baltics, Belgium, Czech Republic, Denmark, Finland, France, Germany, Italy, Netherlands, Norway, Poland, Portugal, Slovakia, Spain, Sweden, Switzerland and UKI

© 2023 CONTEXT CONFIDENTIAL // Not to be reproduced or disseminated without permission

Outlook 2024

WE ARE FORECASTING MODEST GROWTH IN 2024



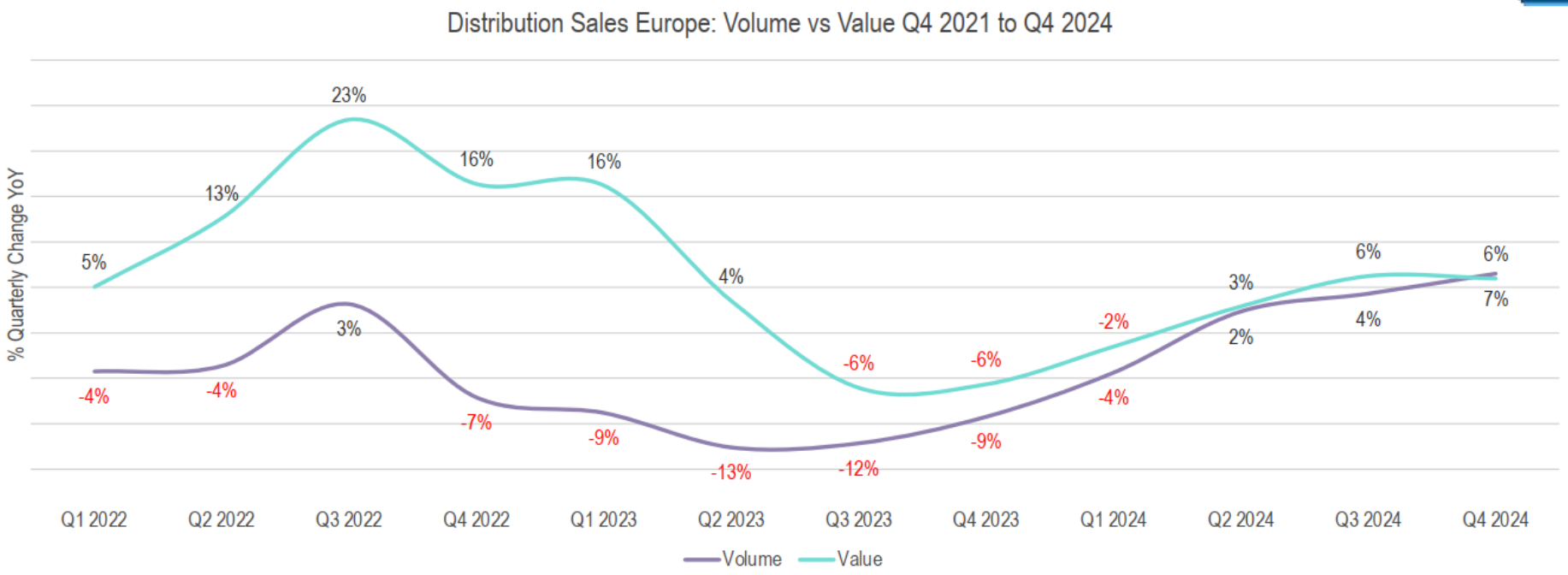
2024 forecast range from 6.5% to -0.5%

Distribution sales translated at fixed € exchange rate and Panel Europe includes:
Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Ireland, Italy, Latvia, Lithuania, Netherlands, Norway, Poland, Portugal, Slovakia, Spain, Sweden, Switzerland, UK.

Source CONTEXT SalesWatch © 2023 CONTEXT CONFIDENTIAL
// Not to be reproduced or disseminated without permission // Data not adjusted for trading days // Revenue based on fixed FX rates

Outlook 2024

GROWTH RATES CONVERGE IN Q2 2024



Distribution sales translated at fixed € exchange rate and Panel Europe includes:
Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Ireland, Italy, Latvia, Lithuania, Netherlands, Norway, Poland, Portugal, Slovakia, Spain, Sweden, Switzerland, UK.

Source CONTEXT SalesWatch © 2023 CONTEXT CONFIDENTIAL
// Not to be reproduced or disseminated without permission // Data not adjusted for trading days // Revenue based on fixed FX rates

canalys

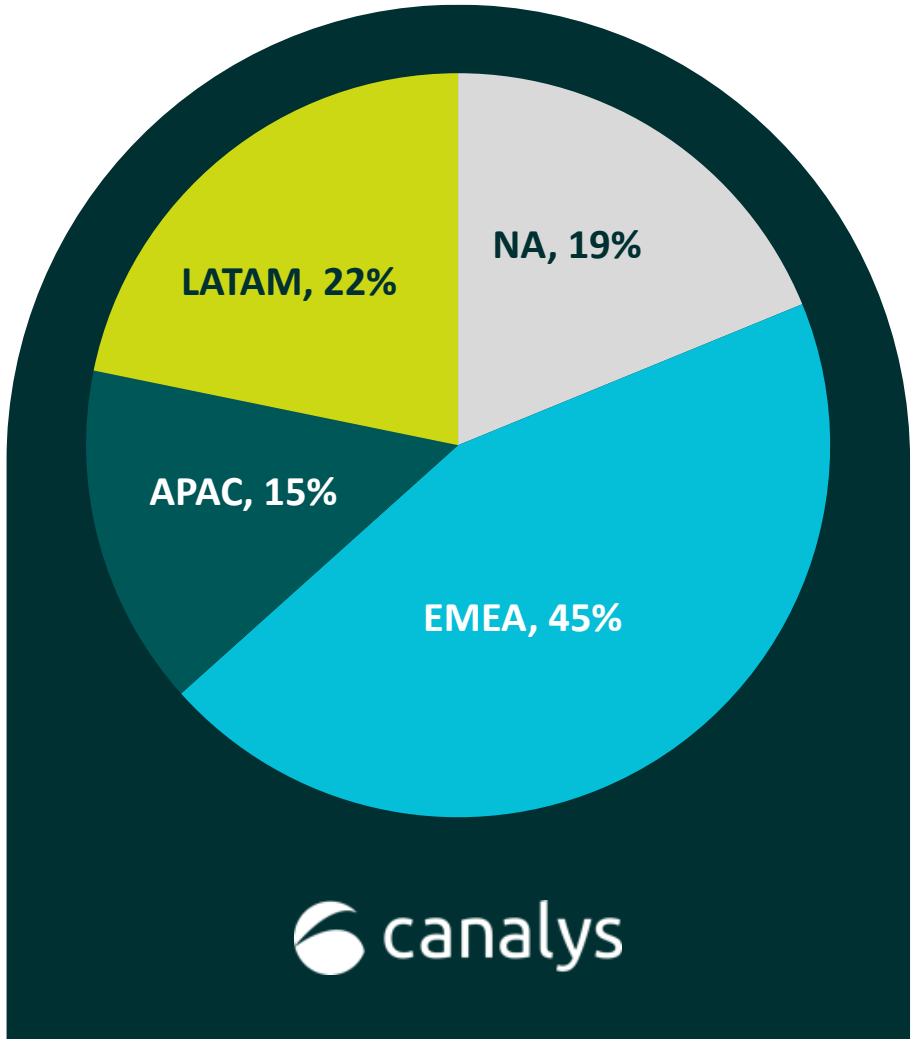
TD SYNNEX technology ecosystem perspectives project results

Prepared for TD SYNNEX

TD SYNNEX survey 2023

Online questionnaire on Canalys' Candefero website. Feedback from 550 business to business channel partners in 60 countries, spanning resellers, systems integrators, service providers, MSPs and distributors.

Respondent breakdown by region



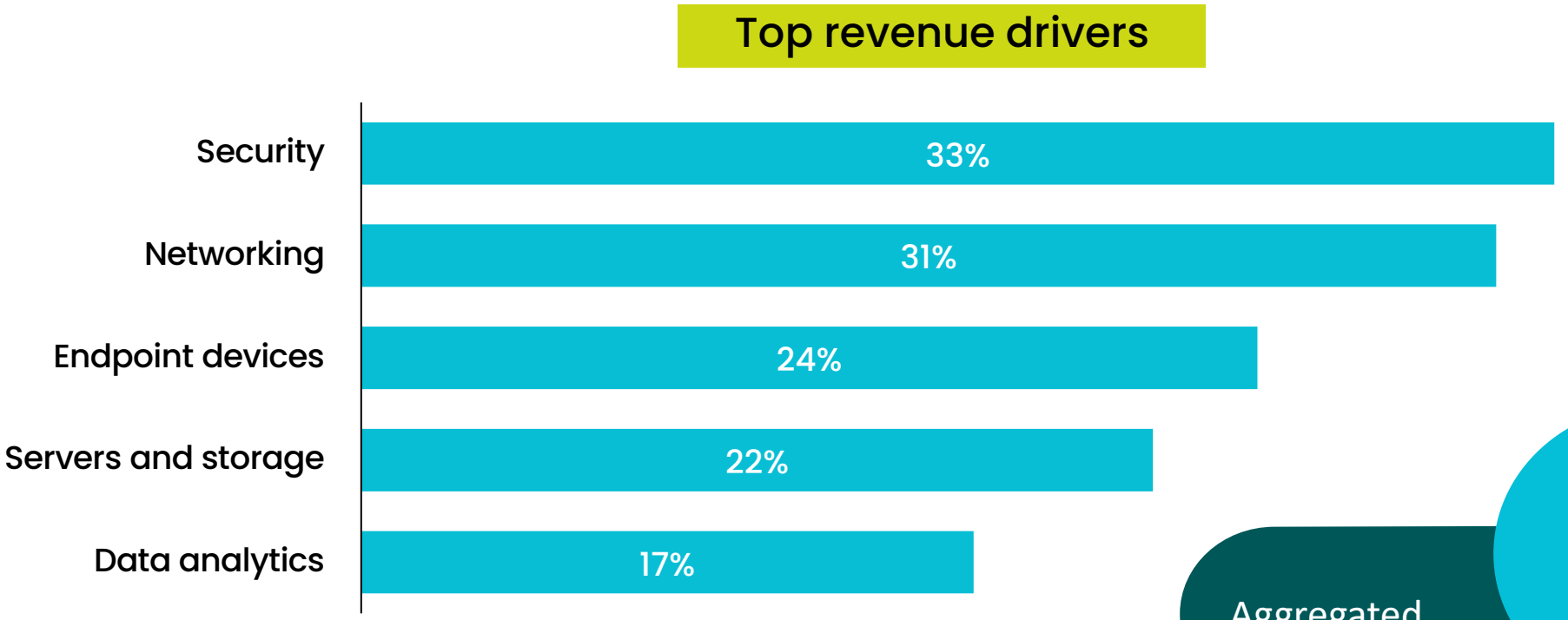
Source: Canalys, Candefero survey, 550 global respondents, May 2023 to July 2023

Insight

What do you sell most?

canalys

Networking, servers & storage important to revenue



Aggregated

Considering your business during the last 12 months, from the list of technologies,

please choose the top three revenue drivers.

Source: Canalys, Candefero TD Synnex survey, 246 EMEA respondents, May – June 2023

canalys

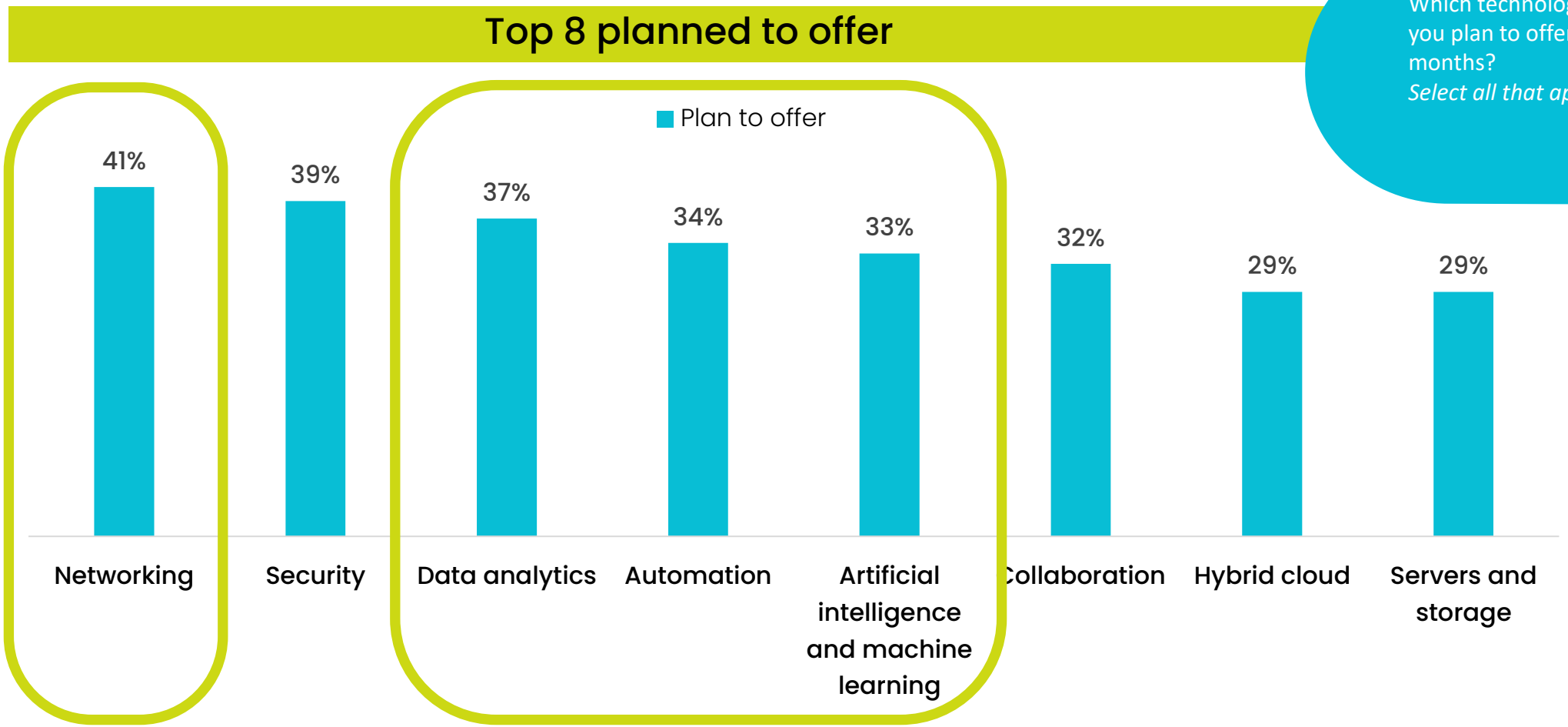
Insight

What do you plan to offer?

canalys

Analytics, AI, automation making an appearance

Which technology solutions do you plan to offer in within 24 months?
Select all that apply.



Source: Canalys, Candefero TD Synnex survey, 246 EMEA respondents, May – June 2023

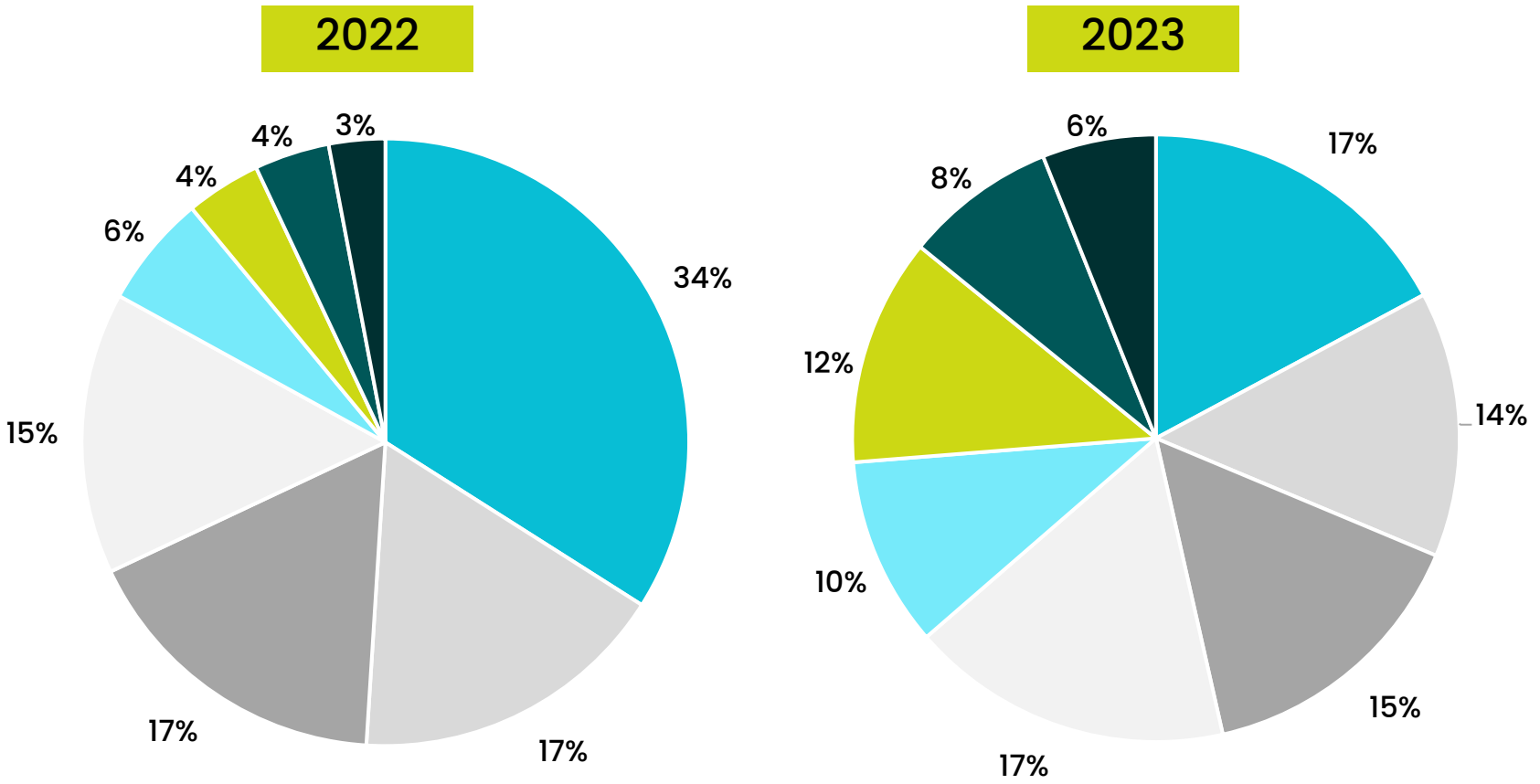
canalys

Insight

How is your portfolio evolving?

canalys

Services take an important share…



What percentage of your business is derived from the following today?

