Comment les nouvelles régulations (DORA, NIS-2, CER,...) rapprochent les acteurs de la continuité et de la (cyber-) sécurité pour assurer la résilience opérationnelle: présentation des recherches du Business Continuity Institute.

Who am I ?

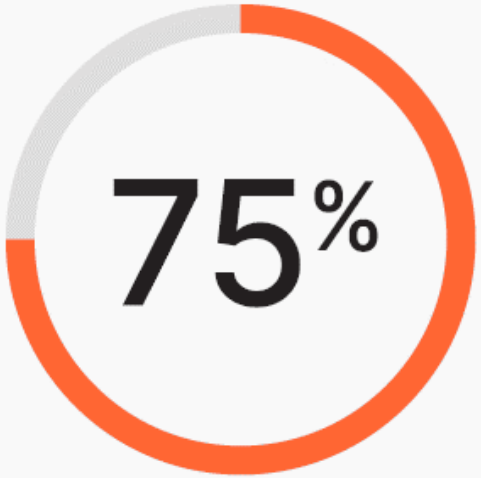
Christian De Boeck, PhD, mBCI

- Since 20+ years in Operational Resilience profession
- BE Chapter Leader for the Business Continuity Institute
- Consultant
- Auditor
- Trainer
- Climate activist
- Coach
- Proud father of 2 daughters

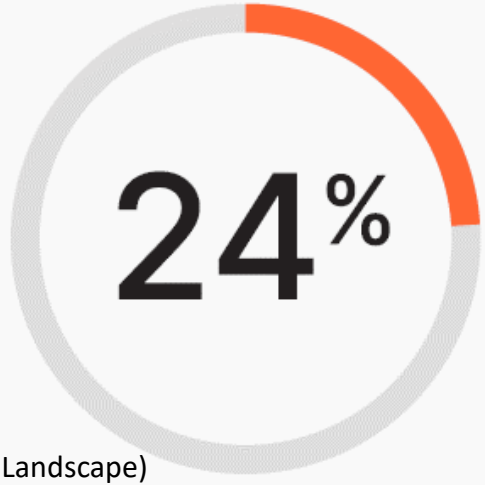
We are

SYNERGIT.BE

The financial consequences of complacency in *Belgium*.



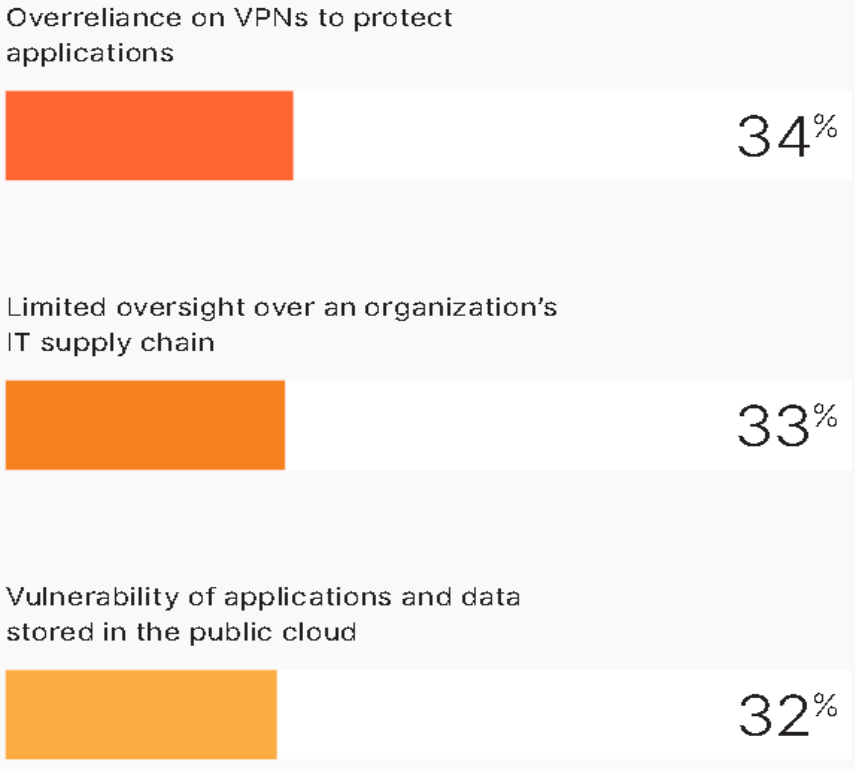
of respondents from organizations that have experienced attacks in the past 12 months estimated the financial impact of these to be at least **€940.000**



estimate the loss to be **€1.88 million** or more

Source: Cloudflare
(Shielding the Future:Belgium Cyber Threat Landscape)

Top issues with current cybersecurity architecture



Ranking among the top three most common types of cyberattacks

Web Attacks **53%**

Phishing **47%**

Distributed Denial of Service (DDoS) attacks **33%**

10 keywords of DORA (according to Google I.A.)

1. **Résilience opérationnelle numérique:** C'est le cœur de DORA, visant à renforcer la capacité des entités financières à résister aux cyberattaques et aux incidents technologiques.
2. **Cyber-résilience:** Synonyme de résilience opérationnelle numérique, ce terme souligne l'importance de se protéger contre les menaces cybernétiques.
3. **Secteur financier:** DORA s'adresse spécifiquement aux institutions financières.
4. **TIC:** Au cœur des activités financières modernes et donc particulièrement visées par DORA.
5. **Risques technologiques:** Evaluer et gérer les risques liés à l'utilisation des technologies.
6. **Cyberattaques:** DORA impose des mesures de protection renforcées contre ces menaces.
7. **Incident de sécurité:** Tout événement qui compromet la sécurité des systèmes d'information.
8. **Continuité des activités:** Les entreprises financières doivent être capables de maintenir leurs activités en cas d'incident.
9. **Surveillance:** Pour s'assurer que les entités financières respectent les nouvelles exigences.
10. **Réglementation:** DORA est un nouveau texte réglementaire.