Average percentage across all respondents

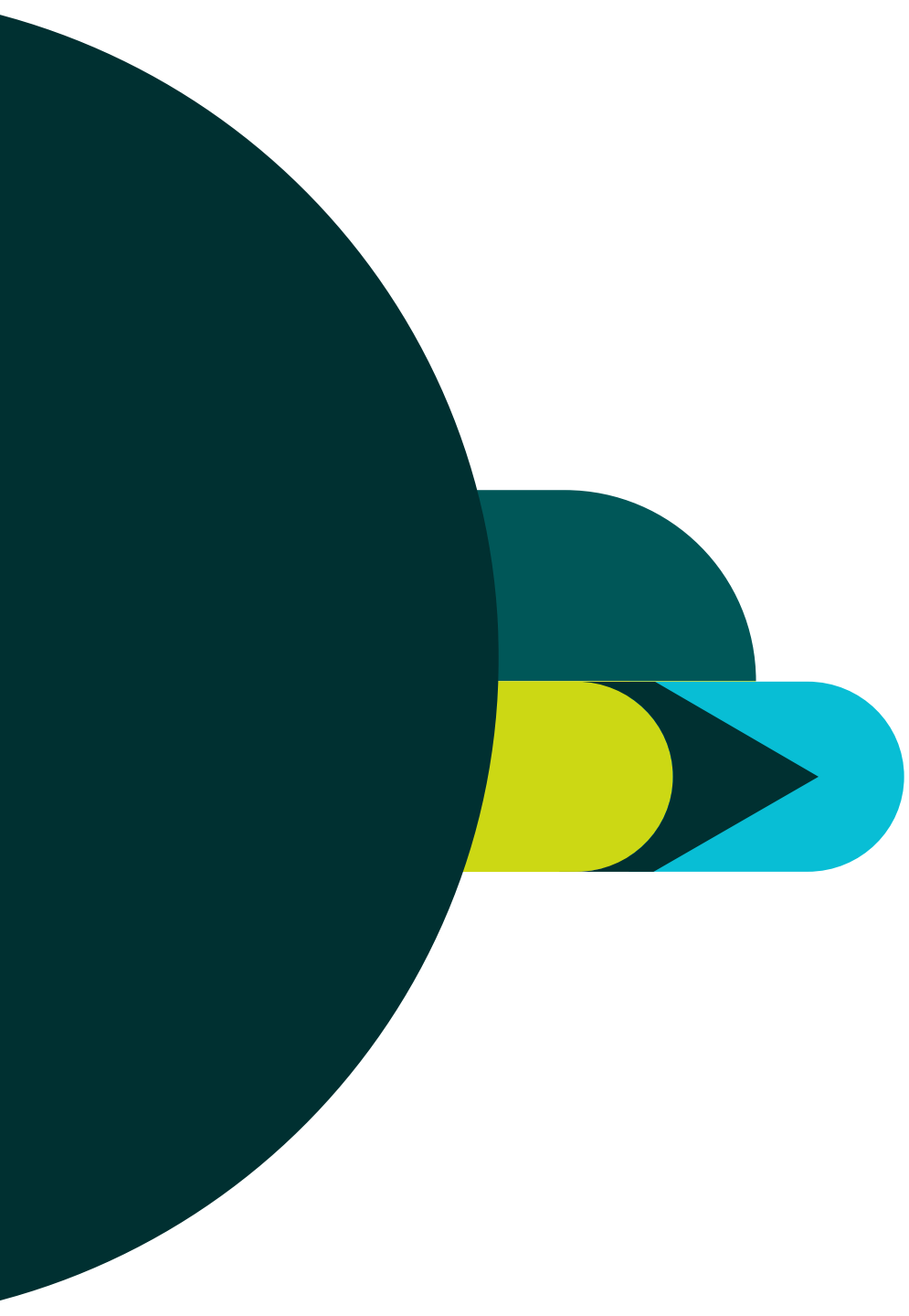
- Resell of hardware
- Resell of software
- Selling managed services
- Selling professional services
- Resell of packaged services
- Selling your own IP
- Selling product lifecycle services
- Selling consumption based XaaS

Source: Canalys, Candefero TD Synnex survey, 246 EMEA respondents, May – June 2023

canalys

You are transforming FAST…

Our ecosystem is changing

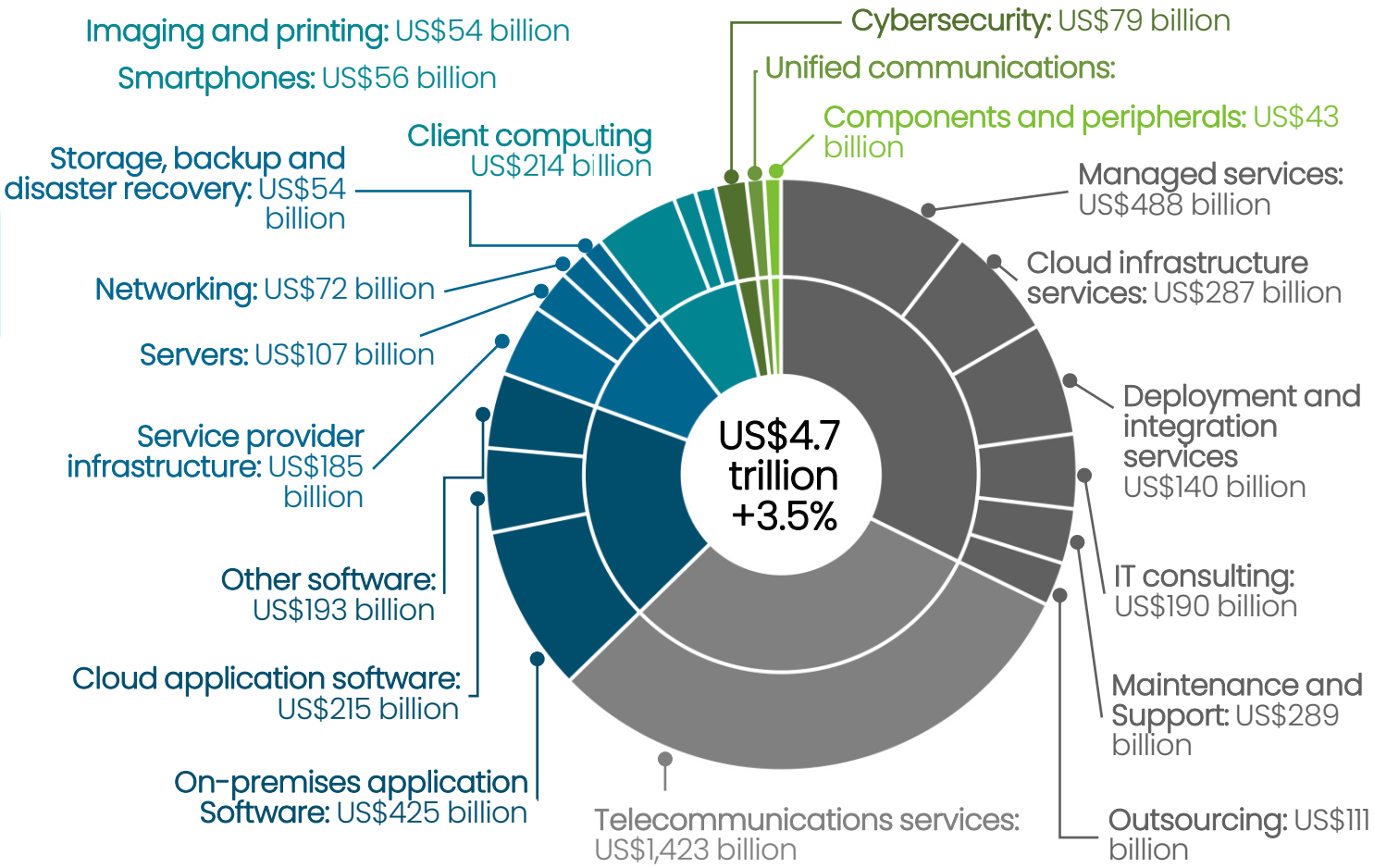


How big is the technology market?

Cybersecurity spending remains a high priority

Worldwide total addressable IT market by category, 2023 forecast

Category	2023 forecast (US$ billion)	Growth
Components and peripherals	43	-7.1%
Unified communications	45	2.6%
Cybersecurity	79	11.1%
Client devices, imaging and printing	324	-2.8%
Infrastructure	417	-0.1%
Software	833	5.5%
Telecommunications services	1,423	0.9%
IT services	1,506	7.5%
Total IT spend	**4,670**	**3.5%**



Source: Canalys estimates, Channels Analysis, July 2023 (excluding consumer IT spending)