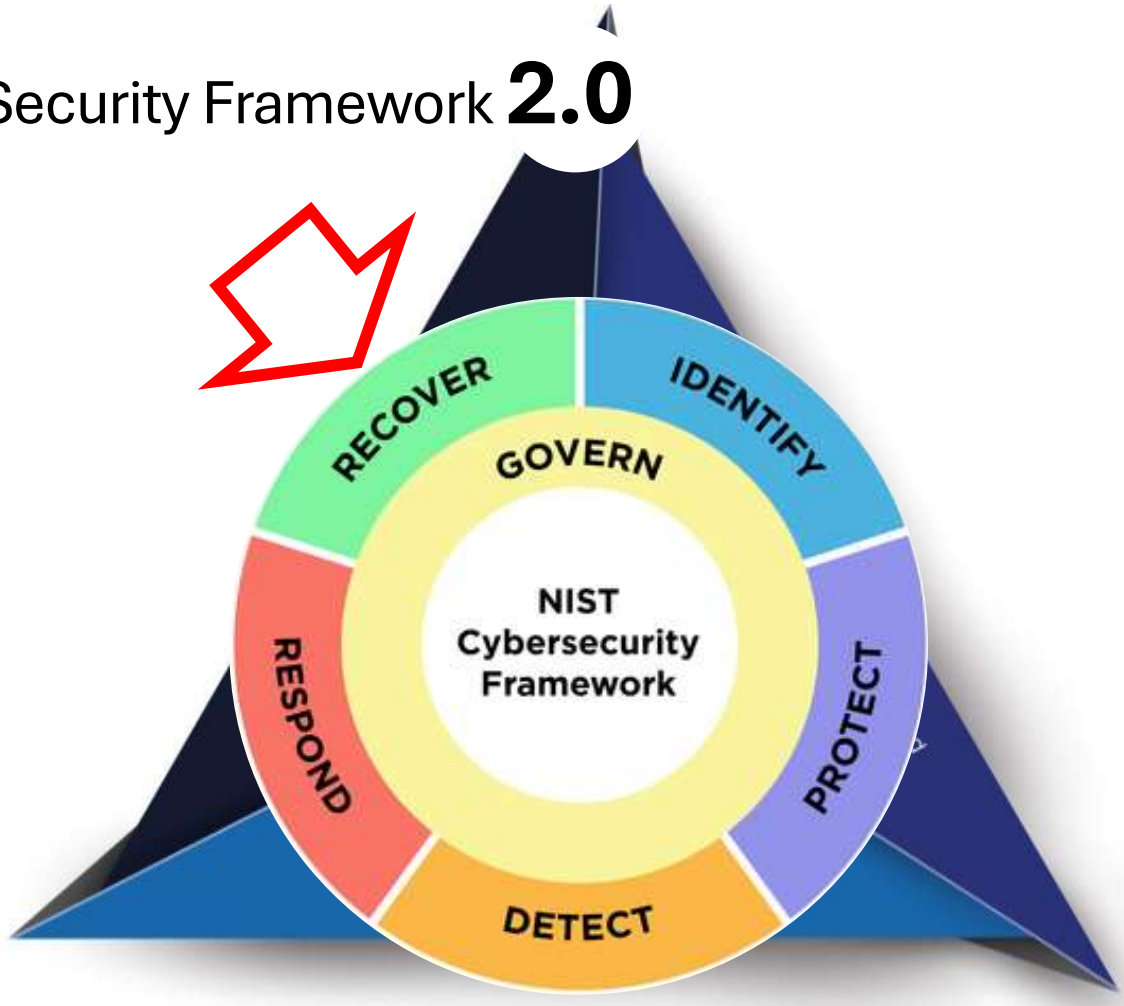
Ce qui manque: Gestion des fournisseurs / parties tierces, …

10 keywords:

NIS-2	CER
1.Cyber-sécurité	1.Résilience
2.Entités essentielles	2.Entités critiques
3.Risques cybernétiques	3.Cyber-sécurité
4.Incident de sécurité	4.Risques
5.Gestion des risques	5.Incident
6.Plan de reprise d'activité (PRA)	6.Plan de continuité d'activité (PCA)
7.Coopération internationale	7.Coopération
8.Notification d'incident	8.Surveillance
9.Responsabilité	9.Notification
10.Surveillance	10.Transposition