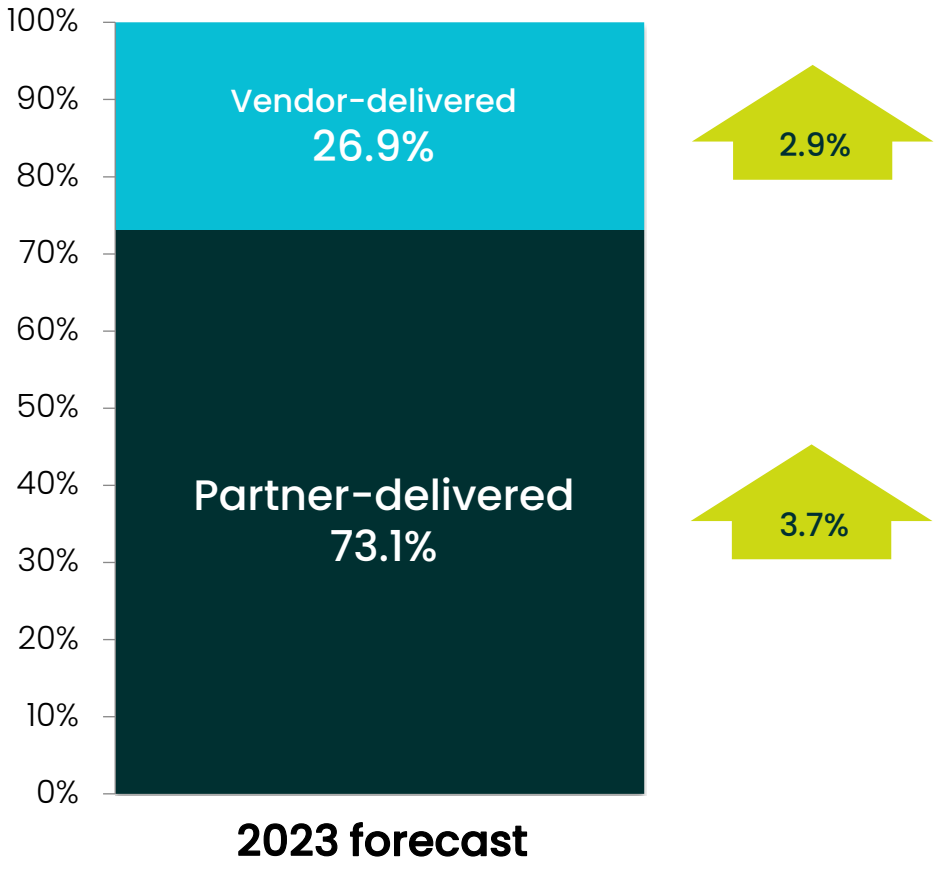
TD SYNNEX

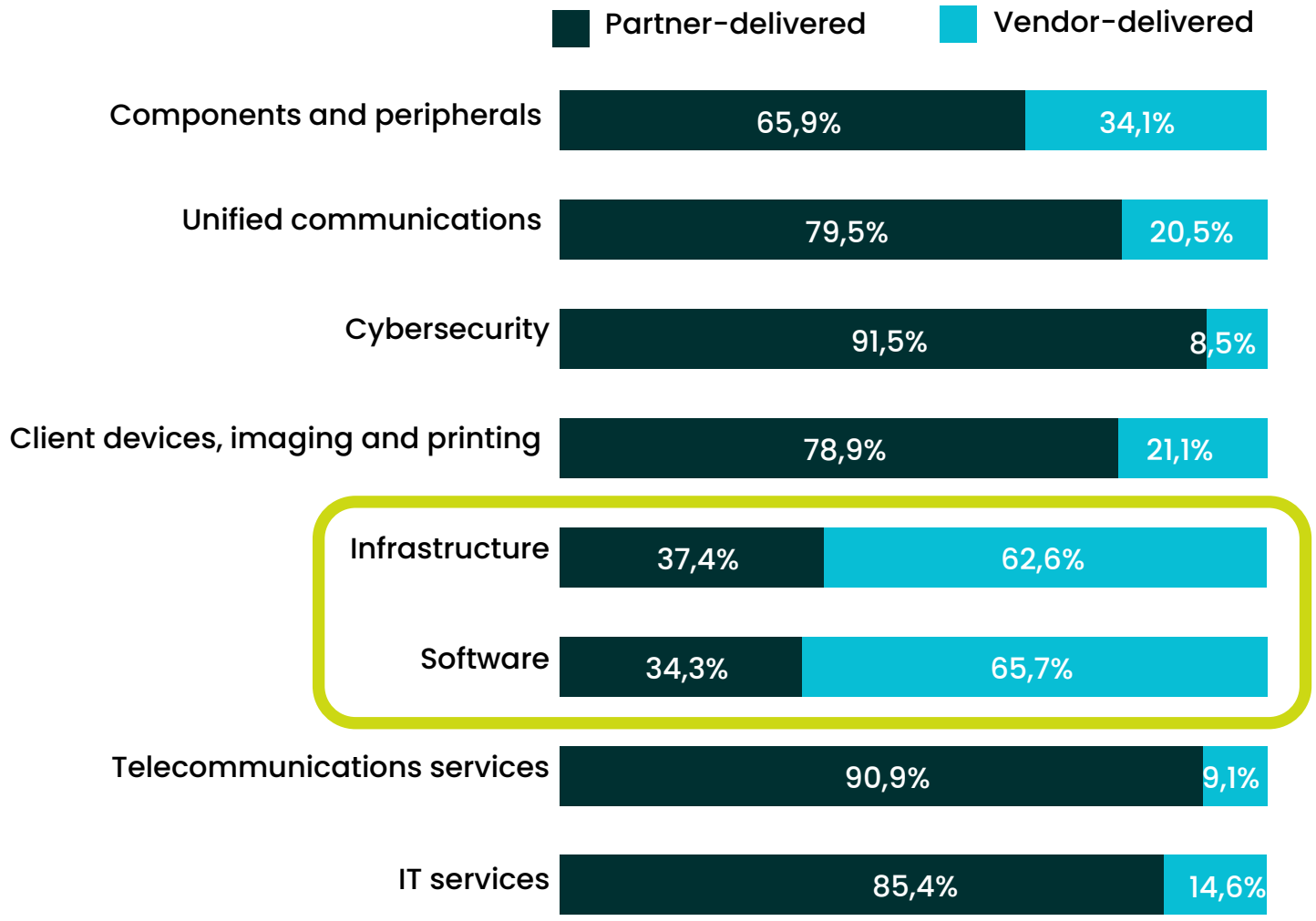
canalys

Channel growth to outpace direct vendor sales

Worldwide total addressable IT market by route to market, 2023 forecast

Total IT spend: US$4.7 trillion
Growth: 3.5%



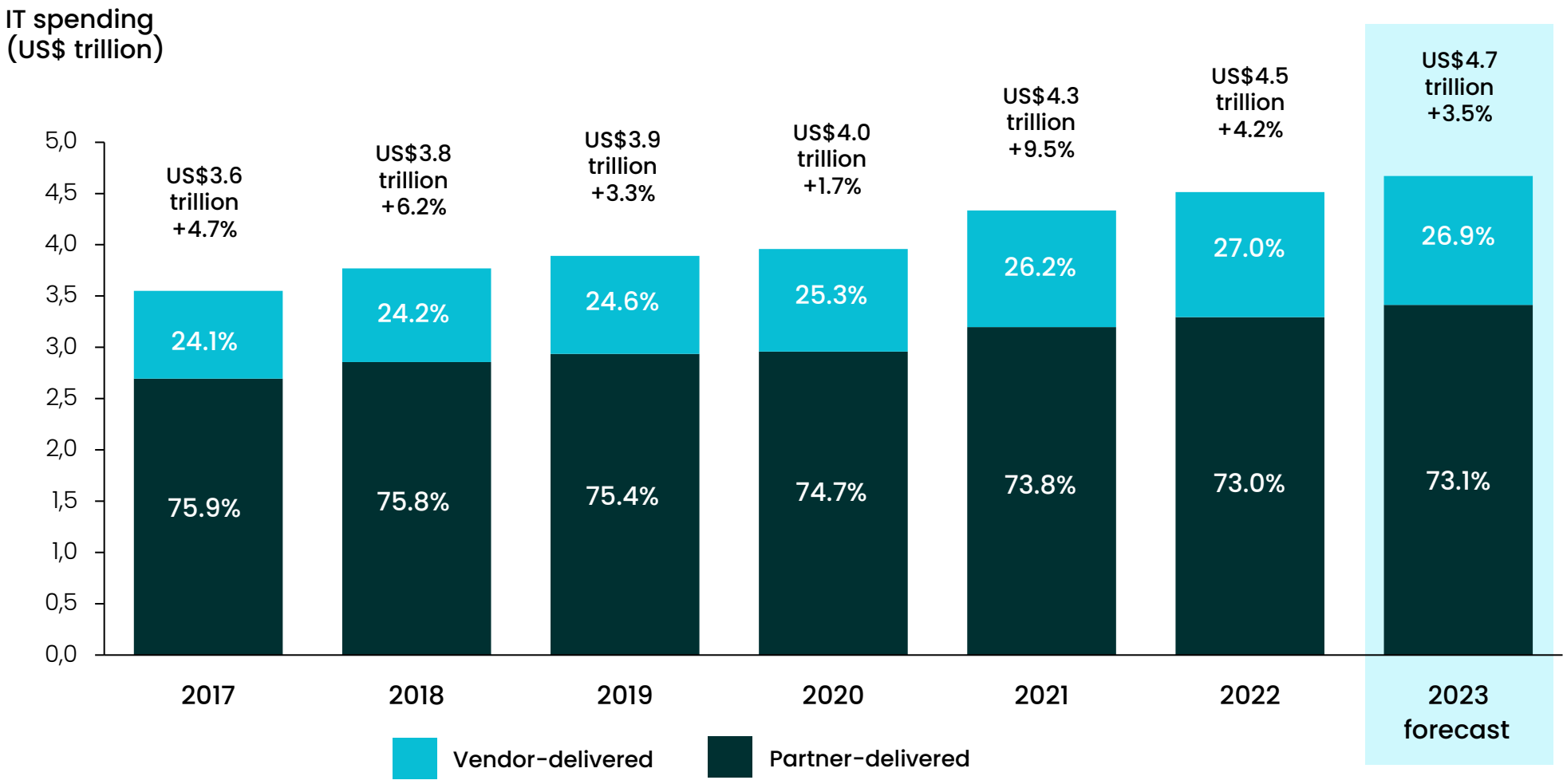


Source: Canalys estimates, Channels Analysis, July 2023 (excluding consumer IT spending)

canalys

The channel remains vital

Worldwide total addressable IT market forecast by route to market and by year



Source: Canalys estimates, Channels Analysis, July 2023 (excluding consumer IT spending)

canalys

NEW ROLES
in the ecosystem

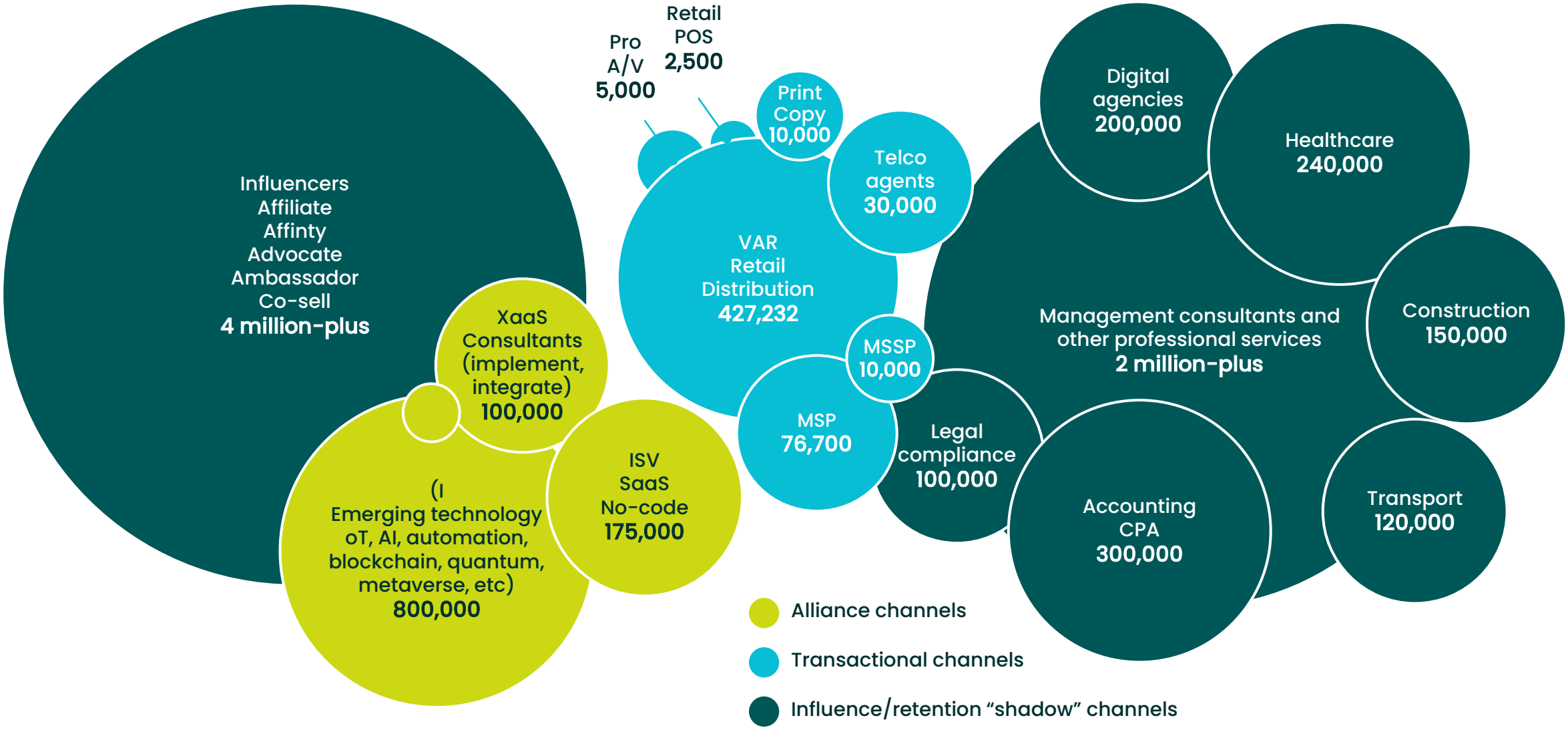
Non-transactional partners are becoming important

Alliances: technology, strategic and business

Source: Canalys take, June 2022

canalys

The new channels ecosystem is vast



Source: Canalys estimates, June 2022

canalys

FUTURE-PROOF

Leadership

What is expected from leaders?

Delivering results

Cope with accelerating change

Cope with several generations

Manage hybrid working

ESG specialist

Corporate Social Responsibility

Environmental

- Lowering our global carbon footprint
- Setting targets for emission reductions
- Accelerating our sustainability initiatives
- Supporting our customers and vendors with circular economy and sustainable product choices

Social

- Recognized as a great place to work
- A leader in the promotion and practice of diversity, equity and inclusion
- An active member of the local communities where we live and work

Governance

Strong corporate governance based on best practices, local requirements, and the needs of our co-workers, customers, vendors and investors

Foster DEI

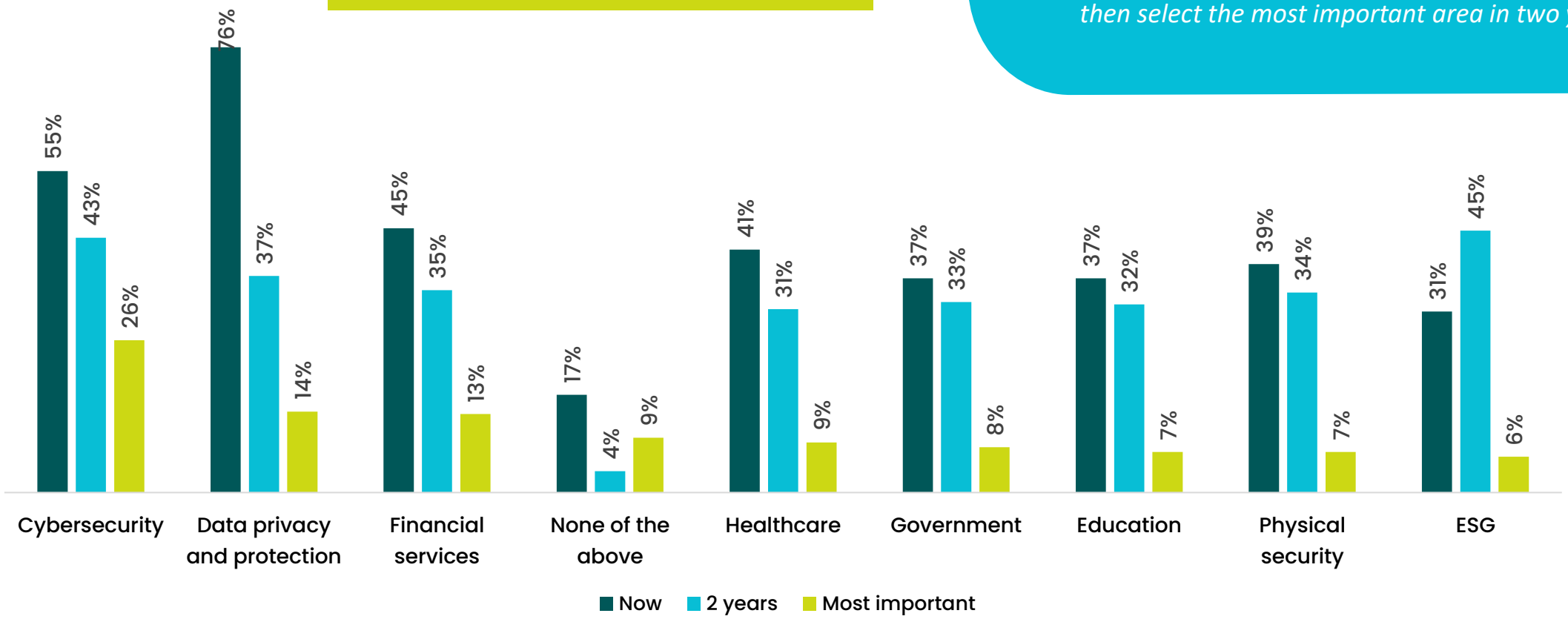
Go woke … Go broke

Make
no mistakes

ESG to jump in importance in the next two years

Ranked on most important

Which areas of regulatory expertise or certification are most important to your business today? *Please choose all that apply today and in two years time and then select the most important area in two years time.*



Source: Canalys, Candefero TD Synnex survey, 246 EMEA respondents, May – June 2023

canalys

IQ – EQ

AQ

RQ

Leadership in a volatile world

Havard Business Review

Article by Francesca Gino and Bradley Staats

the agreeable challenger

agreeable & challenger

Contradictory Qualities

Agreeableness

Collaborative, empathetic, build strong relationship with others, good listeners, value different perspectives , willing to compromise

Challenging

push back on status quo, ask tough questions, hold people accountable on high standards, not afraid to rock the boat, willing to take risks to achieve ambitious goals

agreeable & challenger

Skill to effectively balance both

Some examples

Mary Barra CEO of General Motors

- Building strong relationships
- Collaborate with others
- Tough negotiator
- Makes difficult decisions, e.g. costly recall of millions of cars

Satya Nadella CEO of Microsoft

- Empathetic leadership style, collaborative
- Challenging the status quo
- Makes tough decisions e.g. Shift from personal computers to cloud computing

Some examples

Michele Obama former first lady of US

- Using her platforms to advocate for education, health and women rights
- Fosters partnerships and collaboration
- Challenges societal norms

Justin Trudeau Prime Minister Canada

- Known for diplomatic approach
- Focus on building consensus
- Tackled complex issues like Climate Change and indigenous rights

Agreeable
challenging

Merci !

Patrick Steenssens

p.steenssens@tdsynnex.com

+32 486 439 474

11:10 – 11:20 Attracting Women to Tech

11:20 – 12:00 Respect: The Key to Empowerment

12:00 – 13:00 Lunch

13:00 – 14:00 Keynote: Future-Proofing your Company

14:00 – 15:00 ***Decoding NIS2***

15:00 – 15:30 Break

15:30 – 16:30 Insights from CompTIA Community UK&I / Ask The Experts on NIS2

WE ARE THE

CompTIA®

COMMUNITY

Mario Casier

Copaco

NIS2 for MSPs

8 February 2024

Mario Casier – BU Manager Cybersecurity

Agenda

- Cyberattack trends 2023
- 6 Fundamentals of Cyberhygiene can stop 99% of attacks
- Why NIS2?
- MSP key role in NIS2 & What to do NOW?

FACTS & FIGURES

1984 Private enterprise	475 Employees	8,000 Partners
220 Brands	50,000 m^2 Warehouse	Top 3 Line
€1.33 billion Turnover (FY2023)	COPACO .COM COPACO CLOUD COPACO SERVICES	


Acronis


COPACO
SERVICES


DELL
Technologies


WatchGuard™


Microsoft


ZYXEL


SONICWALL™


Parallels
Awingu


JIMBER


COPACO

The Cybersecurity perimeter has changed...

Global cyberattacks spiked by 40 to 45% in 2023

70% of successful attacks are against organizations with **<500 employees**

Hactivism (mainly DDoS) is growing strongly, mainly related to **geopolitical tensions**.
Over 75% of eligible citizens living in democratic nations **within the next year and a half will have the opportunity to vote.**

Password based **attacks spiked in 2023**. 81% of breaches leverage stolen or weak passwords.