(Cyber-) Resilience – Operational Resilience

NIST CyberSecurity Framework 2.0

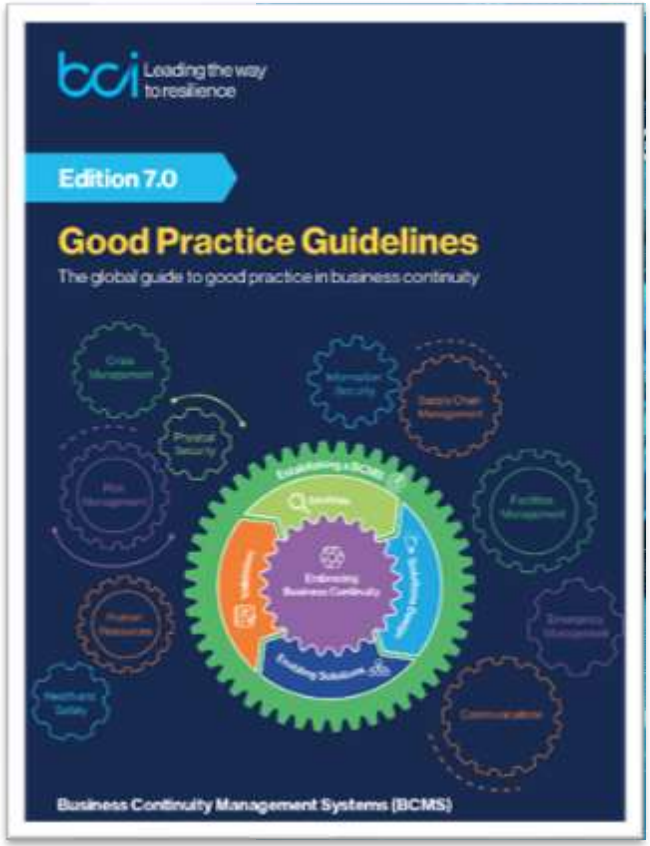


Standard	Title
ISO 22300:2021(en)	**Vocabulary**
ISO 22301:2019(en) + Amd 2:2024	**Business continuity management systems — Requirements** **AMENDMENT 1: Climate action changes**
ISO 22313:2020(en)	**Business continuity management systems — Guidance on the use of ISO 22301**
ISO 22315:2014(en)	Societal security — Mass evacuation — Guidelines for planning
ISO 22316:2017(en)	**Organizational resilience — Principles and attributes**
ISO/TS 22317:2021(en)	Business continuity management systems — Guidelines for business impact analysis
ISO/TS 22318:2021(en)	Business continuity management systems — Guidelines for supply chain continuity management
ISO 22320:2018(en)	Emergency management — Guidelines for incident management
ISO 22325:2016(en)	Emergency management — Guidelines for capability assessment
ISO 22326:2018(en)	Emergency management — Guidelines for monitoring facilities with identified hazards
ISO 22329:2021(en)	Emergency management — Guidelines for the use of social media in emergencies
ISO/TS 22330:2018(en)	Business continuity management systems — Guidelines for people aspects of business continuity
ISO/TS 22331:2018(en)	Business continuity management systems — Guidelines for business continuity strategy
ISO/TS 22332:2021(en)	Business continuity management systems — Guidelines for developing business continuity plans & procedures
ISO 22342:2023(en)	Protective security — Guidelines for the development of a security plan for an organization
ISO/TR 22351:2015(en)	Societal security — Emergency management — Message structure for exchange of information
ISO 22361:2022(en)	**Crisis management — Guidelines**
ISO 22388:2023(en)	Authenticity, integrity and trust for products and documents — Guidelines for securing physical documents
ISO 22396:2020(en)	Community resilience — Guidelines for information exchange between organizations
ISO 22397:2014(en)	Societal security — Guidelines for establishing partnering arrangements
ISO 22398:2013(en)	Societal security — Guidelines for exercises


Leading the way
to resilience

BCI updates & resources:

- BCI Education month is just over (see you next year).
- BCI World Hybrid 2024 (30th and 31st October), Physical (London – UK) and Virtual.
- Int'l events and calendar for 2025 available soon – BE to be agreed.
- GPG (Good Practice Guide) 7.0
- CBCI 7.0 certification course (3-5 day's or online)
- CBCI refreshment course (1 of 2 day's)
- Specific 1day deep dive courses (BIA, BCP, exercises…)
- Dozens of knowledge, researches, reports, webinar available, … on www.thebci.org (some are reserved / free for affiliated).



Continuité? Résilience?