IoT Malware increases +37%
Of the 78% of IoT devices with known vulnerabilities, **46% cannot be patched.**

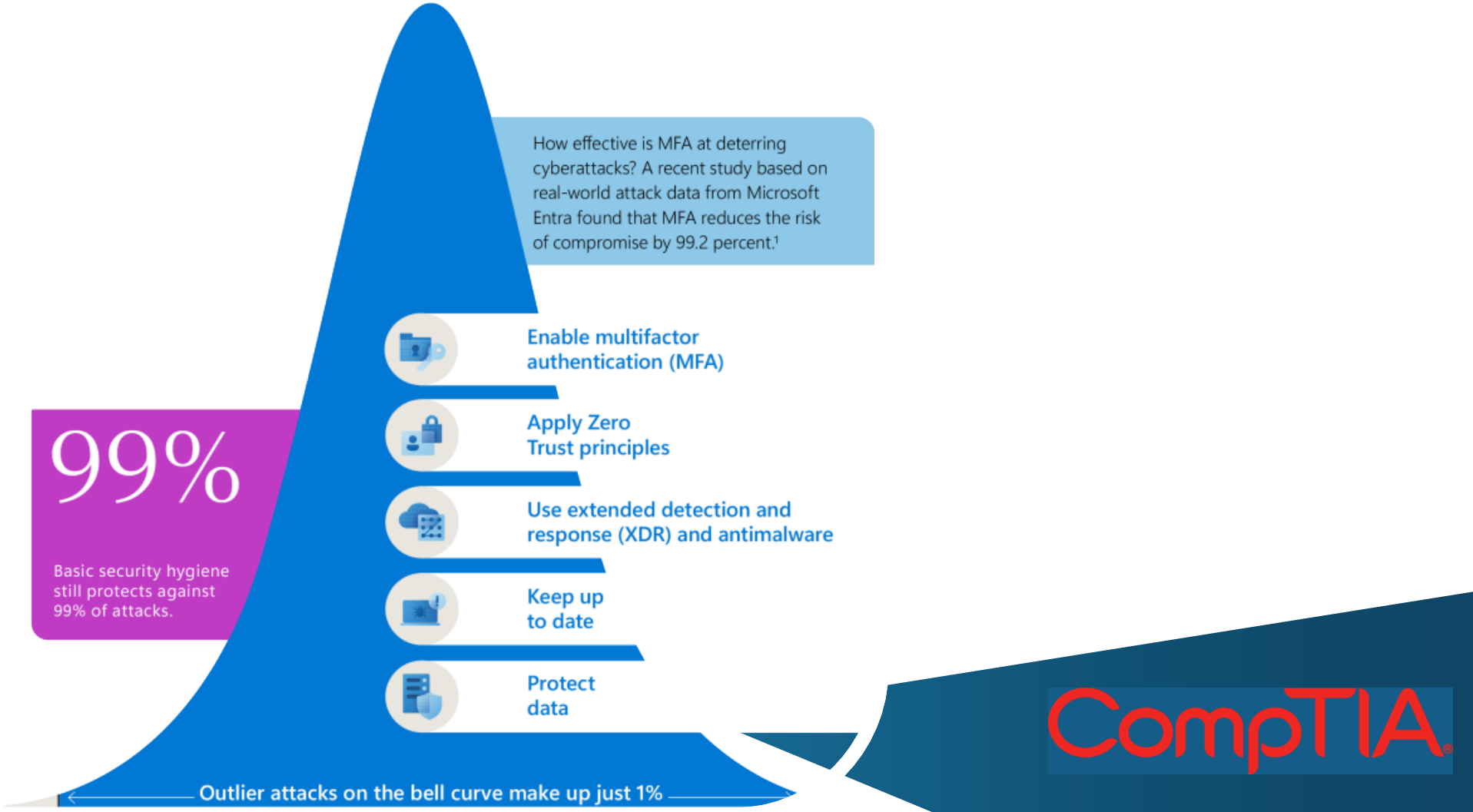
(source Microsoft Defense report '23)

Alle slachtoffers België en Nederland blootgesteld op darkweb

Slachtoffer	Cybercriminelen	Website	Land	Sector	Publicatie datum darkweb ↑
ese.com	LockBit	ese.com	Netherlands	Miscellaneous Services	29-jan-24
ANS COMPUTER	BlackCat (ALPHV)	anscomputer.be	Belgium	IT Services	22-jan-24
deknudtframes.be	Cuba	deknudtframes.be	Belgium	Furniture	22-jan-24
Home Waremmien	LockBit	home-waremmien.be	Belgium	Housing sector	21-jan-24
DENHAM the Jeanmaker	Akira	www.denham.com	Netherlands	Apparel And Accessory Stores	17-jan-24
Limburg	Medusa	www.limburg.net	Belgium	Electric, Gas, And Sanitary Services	11-jan-24
krijnen.be	LockBit	krijnen.be	Belgium	Furniture	29-dec-23
walkro.eu	LockBit	walkro.eu	Netherlands	Chemical Producers	25-dec-23
Succes Schoonmaak	PLAY	www.successchoonmaak.nl	Netherlands	Miscellaneous Services	18-dec-23
Soethoudt metaalbewerking b.v.	8BASE	soethoudt.nl	Netherlands	Fabricated Metal Products	13-dec-23
igt.nl	LockBit	igt.nl	Netherlands	Publishing, printing	11-dec-23
Vitro Plus	PLAY	www.vitroplus.nl	Netherlands	Research Services	7-dec-23
skalar.com	Medusa Locker	skalar.com	Netherlands	Machinery, Computer Equipment	5-dec-23
fps.com	BLACK SUIT	fps.com	Netherlands	Miscellaneous Manufacturing	4-dec-23

Source: https://www.ccinfo.nl/actuele-aanvallen/alle-slachtoffers-belgie-en-nederland-blootgesteld-op-darkweb

6 Fundamentals of Cyberhygiene can stop 99% of attacks!

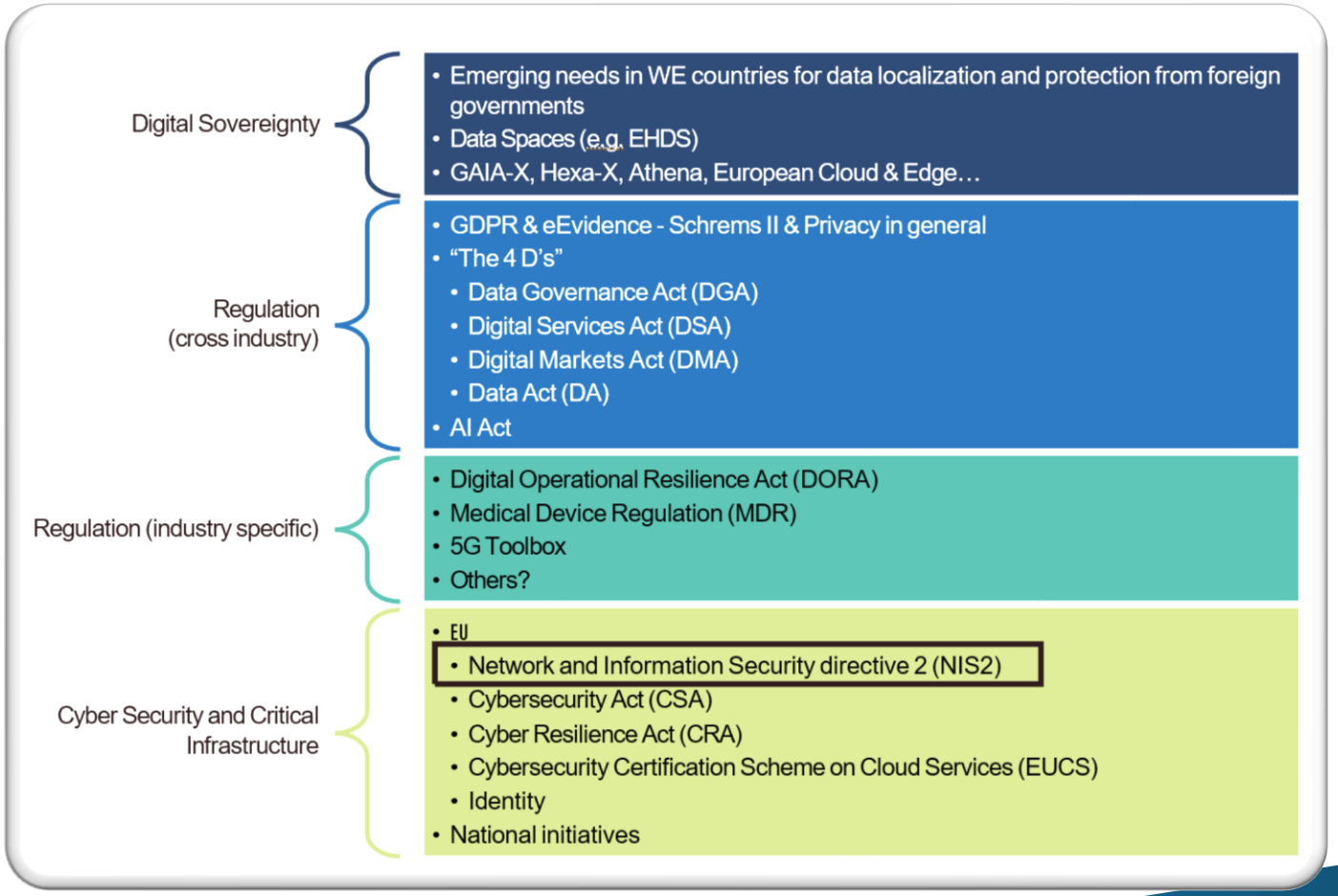


(source Microsoft Defense report '23)

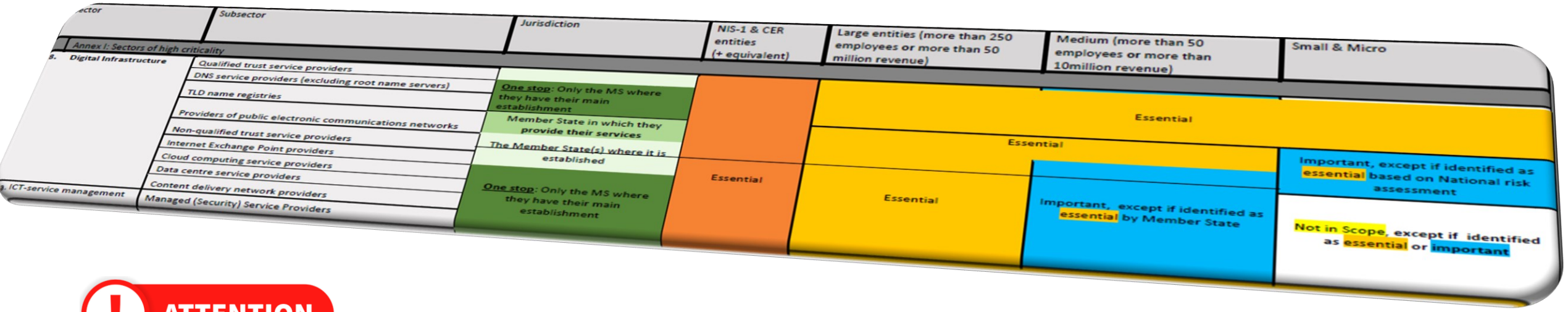
Securing our future together

> Defenders are being driven to innovate and collaborate more closely than ever.

The evolving Policy Landscape in Western Europe



MSPs: key role in NIS2



Sector	Subsector	Jurisdiction	NIS-1 & CER entities (+ equivalent)	Large entities (more than 250 employees or more than 50 million revenue)	Medium (more than 50 employees or more than 10million revenue)	Small & Micro
Annex I: Sectors of high criticality						
8. Digital Infrastructure	Qualified trust service providers	One stop: Only the MS where they have their main establishment		Essential		
	DNS service providers (excluding root name servers)					
	TLD name registries					
	Providers of public electronic communications networks	Member State in which they provide their services				
	Non-qualified trust service providers	The Member State(s) where it is established		Essential		
	Internet Exchange Point providers					
	Cloud computing service providers	One stop: Only the MS where they have their main establishment	Essential	Essential	Important, except if identified as essential by Member State	Important, except if identified as essential based on National risk assessment
	Data centre service providers					
	Content delivery network providers					Not in Scope, except if identified as essential or important
9. ICT-service management	Managed (Security) Service Providers					

ATTENTION

Supply chain security:

"Essential and important entities should therefore assess and consider the overall quality and resilience of products and services, the cybersecurity risk management measures contained therein, and the cybersecurity practices of their suppliers and service providers, including their secure development procedures. In particular, ***essential and important entities should be encouraged to include cybersecurity risk management measures in contractual arrangements with their direct suppliers and service providers.*** *Those entities may also consider risks arising from the activities of suppliers and service providers at another level."*

CompTIA

What to do NOW as MSP?

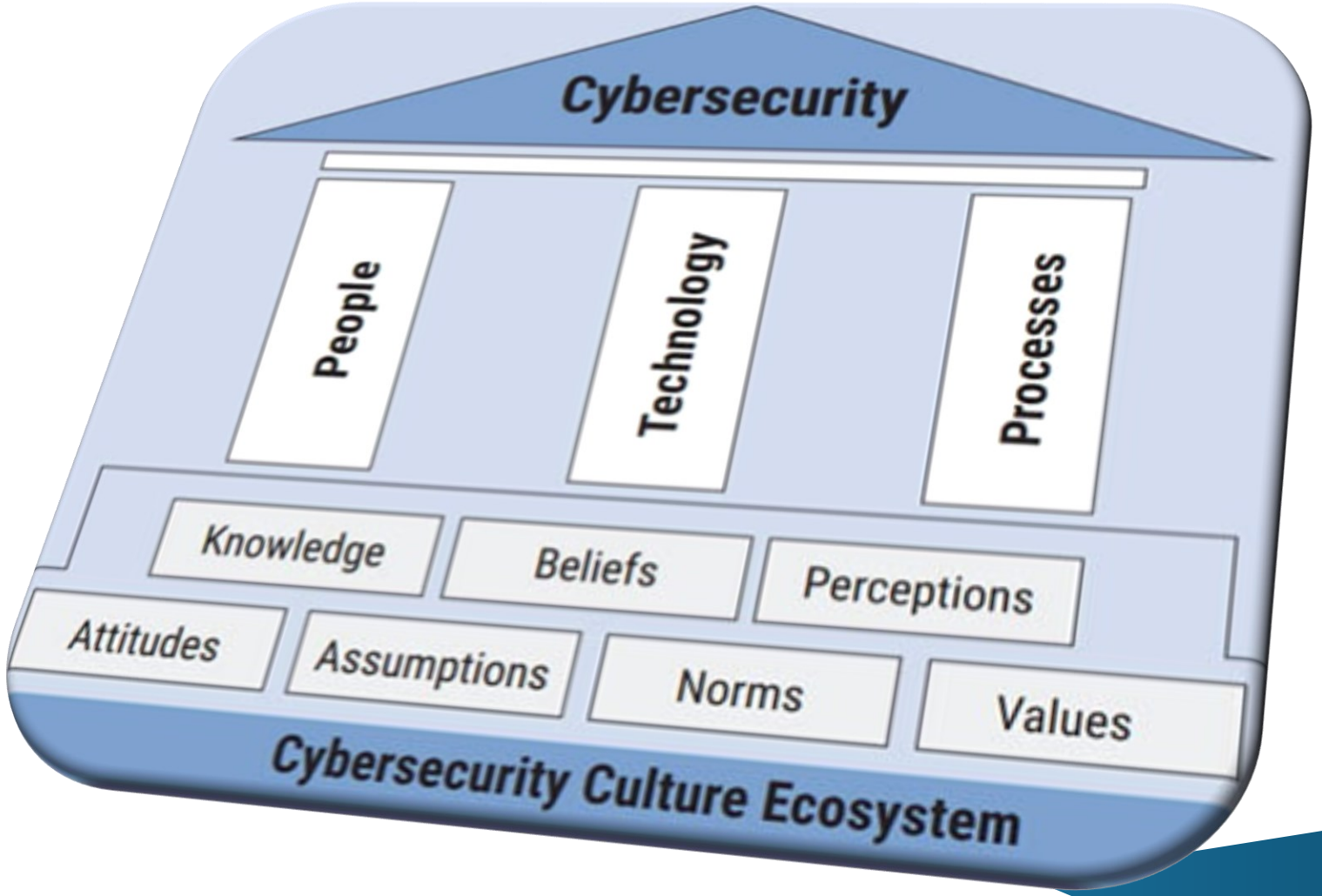
ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

CENTRE FOR CYBERSECURITY BELGIUM

MSP plays a key role, but…


“Our Cybersecurity is handled by IT”
IT
Wrong
We all need to be aware

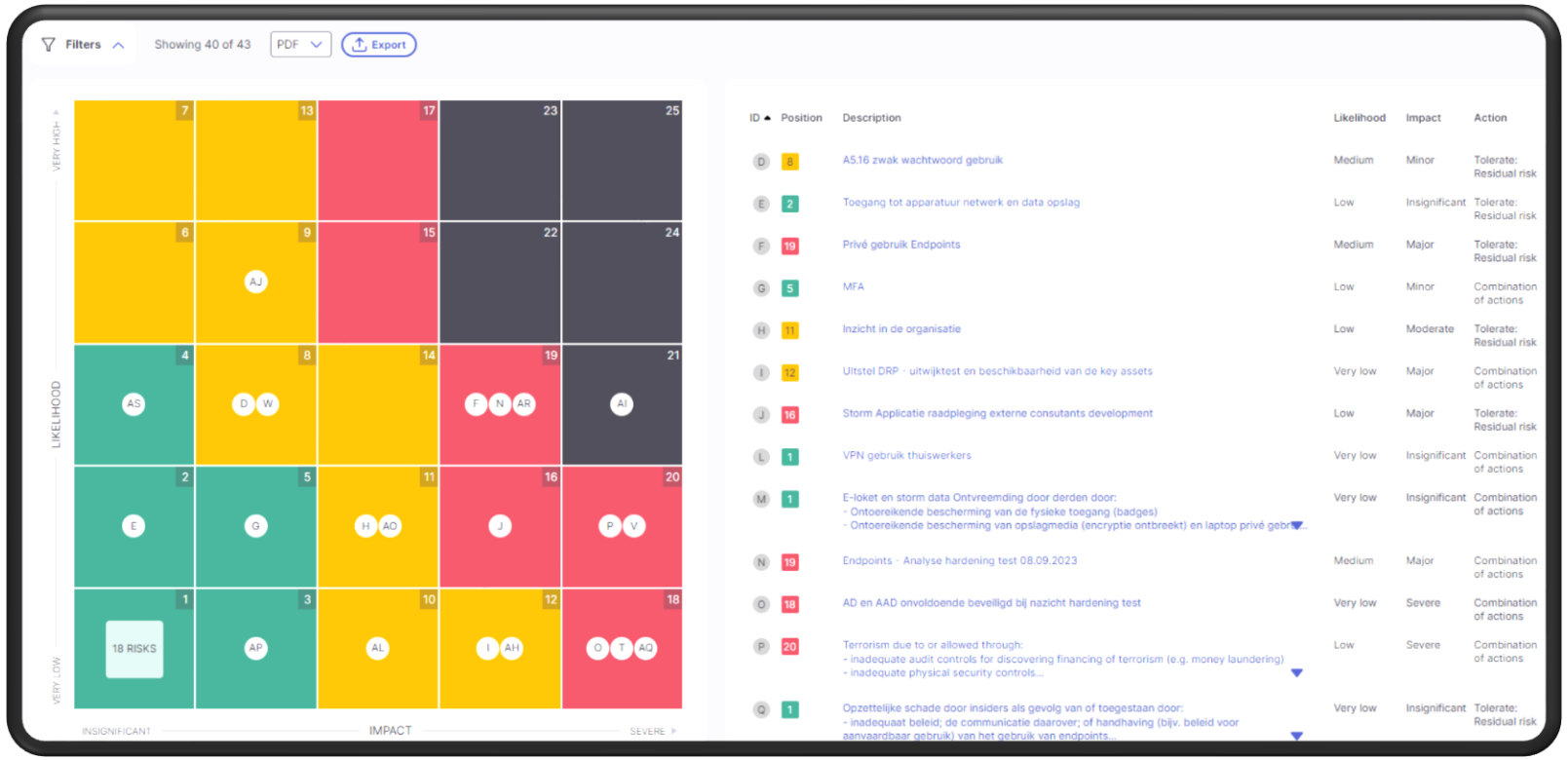
Cybersecurity strategy is mainly about 3 things …



… With a Cybersecurity framework

Stage	Process	People	Technology
Identify risks, assets, sensitive data ('crown jewels')…	*Risk analysis*		
Protect Digital assets & infrastructure			
Detect events & incidents			
React to incidents			
Recover after cyberincident			

Risk analysis from theory to practice



QFIRST
ISMS & NIS2 Certification Framework

CompTIA

NIST Cybersecurity framework

Stage	Process	People	Technology
Identify risks, assets, sensitive data ('crown jewels')...	*Risk analysis* *Regular testing BCM*	*Zero trust mindset*	*Endpoint management* *Pentesting …*
Protect Digital assets & infrastructure	*ISMS*	*User awareness training*	*MFA* *ZTNA* *Firewalls …*
Detect events & incidents	*Firewall policies* *Incident handling policies*	*Apply awareness training*	*SIEM, XDR* *Antivirus* *Digital minefield*
React to incidents	*Start BCM procedure*	*Increased attention logging*	*XDR* *SOAR*
Recover after cyberincident	*Cyberinsurance* *Apply BCM policies*	*Who's doing what*	*Restore backup* *DRP*

“No budget”

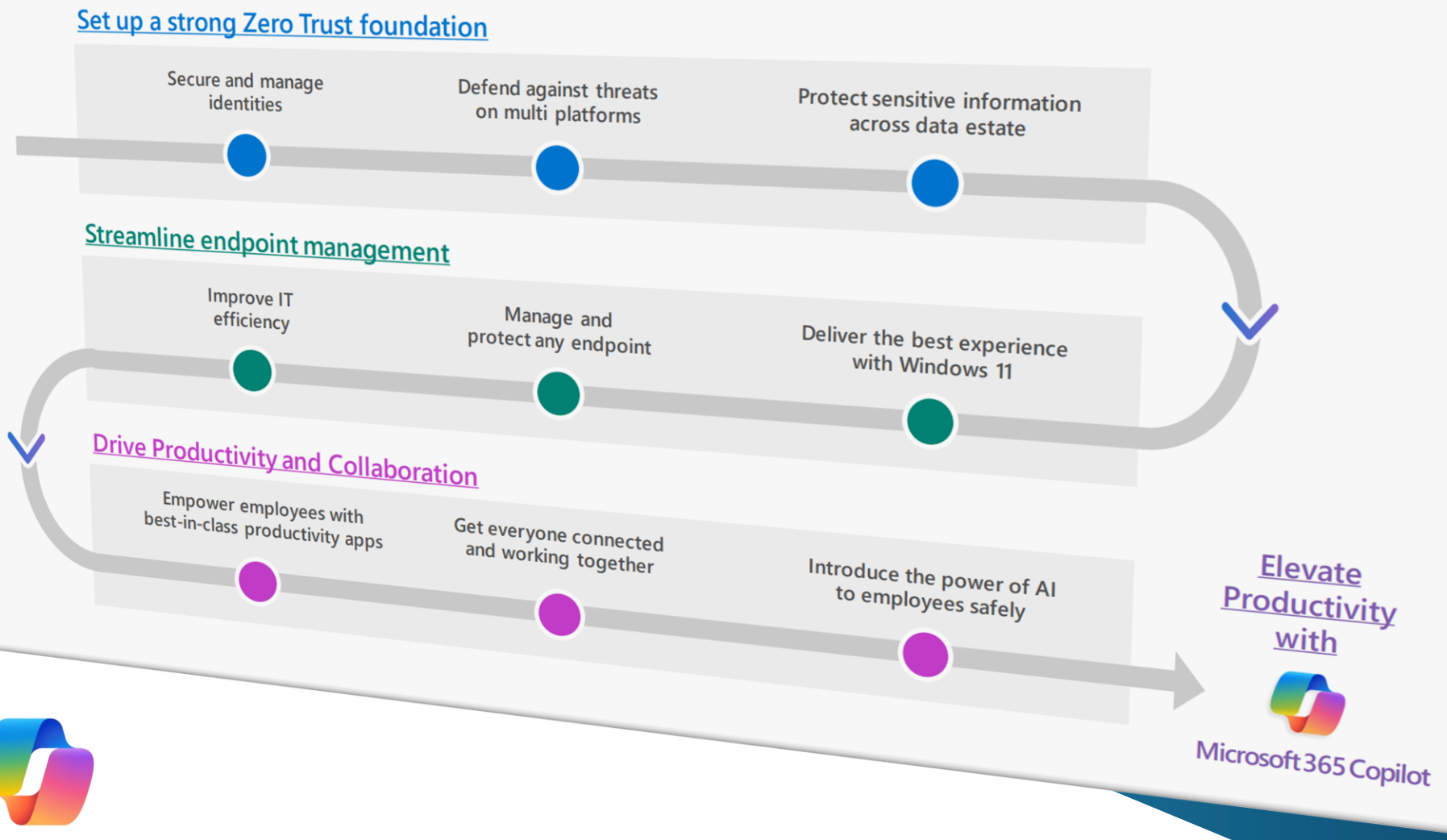
Different views on adequate Cyberdefense

Enduser view on their Cyberdefense

Hacker view on Cyberdefense Enduser

Microsoft 365

The journey to a new way of working



Conclusion: Get NIS2 Ready – start today

- ISO27001 certification
- Apply fundamentals of Cyberhygiene
- We’re all on the same boat: Awareness & Training

Need help?

Danny Zeegers
danny@qfirst.be
0471/ 686 878

Karin Printemps
karin@qfirst.be

Mario Casier
Mario.casier@copaco.com
0479/270 992

security.belgium@copaco.com
053 281 107

WE ARE THE

CompTIA®

COMMUNITY

Vicky Vandergeeten

Vanbreda

Tom Van Britsom

Vanbreda

New digital risks:

we provide an answer with our cyber and fraud insurance

Vanbreda Risk & Benefits

Introduction

Vanbreda Risk & Benefits is the largest insurance broker and risk consultant in Belgium and a leading player in Benelux.

We have been providing tailor-made solutions to businesses, public organisations, social institutions and the self-employed for more than 80 years.

Vanbreda Risk & Benefits

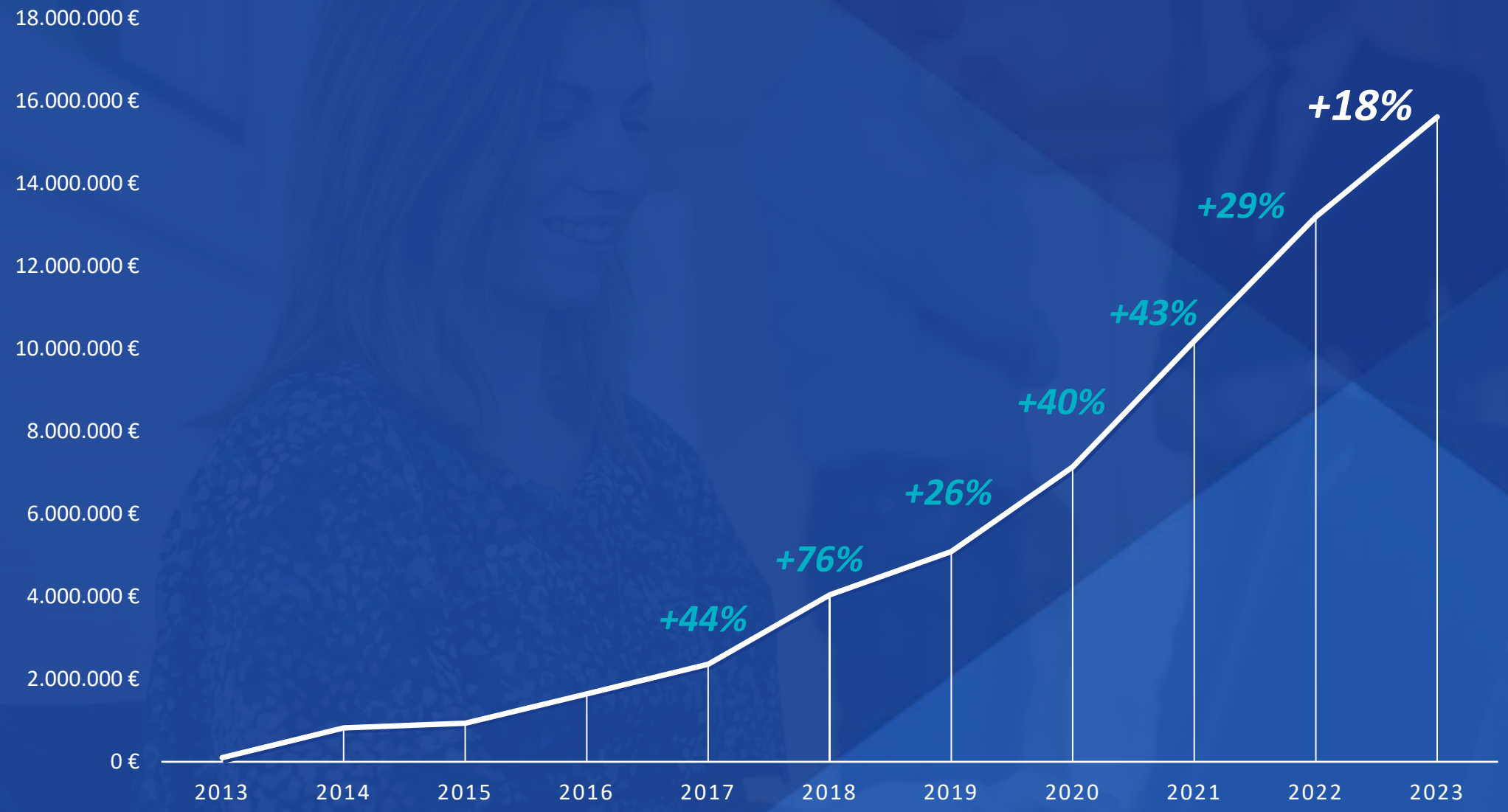
Introduction

Our role as a broker → risk consultant

- Looking for the right insurance for you
- Managing your insurance
- Defending your rights in the event of a claim
- Identifying new risks and providing insurance solutions

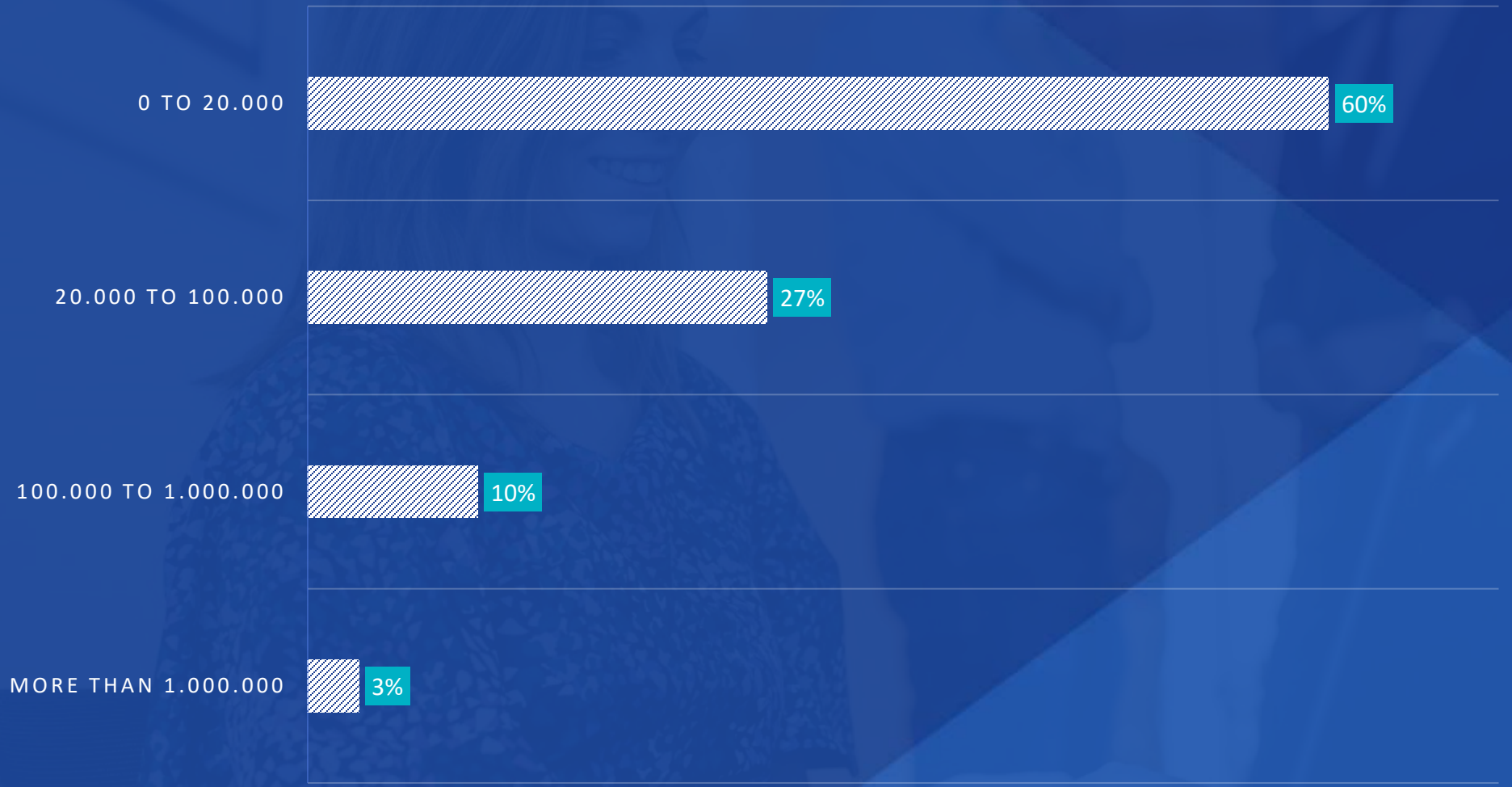
Policy growth in cyber

Premium volume

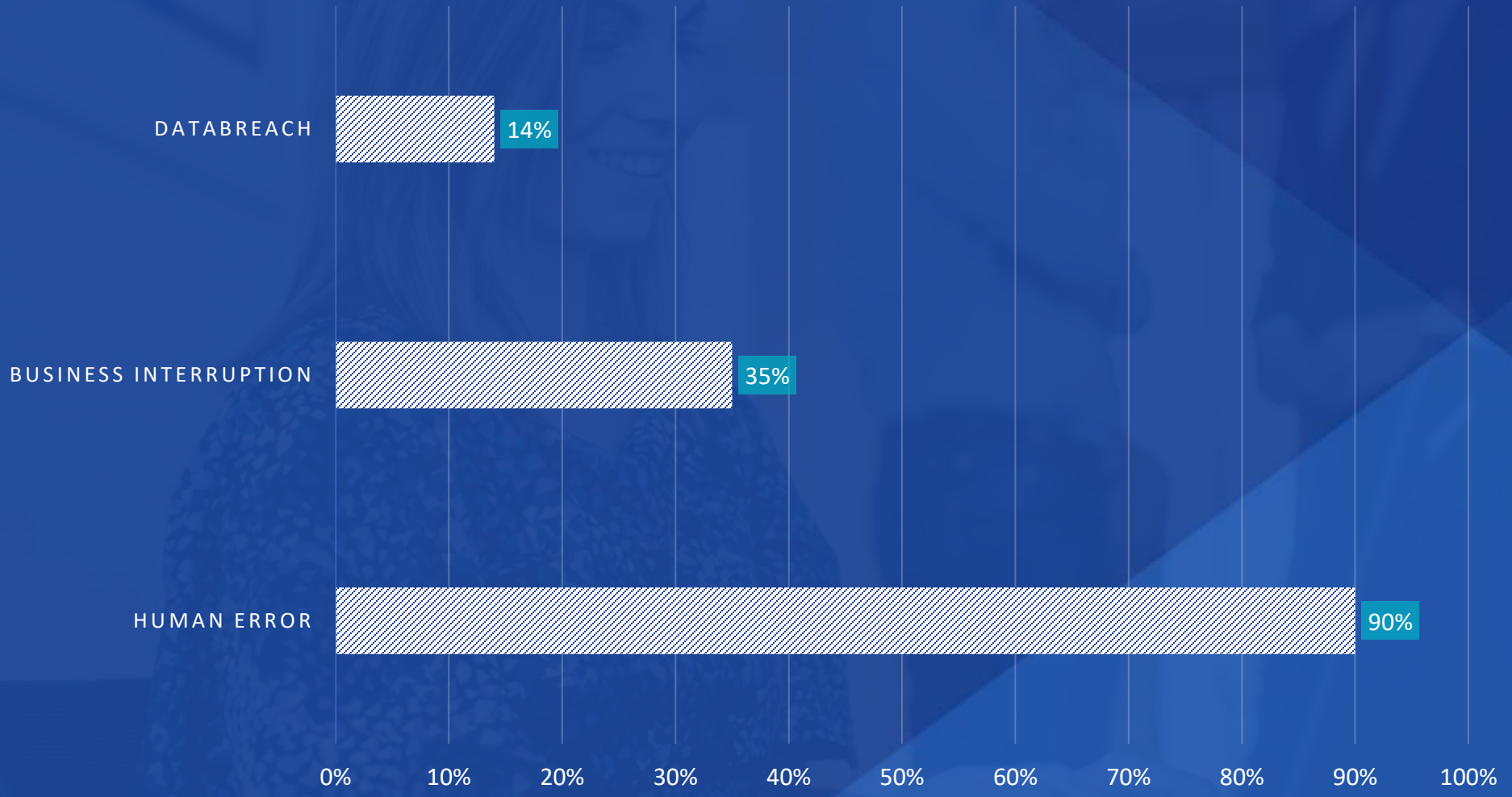


Cyber loss figures

Distribution by size %



Other notable figures



Cyber insurance: insurance solutions for digital risks

What can go wrong...