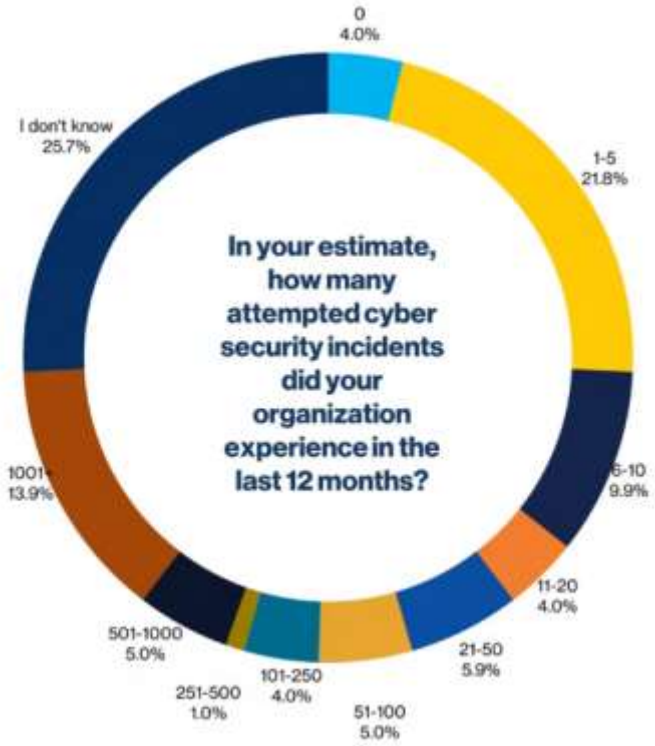
Defining Operational Resilience

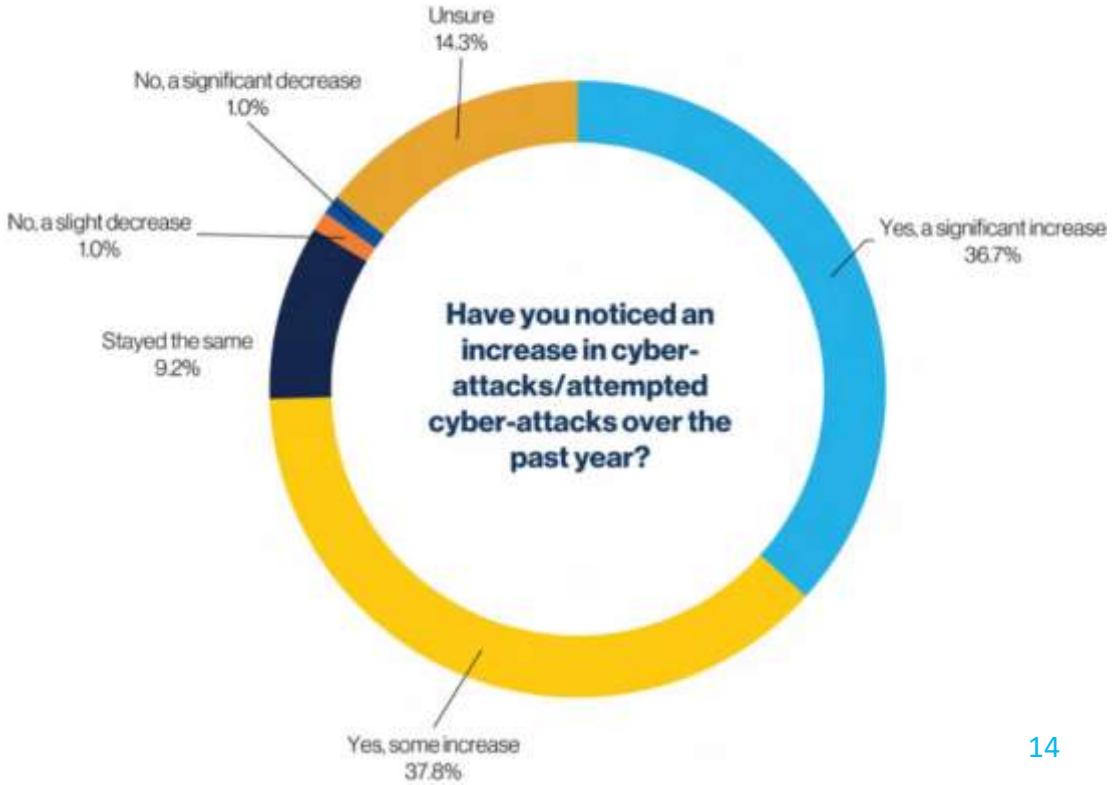
Providing a universal definition of operational resilience is difficult due to the varying requirements, regulations, and understanding in different regions and sectors. However, there are some tools and processes which are universally recognised as being critical components of an effective operational resilience programme.

Business Continuity, c'est récupérer l'existant (même outils, méthodes, …).

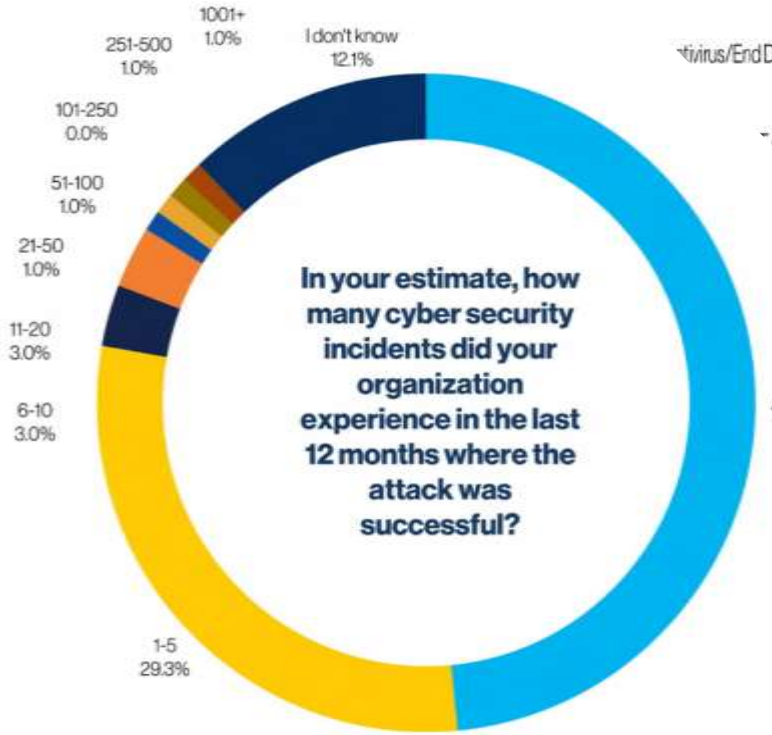
La résilience opérationnelle peut incorporer de *rebondir* grâce à des outils, des processus, … des objectifs différents. Et la résilience organisationnelle?

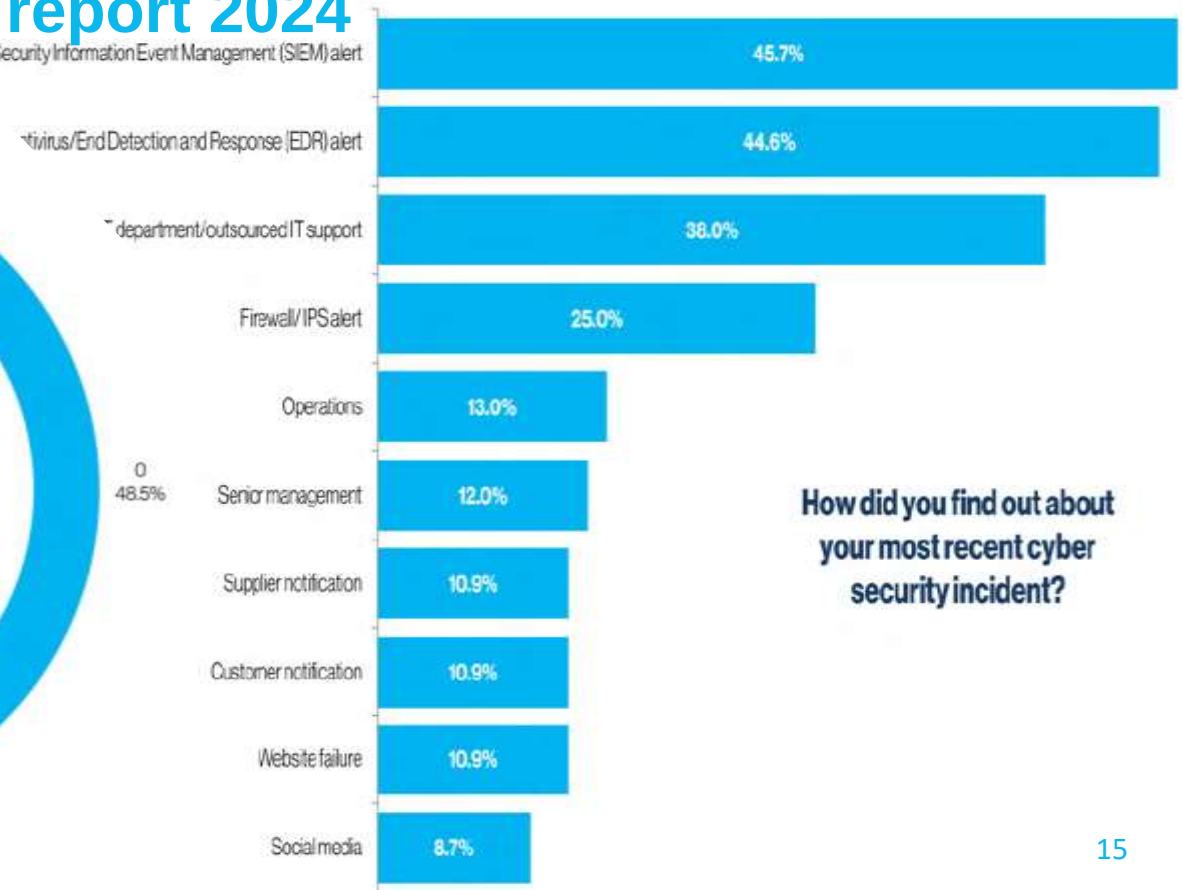
BCI Cyber-resilience report 2024



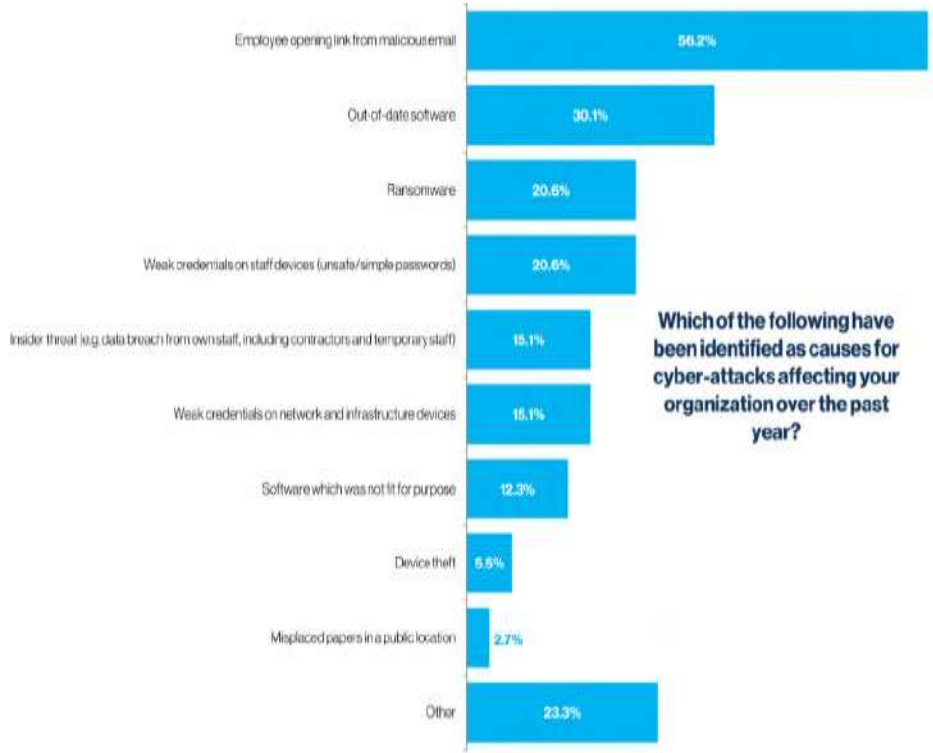


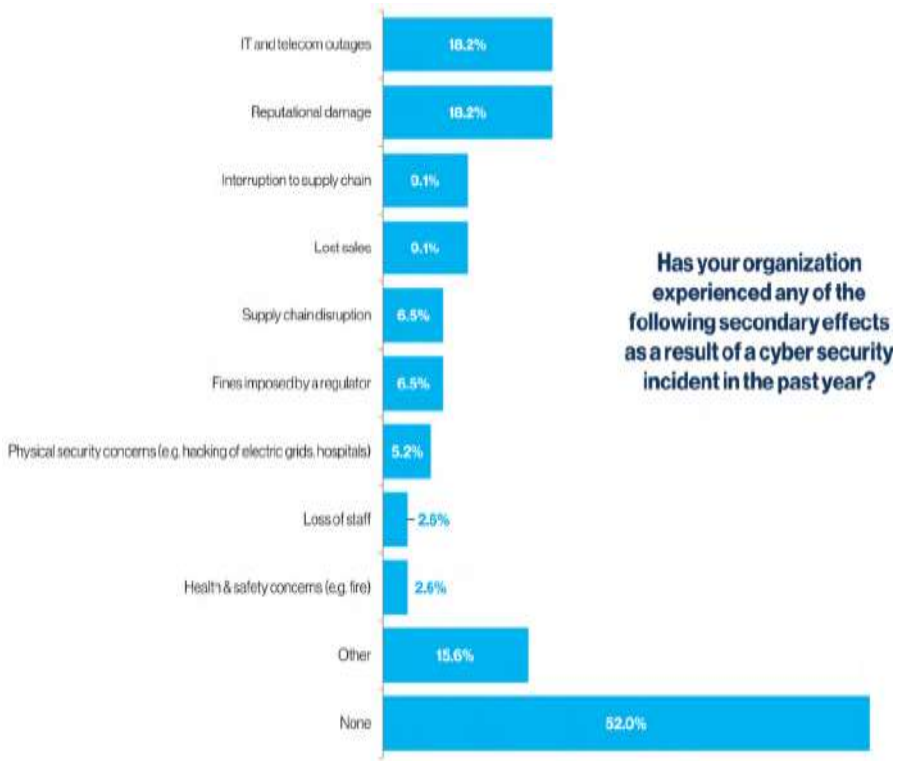
BCI Cyber-resilience report 2024





BCI Cyber-resilience report 2024