ERROR

- Editing error
- Accidental deletion

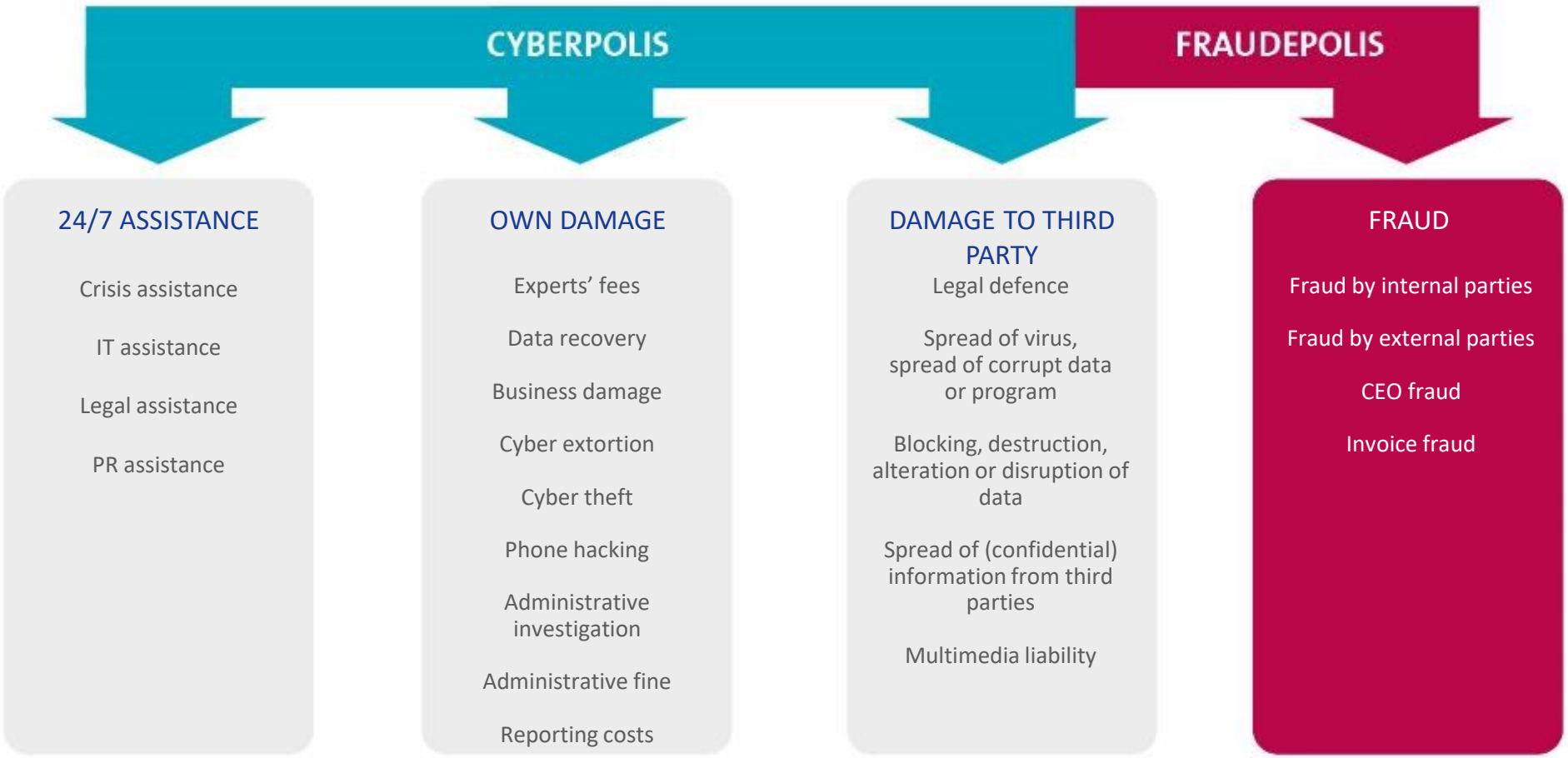
MALICIOUS ACTS

- Hacking, DDoS, viruses, ...
- Unauthorised use

FRAUD

- Internal - External
- CEO
- Invoice

What does the ideal cyber policy look like?



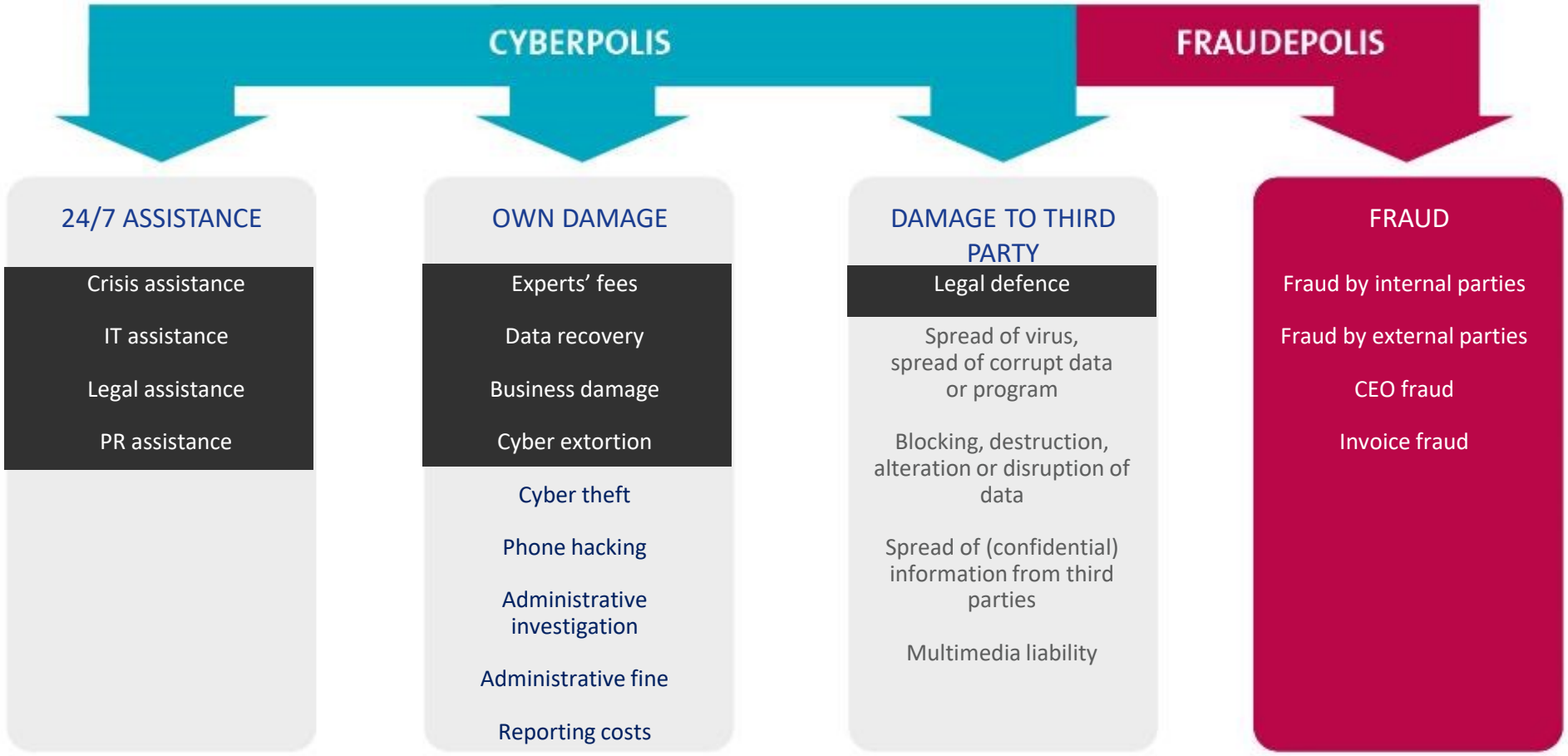
Hacking

Cyber fraud

Invoice fraud

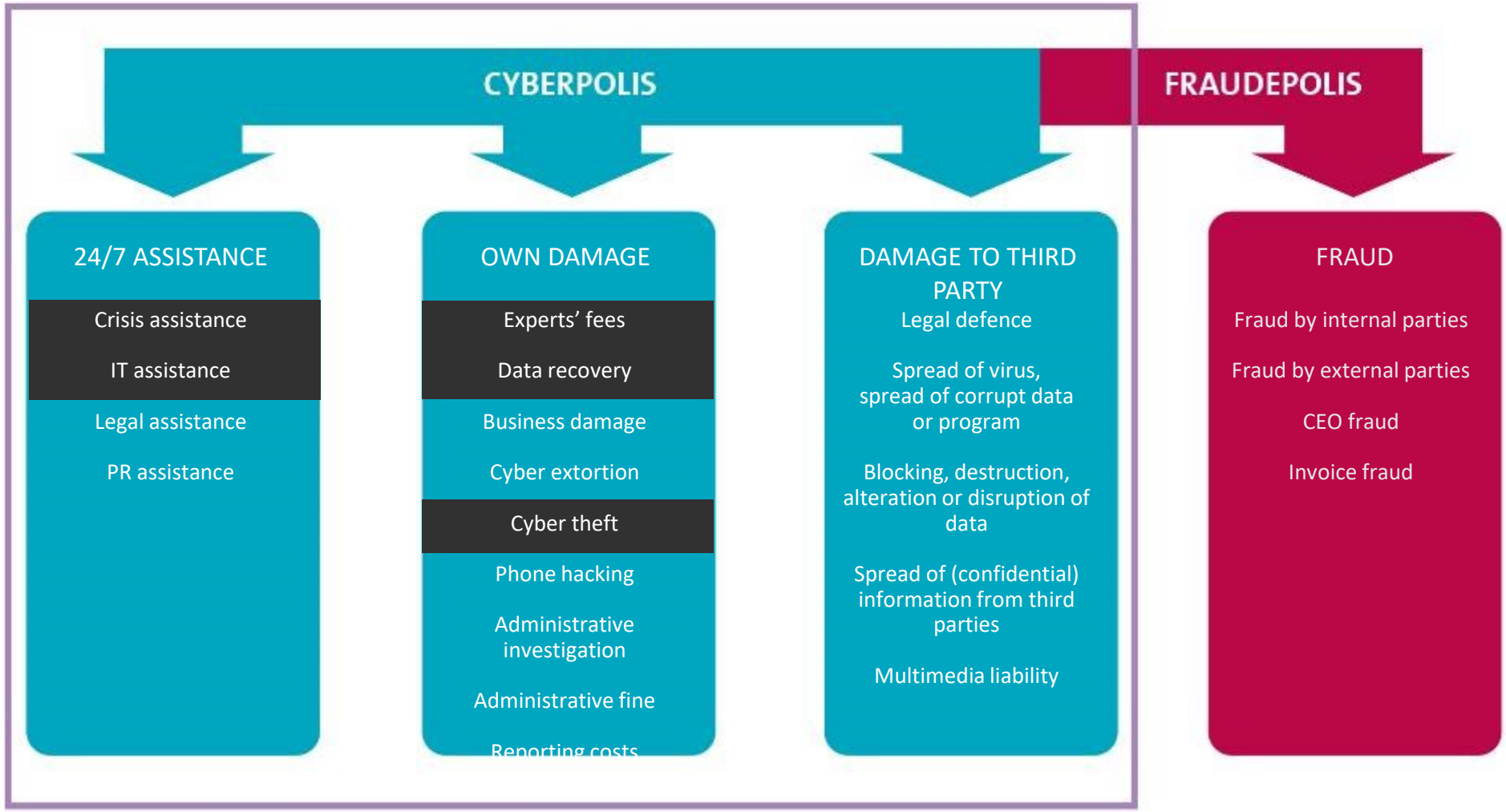
Case 1:
Hacking

Case 1: Hacking



Case 2:
Cyber fraud

Case 2: Invoice fraud



Case 3:

Invoice fraud

Case 3: Invoice fraud

Case 3: Invoice fraud

Accessed cover

TPP c57669

European Trademark & Patent Publications

Trademark no. 12544185 / 0915

VANBREDA RISK & BENEFITS
Plantin en Moretuslei 297
2140 ANTWERPEN
BELGIUM

Registration Number:	0997409
Registration Date:	30.08.2016
Application Number:	1334182
Application Date:	14.06.2016
Classes:	35, 36, 38

TRADEMARK REGISTRATION

REPRODUCTION OF MARK:

my vanbreda

VRB000025941

Pos.	Description	Curr.	Amount
01	Filing Fee	EUR	1370,00
02	Additional Fee	EUR	0,00
	Total Filing Fee	EUR	1370,00

PAYMENT:

BY WIRE TRANSFER :

AMOUNT:	1370,00 €
BENEFICIARY :	TPP Trademark and Patent
BANK NAME :	WBK Bank
IBAN :	PL47 1090 1711 0000 0001 2990 7937
BIC/SWIFT :	WBKPPLPP
PAYMENT TITLE :	Trademark no. 12544185 / 0915

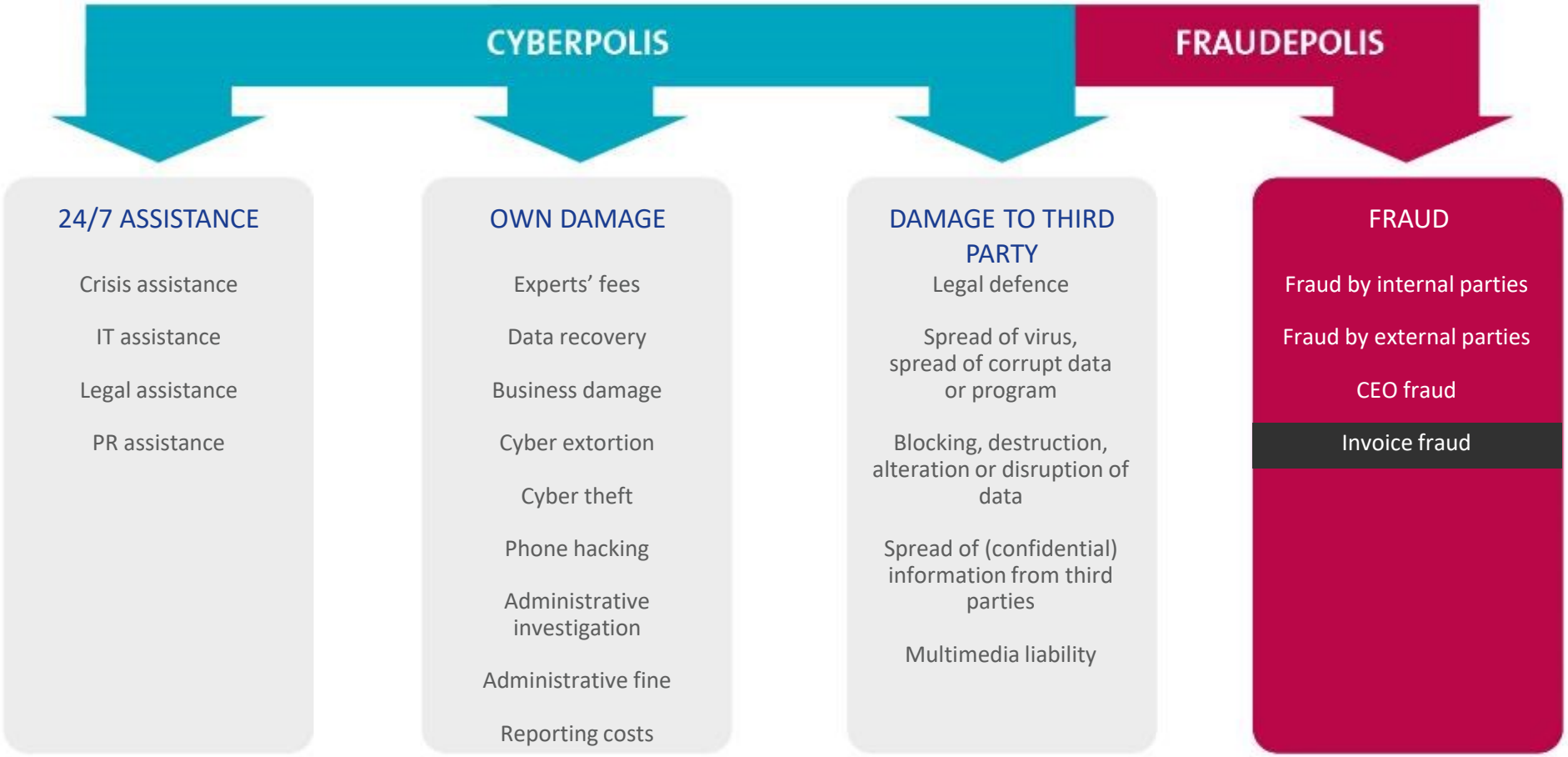
BY CHECK:
TPP Trademark and Patent Publication
Przemyslowa 8/108
75-216 Koszalin Poland (European Union)

Please pay the amount, within 10 days by wire transfer. Don't forget to quote the trademark number.