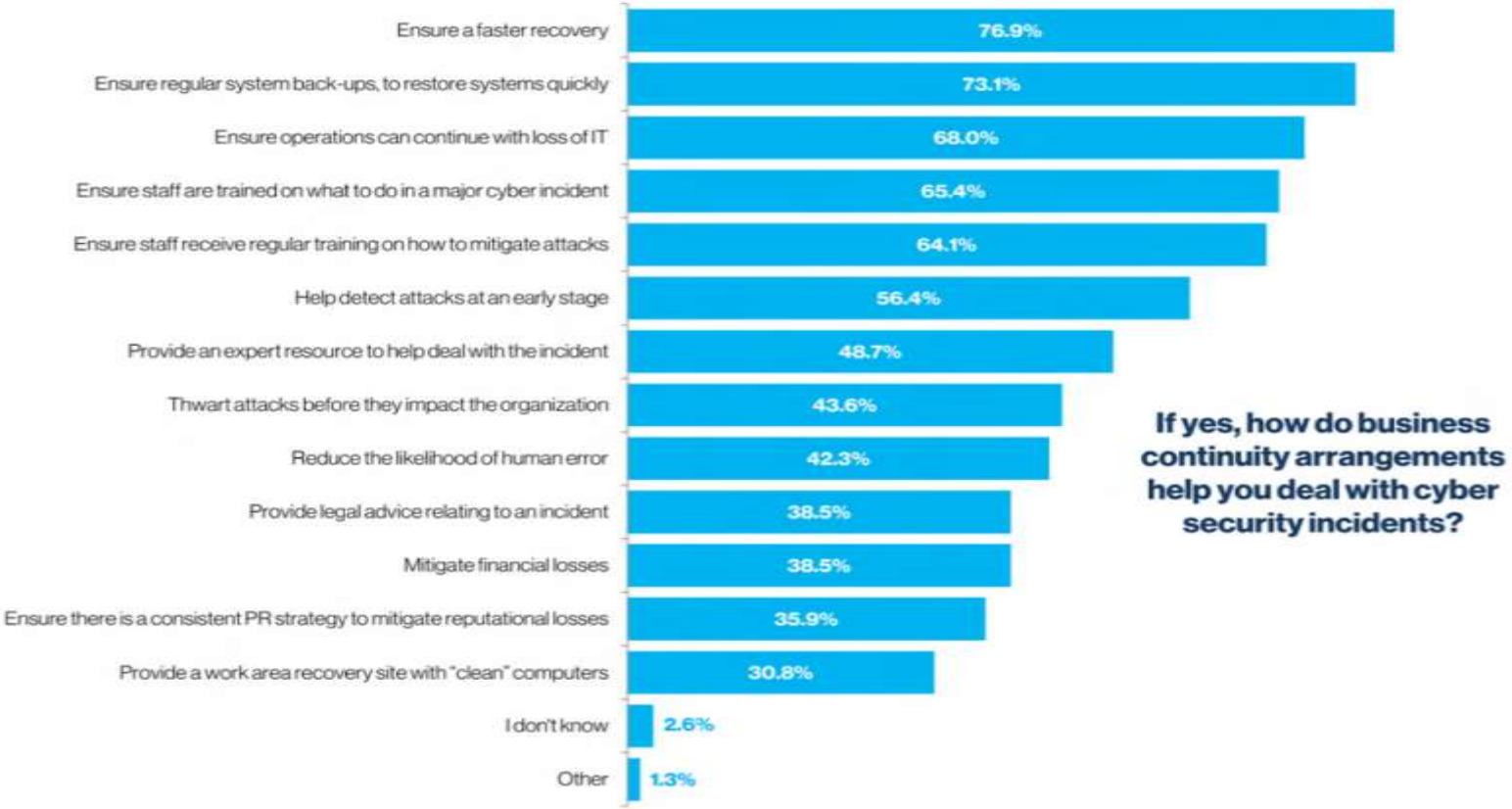
Leading the way to resilience

BCI Cyber-resilience report 2024

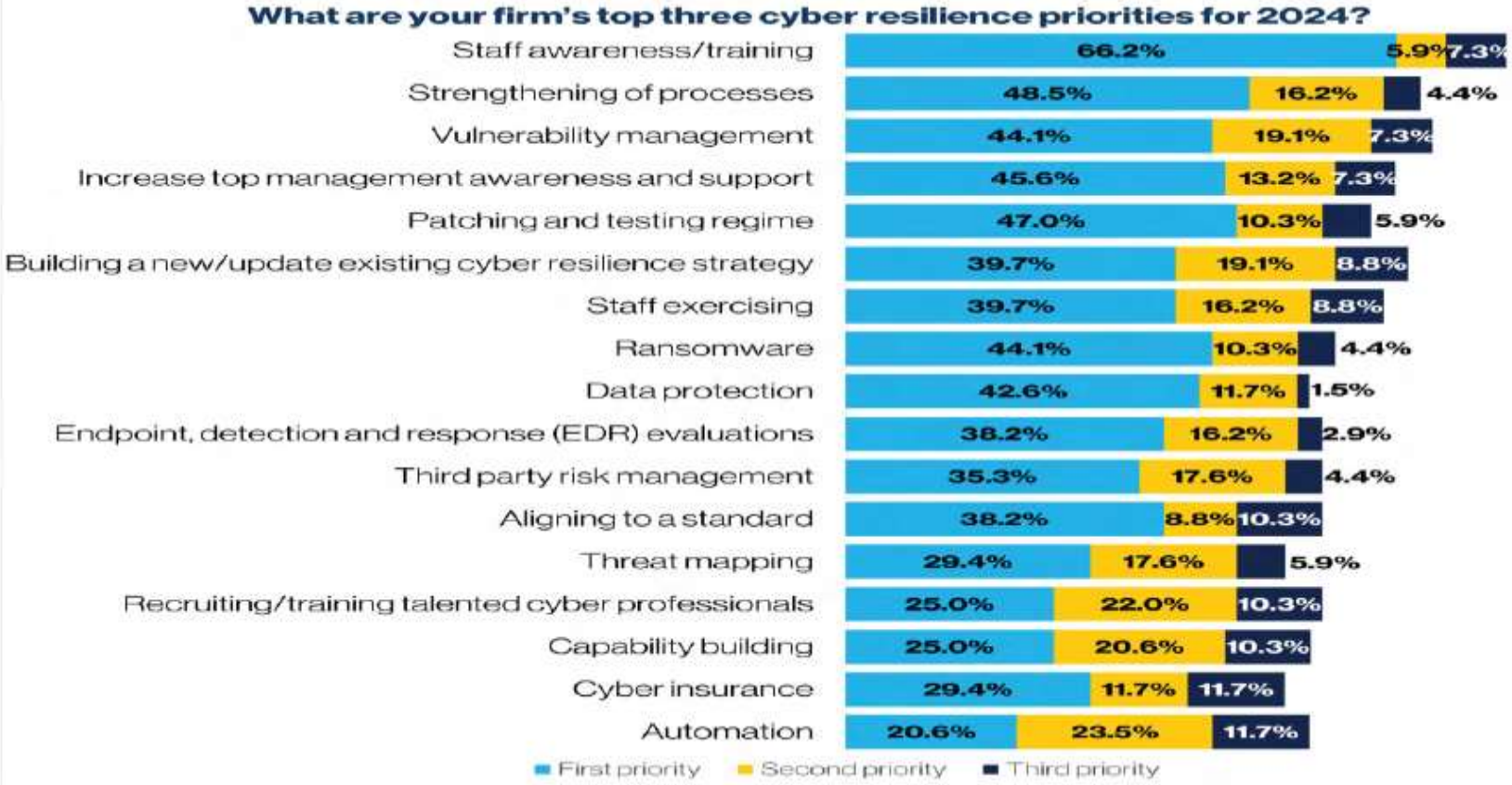
BCI Cyber-resilience report 2024

BCI Cyber-resilience report 2024

BCI Cyber-resilience report 2024