Dear Customer,
Please notice, that this form is not an invoice. This is an offer for the annual registration of your Trademark in our internet database www.tpp-publication.com. Please also notice that this offer will become a binding contract with the payment of the amount. The registration on our database has not any connection with an official government organization. There is no obligation for you to pay the amount and we have not any business relation yet. We point on our general terms and conditions on our website. If there are any mistakes or modifications relating to your data, please inform us to correct or update them.
TPP Trademark and Patent Publication, Przemyslowa 8 / 108, 75-216 Koszalin, VAT: PL6692524455, info@tpp-publication.com

Case 3: Invoice fraud

Accessed cover



How much does it cost?

TRANSPORT
TURNOVER EUR 2,500,000
10 employees

CYBER

- OWN DAMAGE **EUR 250,000**
- THIRD PARTY DAMAGE **EUR 250,000**
- 24/7
- EXCESS **EUR 1,000**

FRAUD **EUR 100,000**

- INVOICE FRAUD
- CEO FRAUD
- FRAUD BY INTERNAL/EXTERNAL PARTIES

CYBER PREMIUM **EUR 1,300**

FRAUD PREMIUM **EUR 950**

PHISHING AS A SERVICE **EUR 1,240**

TRANSPORT
TURNOVER EUR 35,000,000
105 employees

CYBER

- OWN DAMAGE **EUR 1,500,000**
- THIRD PARTY DAMAGE **EUR 1,500,000**
- 24/7
- EXCESS **EUR 5,000**

FRAUD **EUR 500,000**

- INVOICE FRAUD
- CEO FRAUD
- FRAUD BY INTERNAL/EXTERNAL PARTIES

CYBER PREMIUM **EUR 5,500**

FRAUD PREMIUM **EUR 5,000**

PHISHING AS A SERVICE **EUR 4,174**

Everybody has a plan…

…until they get punched in the face!

Contact

Vicky Vandergeeten

Vicky.vandergeeten@vanbreda.be

0479 72 51 75

Tom Van Britsom

Tom.vanbritsom@vanbreda.be

0479 69 57 80

Thank You

11:10 – 11:20 Attracting Women to Tech

11:20 – 12:00 Respect: The Key to Empowerment

12:00 – 13:00 Lunch

13:00 – 14:00 Keynote: Future-Proofing your Company

14:00 – 15:00 Decoding NIS2

15:00 – 15:30 ***Break***

15:30 – 16:30 Insights from CompTIA Community UK&I / Ask The Experts on NIS2

WE ARE THE

CompTIA®

COMMUNITY

Insights from the CompTIA Community - UK&I Cybersecurity Interest Group

Greg Jones

Kaseya / Datto

Room: Next Door

WE ARE THE

CompTIA

COMMUNITY

Greg Jones

Kaseya / Datto - VP of Business development EMEA

CompTIA - Chair of the UK&I Cyber Security Community & EC member for the UK&I Community


WARNING

CompTIA COMMUNITY

Agenda

1. Who is Greg Jones & Why CompTIA & Why I get involved
2. An overview of the Cyber Threat Landscape as we see it today
3. How Cyber Security Frameworks can help all businesses & building Cyber Resilience
4. A Cyber Security exercise to drive Cyber resilience
5. A quick overview of the last UK&I Cyber Security meeting in Birmingham, UK
6. The how & why you should get more involved with CompTIA
7. Key Takeaways

CompTIA COMMUNITY

Who is Greg Jones
&
Why CompTIA & Why I get involved

CompTIA COMMUNITY

An overview of the Cyber Threat Landscape as we see it today

MSP / SMB Cyber Threat Landscape 2024

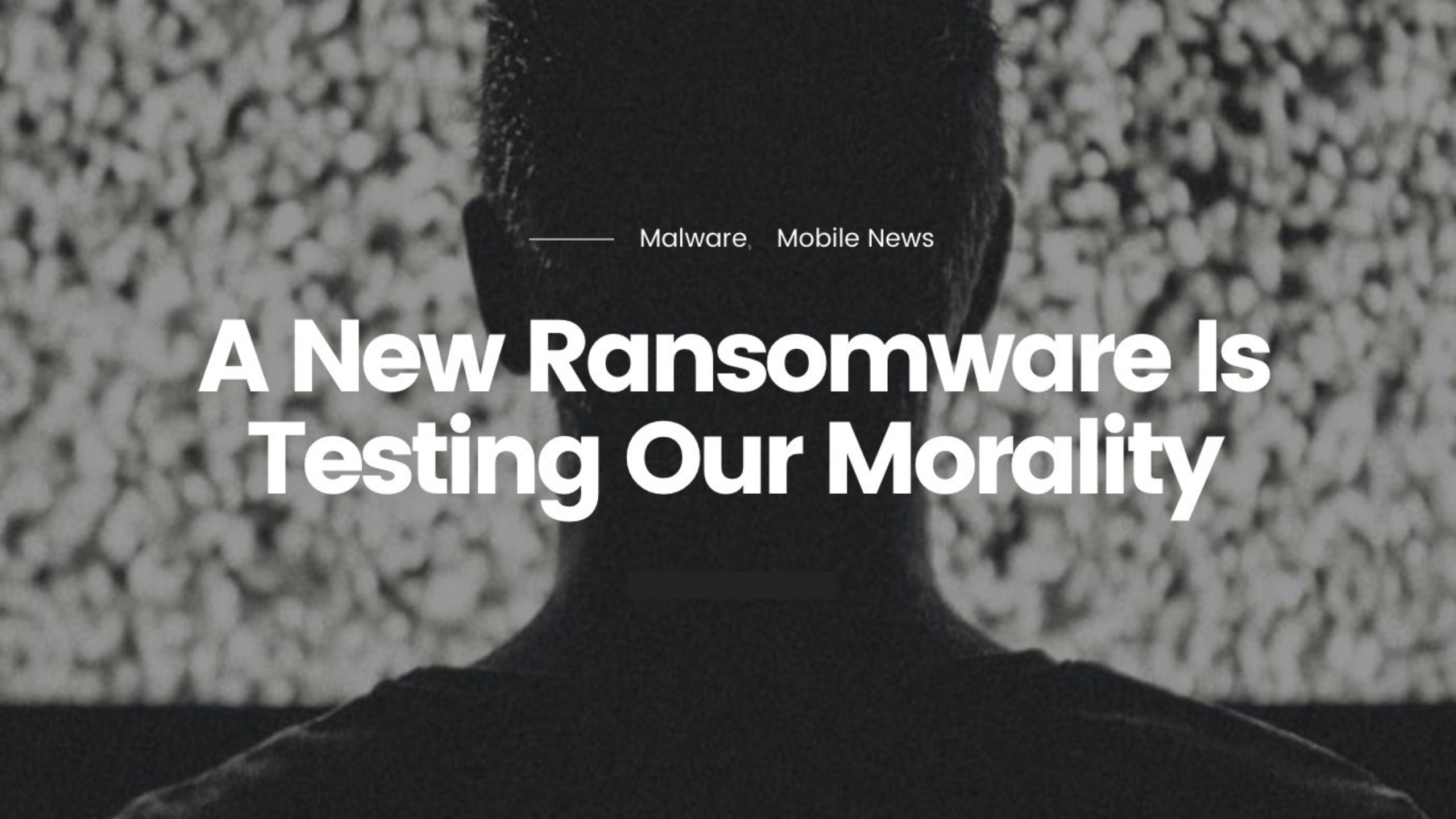
Cyber-Crime & Ransomware Jumps To The Highest Level Of All Time!

Living in a golden age of tech

Surely this is a good thing?

The Ever-Evolving Threat Landscape

Double extortion
Maze / Popcorn Ransomware
IOT devices
Corporate insiders – Large cash offers
Supply chain employees
Ransomware as a Service
Social engineering



Malware, Mobile News

A New Ransomware Is Testing Our Morality

The latest ransomware is pure evil genius

Popcorn Time ransomware melds social engineering with technology to spread itself faster than ever

Credit: Dbreen via Pixabay

Ransomware is always nasty business, but the latest variant discovered by the MalwareHunterTeam takes the nastiness to a whole 'nother level.

Turning victims into criminals

Apparently, the latest Popcorn Time ransomware adds a new twist to the standard M.O. of demanding payment from their victims or permanently lose access to their

RELATED


Much ado about the ransomware scourge


Stupid encryption mistakes criminals make


Ransomware as a Service fuels explosive growth


VIDEO
Setting up DLP features for email security.

Terrifying 'Popcorn Time' computer virus can only be removed by infecting TWO FRIENDS or paying a ransom

- **Access to decryption key given after paying in Bitcoin or nominating two others**
- **Ransomware shares a name with programme that downloads and streams films**
- **Hackers claim to be using proceeds for 'food, medicine and shelter to those in need'**

By LIBBY PLUMMER FOR MAILONLINE

PUBLISHED: 10:16 EDT, 12 December 2016 | **UPDATED:** 18:28 EDT, 12 December 2016

Share

78 shares

21 View comments

A menacing new computer virus leaves victims with a choice between paying hackers a ransom and infecting two friends' computers.

Attacks/Breaches | 5 MIN READ | NEWS

Attackers Are Already Exploiting ChatGPT to Write Malicious Code

The AI-based cha
malware.

AI-Powered Malware Holds Potential For Extreme Consequences

Could Artificial Intelligence Be a Black Ball

Home / AI & Machine Learning / AI-Powered Malware Holds Potential For...

AI-powered malware is a growing security concern, CyberArk survey finds

Attacks Continue to Rise

300%

Increase in reported CyberCrimes since Covid-19

92.7%

Ransomware attacks have nearly doubled

59%

MSPs said remote work increased ransomware attacks

Who are the Bad guys?

Who Are The Threats…

Hacking Collectives
Ethical hackers — break into systems to help make technology more secure. “white-hat hackers”

IoT Hackers
Think your Alexa is safe?

Ransomware Developers
Over £7 Billion pounds in damages since 2018

Nation State
Countries that don’t seem to like the UK

Organized Crime
Gangs, mobs, and things that go bump in the night

Insider Threats
£19 billion lost every year in secrets

Script Kiddies
Lacks programming knowledge - uses existing software to launch attacks. Uses programs without knowing how they work or what they do.

Hacktivist
Hackers with a political goal

Malware Developers
Starting as low at £30 - you to can own a copy of any popular Malware

Mobile Malware
Have an iPhone or Android phone? Think you’re safe? Think again.

RYUK

CONTI

TRICKBOT

How Modern Threats Have Evolved

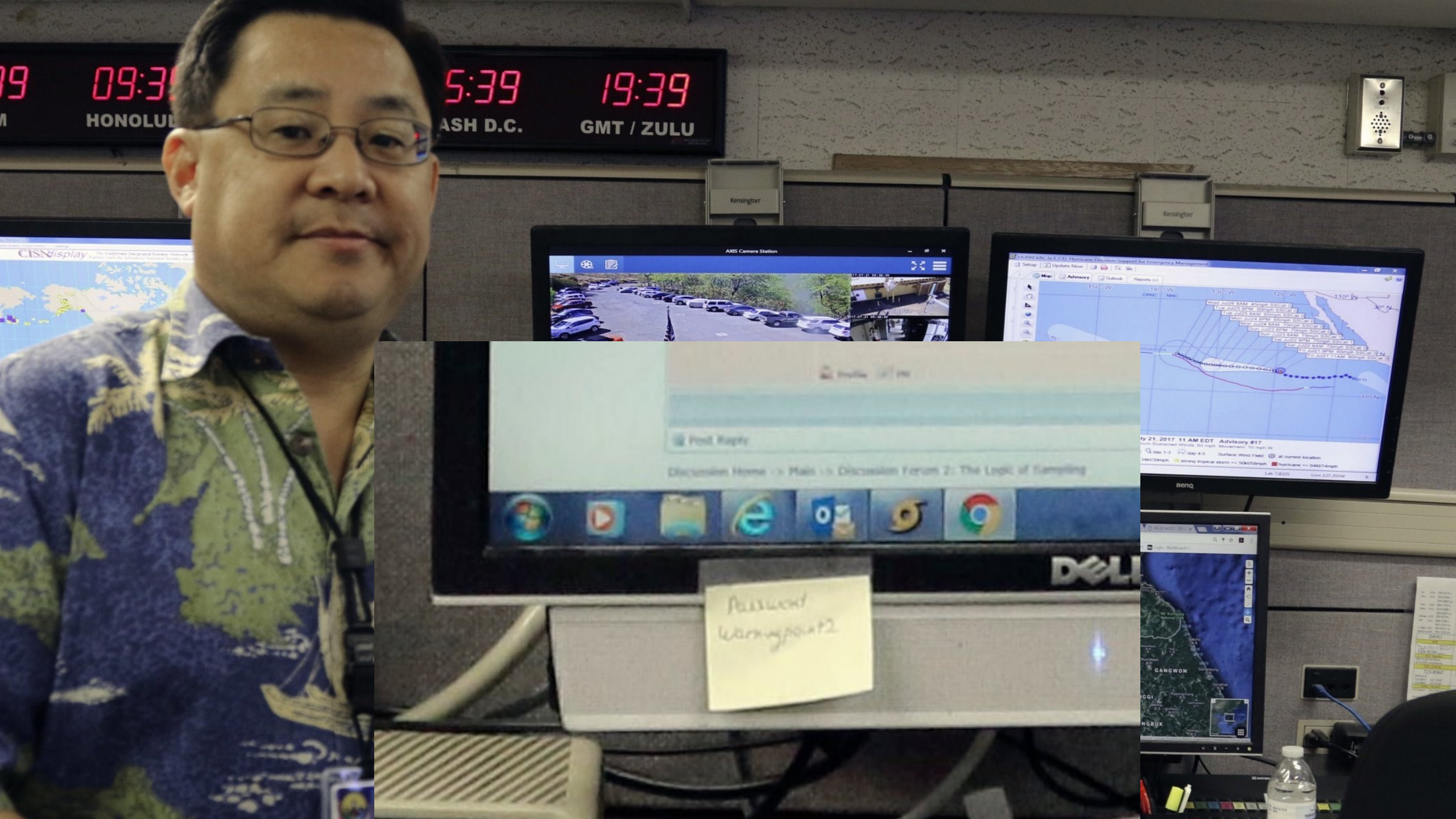
Attackers have adopted new methods to bypass endpoint protection

Modern trends include:

Living Off The Land - “Why deliver my malicious program when I can make your existing admin tools do the work for me?”

Staged Malware & Attacks - Individually, each stage is benign

Disabling Endpoint Protection - Many attacks seek to disable AV and defensive tools before dropping their final stage (e.g. Ransomware)


HONOLULU
ASH D.C.
GMT / ZULU
AXIS Camera Station
Kensington
Kensington
DELL
benq
GANGWON


MilFlip Logon Details


THE GREATEST CASINO HEIST


DXRACER

Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer

Sunday, April 15, 2018 Wang Wei

Share 9.25k Share Tweet Share

GENIUS HACKERS USED A VEGAS CASINO'S FISH TANK THERMOMETER TO STEAL HIGH ROLLERS' PERSONAL INFORMATION

Craziest casino heist ever?

THOMAS FREEMAN · APR 16, 2018

Hackers are increasingly targeting "internet of things" devices, or smart devices hooked up to the Internet that are not nearly as safeguarded as computers or databases.

Case in point: Nicole Eagan, the CEO of cyber-defense company Darktrace, revealed at a conference in London that one particularly clever group of hackers infiltrated a casino through the "smart thermometer" of a lobby fish tank.

"The attackers used that to get a foothold in the network," Eagan said. "They then found the high-roller database and then pulled that back across the network, out the thermostat, and up to the cloud."

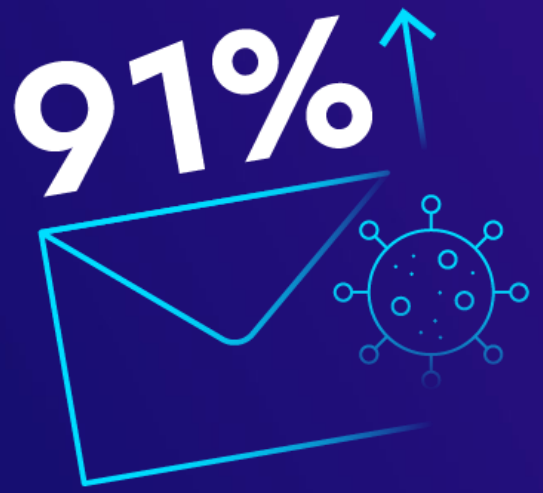
datto

CompTIA COMMUNITY

How Cyber Security Frameworks can help all businesses & Building Cyber Resilience

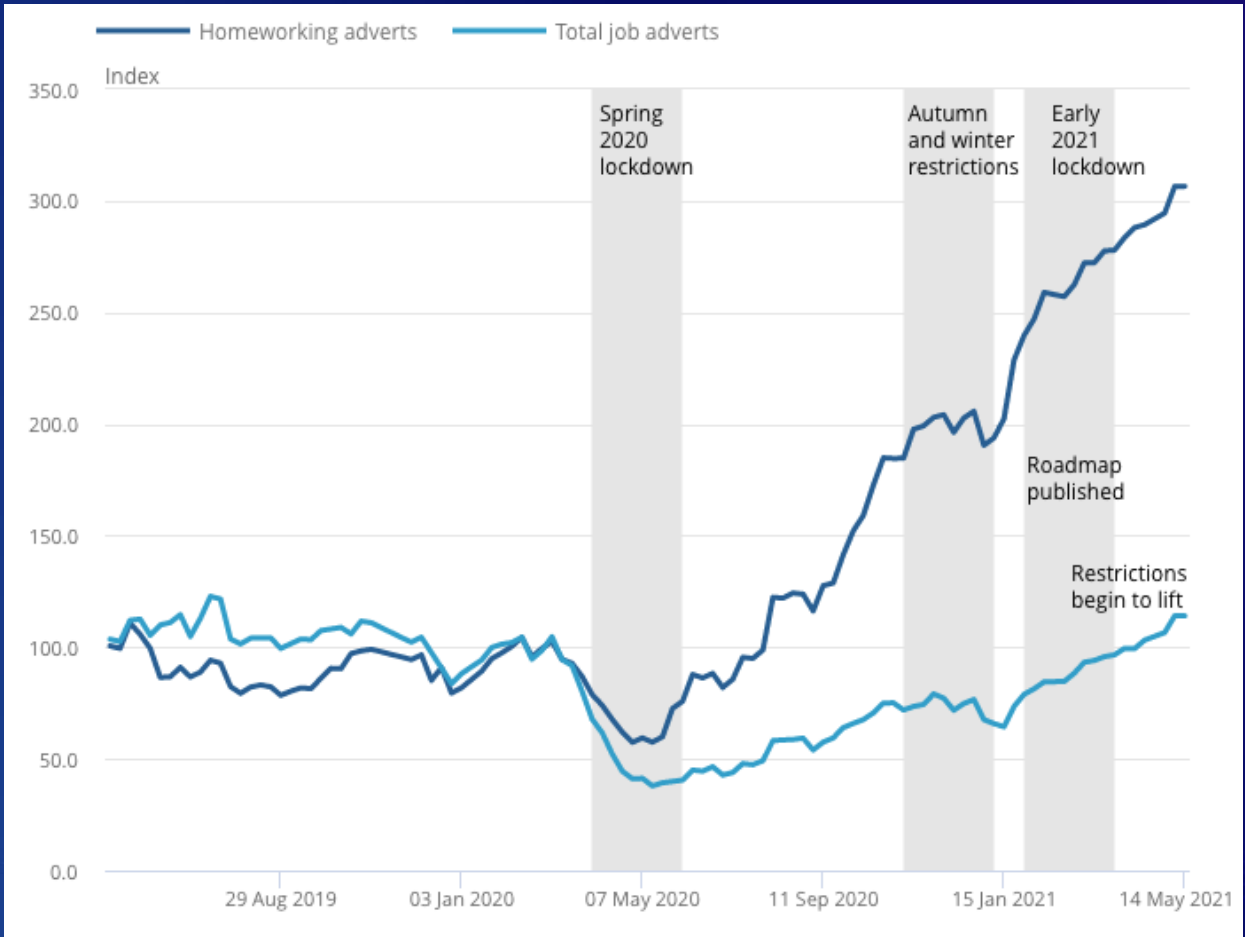
91% OF ALL CYBER ATTACKS
BEGIN WITH A PHISHING EMAIL

THE FREQUENCY OF
PHISHING INCIDENTS
DOUBLED IN 2020 COMPARED TO 2019



Sources: Deloitte, FBI

The new world of business



1. Ups and downs in home working
2. Increased spread in data locations
3. Changing threat vector security
4. Hybrid working
5. Compliance GDPR/Data Protection
6. Supply Chain and Client Requirements
7. To protect your Organisation

ONS - Business and individual attitudes towards the future of homeworking


NOT IF
BUT
WHEN

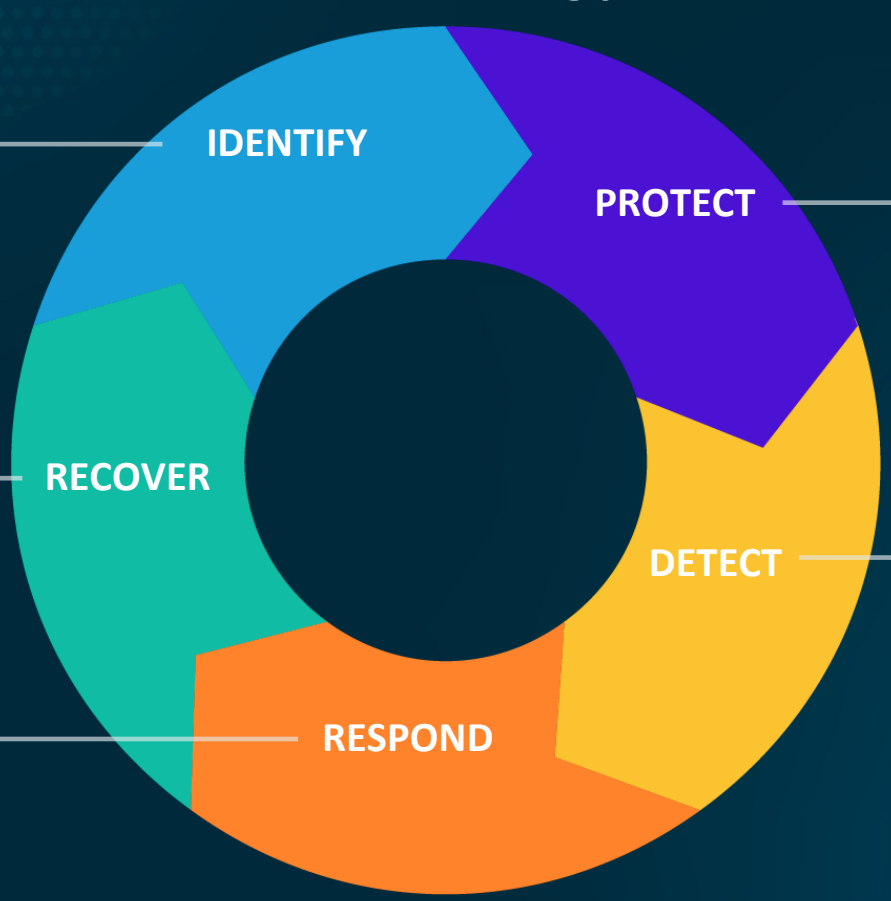
CYBER RESILIENCY

Cyber Resilience is a measure of business strength in preparing for, operating through, and recovering from a cyber attack.

Cyber resilience relies on the successful ability to identify, protect, detect, respond, and recover quickly from any cyber event

NIST Cyber Security Framework

National Institute of Standards and Technology



Asset Management
Business Environment
Risk Management & Strategy
Governance
Risk Assessment
Supply Chain Risk Management

Identity Management, Authentication, & Access Control
Awareness & Training
Data Security
Information Protection Processes & Procedures
Maintenance
Protective Technology

Anomalies & Events
Security Continuous Monitoring
Detection Processes

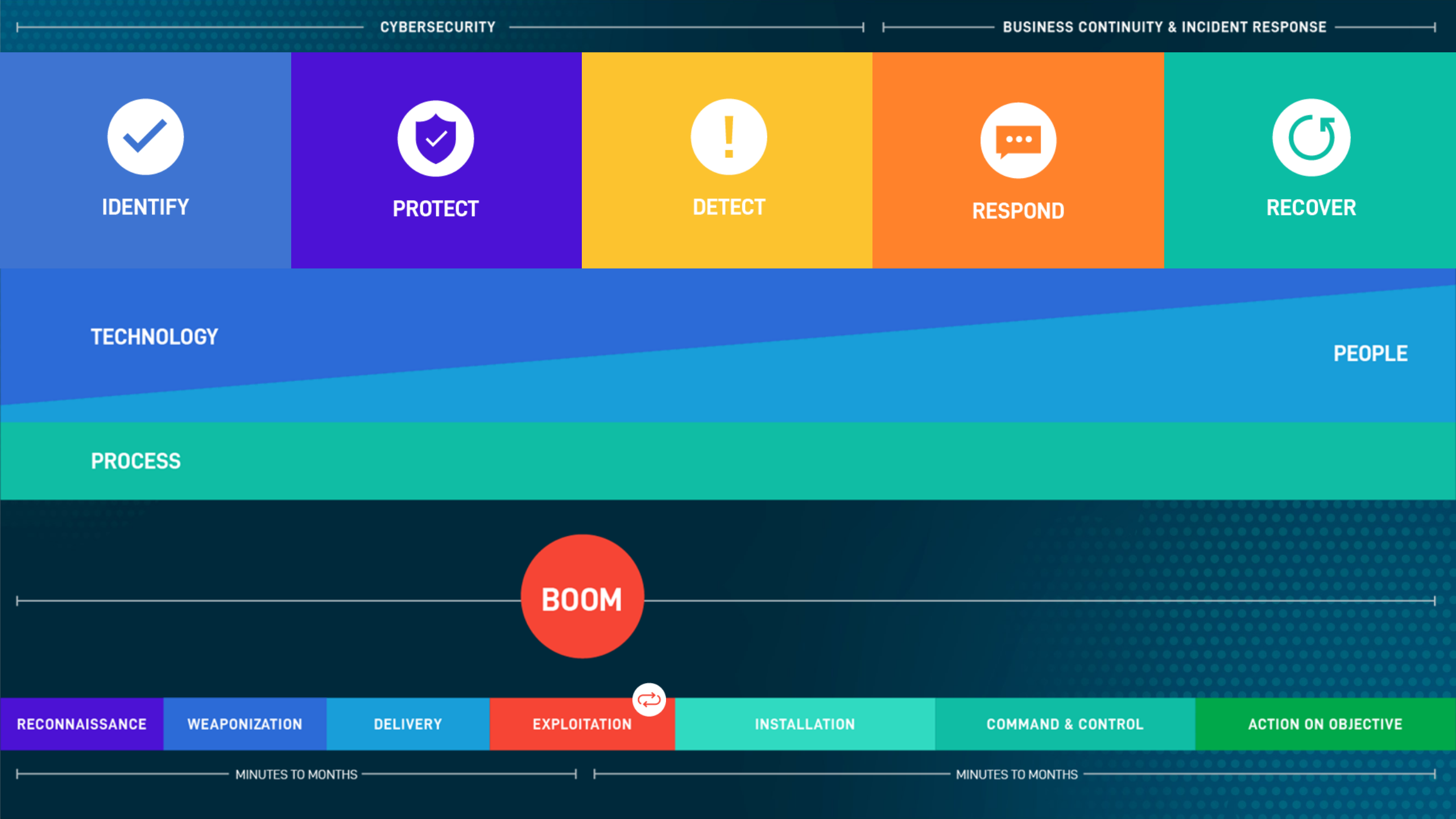
Communications
Mitigations
Improvements
Response Planning
Analysis

Recovery Planning
Improvements
Communications

Three Pillars of Cyber Resilience

Cyber resilience includes security, monitoring, and BCDR technology. However, a successful cyber resilience strategy requires a holistic approach that starts with people and process.

1. **People**
2. **Process**
3. **Technology**


CYBERSECURITY
BUSINESS CONTINUITY & INCIDENT RESPONSE
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
TECHNOLOGY
PEOPLE
PROCESS
BOOM
RECONNAISSANCE
WEAPONIZATION
DELIVERY
EXPLOITATION
INSTALLATION
COMMAND & CONTROL
ACTION ON OBJECTIVE
MINUTES TO MONTHS
MINUTES TO MONTHS

CompTIA COMMUNITY

A Cyber Security Exercise to drive Cyber Resilience

CompTIA
COMMUNITY

CompTIA COMMUNITY

A quick overview of the last UK&I Cyber Security meeting in Birmingham, UK

Key Takeaways

Cyber Resources & Takeaways

Resources

- CompTIA ISAO – Information Sharing & Analysis Organization
- CompTIA Resource Library – State of Cybersecurity, Embedding Security into Company Culture, others
- Emergency Response Team (ERT)

CompTIA ISAO
Information Sharing and Analysis Organization

CompTIA CYBERSECURITY Emergency Response Team

Copyright © 2023 CompTIA, Inc. All Rights Reserved | CompTIA.org

Cyber Resources & Takeaways

Takeaways

- The BIG Hacks:
  - Customer
  - MSP
- Understanding the why and what behind attacks: How can we be proactive against these threats?
- Insurance & Press: What should you have in place?

- Growth & Development
  - What are your next steps?
  - Internal/External Enablement
  - Ready to monetise

CompTIA

Copyright © 2023 CompTIA, Inc. All Rights Reserved | CompTIA.org

CompTIA COMMUNITY

The how & why you should get more involved with CompTIA

CompTIA COMMUNITY

Global Communities

ANZ
ASEAN
Benelux
DACH
North America
UK&I

Industry Advisory Councils

Artificial Intelligence
Blockchain & Web3
Channel Development
Cybersecurity
IoT
SaaS Ecosystem

CompTIA ISAO

Executive Steering Council

Committees

with New Global Task Force

Cybersecurity
DEI
Emerging Technology
Managed Services

Technology Interest Groups

Artificial Intelligence
Blockchain
DEI
Drone
IoT

CompTIA
COMMUNITY

We Are The CompTIA COMMUNITY

#CompTIACommunity

THANK YOU

SCAN ME

Please connect with
me on LinkedIn:
Greg Jones
gjones@datto.com

WE ARE THE CompTIA COMMUNITY

NIS2: ASK THE EXPERTS

Vicky Vandergeeten

Vanbreda

Tom Van Britsom

Vanbreda

Mario Casier

Copaco

Maarten Verhaghe

TRUST Advocaten

15:30 – 16:30 Insights from CompTIA Community UK&I / Ask The Experts on NIS2

16:30 – 16:45 ***CompTIA Cybersecurity Interest Group Benelux***

16:45 – 17:00 End of Day Recap

17:00 – 19:30 Dinner, Drinks & Networking

WE ARE THE

CompTIA®

COMMUNITY

Pierre Kleine Schaars

Tycho Löke

CompTIA COMMUNITY BENELUX

CompTIA Community Benelux Cybersecurity Interest Group

13 February 11am-12noon CET

https://connect.comptia.org/events/view/comptia-community-benelux-cybersecurity-interest-group

15:30 – 16:30 Insights from CompTIA Community UK&I / Ask The Experts on NIS2

16:30 – 16:45 CompTIA Cybersecurity Interest Group Benelux

16:45 – 17:00 ***End of Day Recap***

17:00 – 19:30 Dinner, Drinks & Networking

WE ARE THE CompTIA COMMUNITY

Daniëlle Meulenberg

Sophos

Chair CompTIA Community Benelux

Steven Tytgat

Tyneso

Vice Chair CompTIA Community Benelux


ANY
questions?

15:30 – 16:30 Insights from CompTIA Community UK&I / Ask The Experts on NIS2

16:30 – 16:45 CompTIA Cybersecurity Interest Group Benelux

16:45 – 17:00 End of Day Recap

17:00 – 19:30 ***Dinner, Drinks & Networking***

Please take 3 minutes to do the survey and make sure you get on the photo!

We want to hear from you! Please take this very short survey:

https://forms.office.com/r/1tc6j41YAt?origin=lprLink

Mark your calendars:

Next CompTIA Community Meeting in Benelux 22nd of May Utrecht!


Thank you!

17:00 – 19:30 Networking Food and Drinks