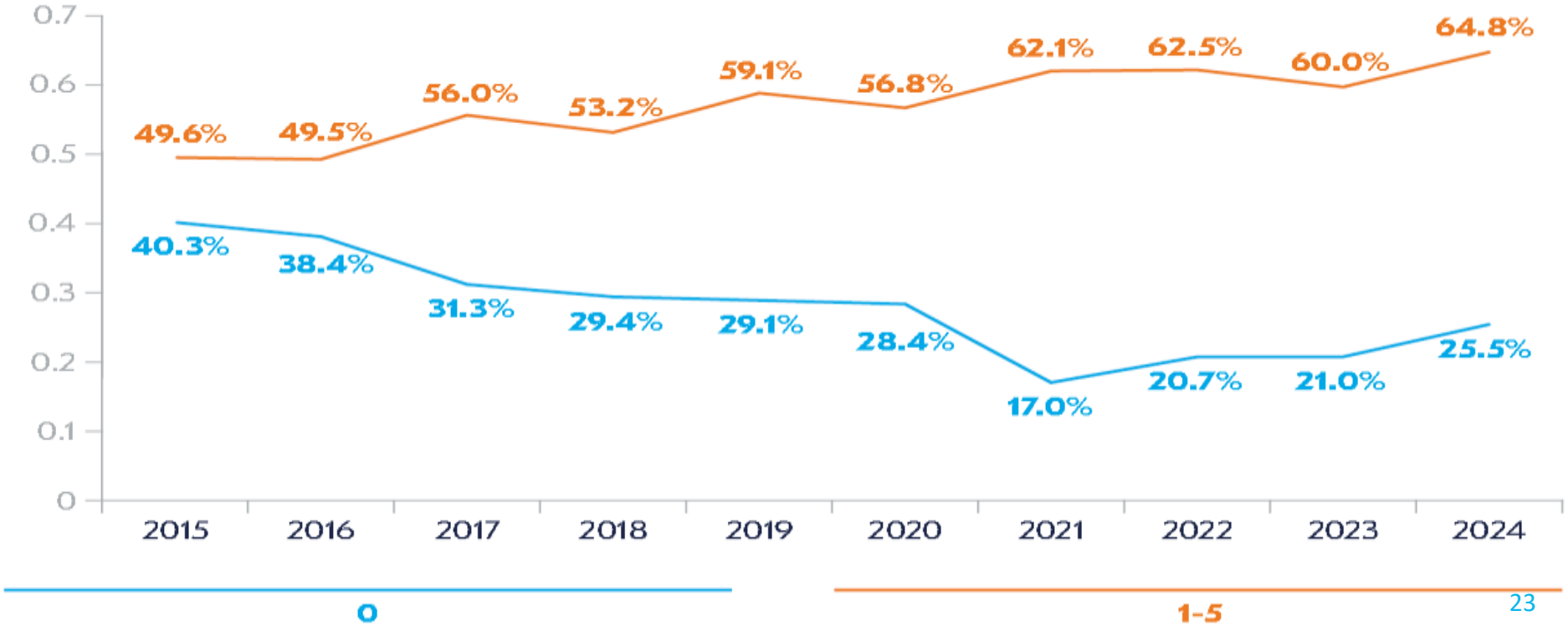
BCI Cyber-resilience report 2024



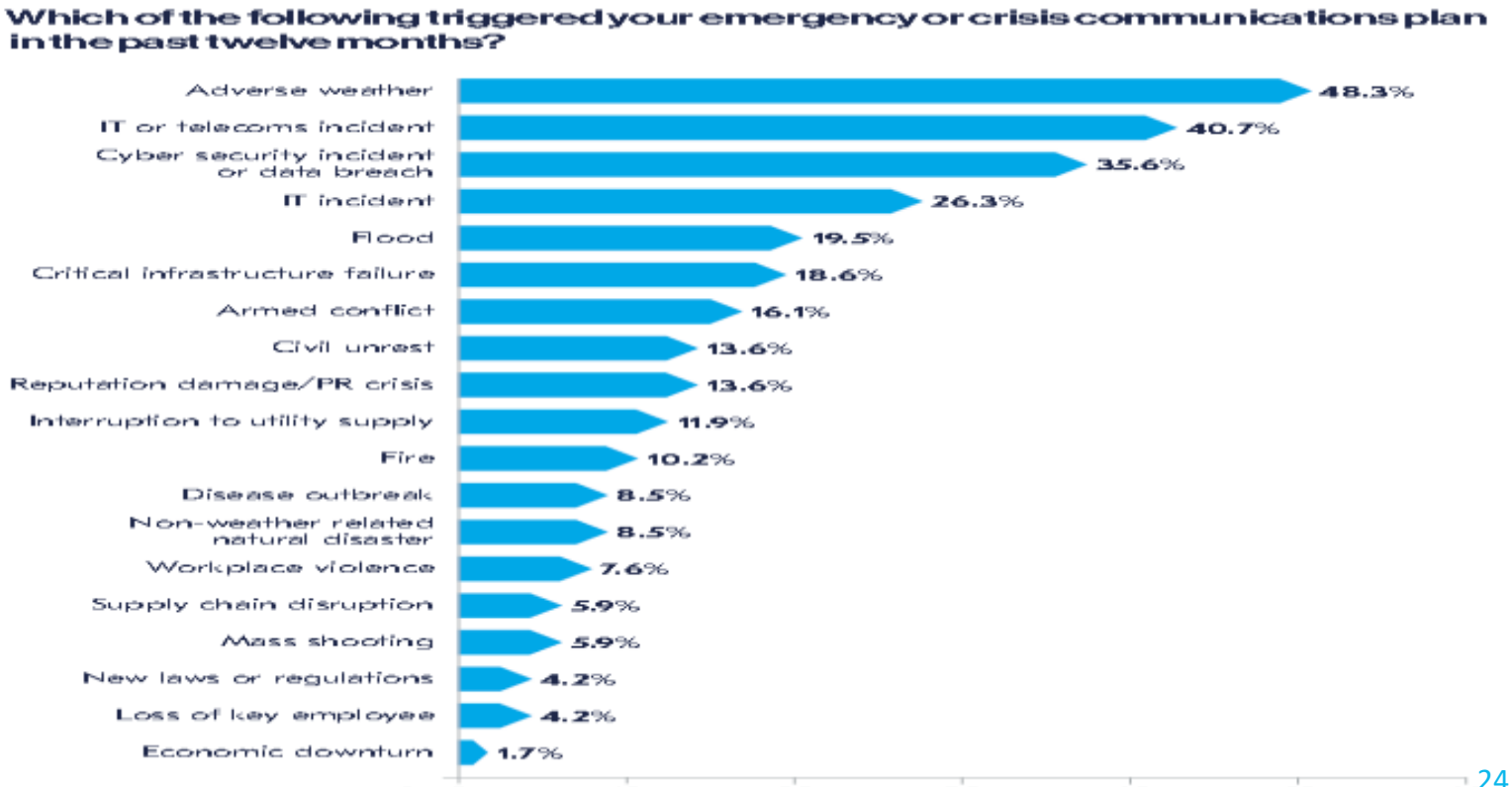
BCI Cyber-resilience report 2024

BCI Emergency & Crisis Communications Report 2024

Activation of emergency communication plan in organizations 2015-2024



BCI Emergency & Crisis Communications Report 2024



BCI Operational Resilience Report 2024

Does your organization have an operational resilience programme or project?

64.8%
Yes

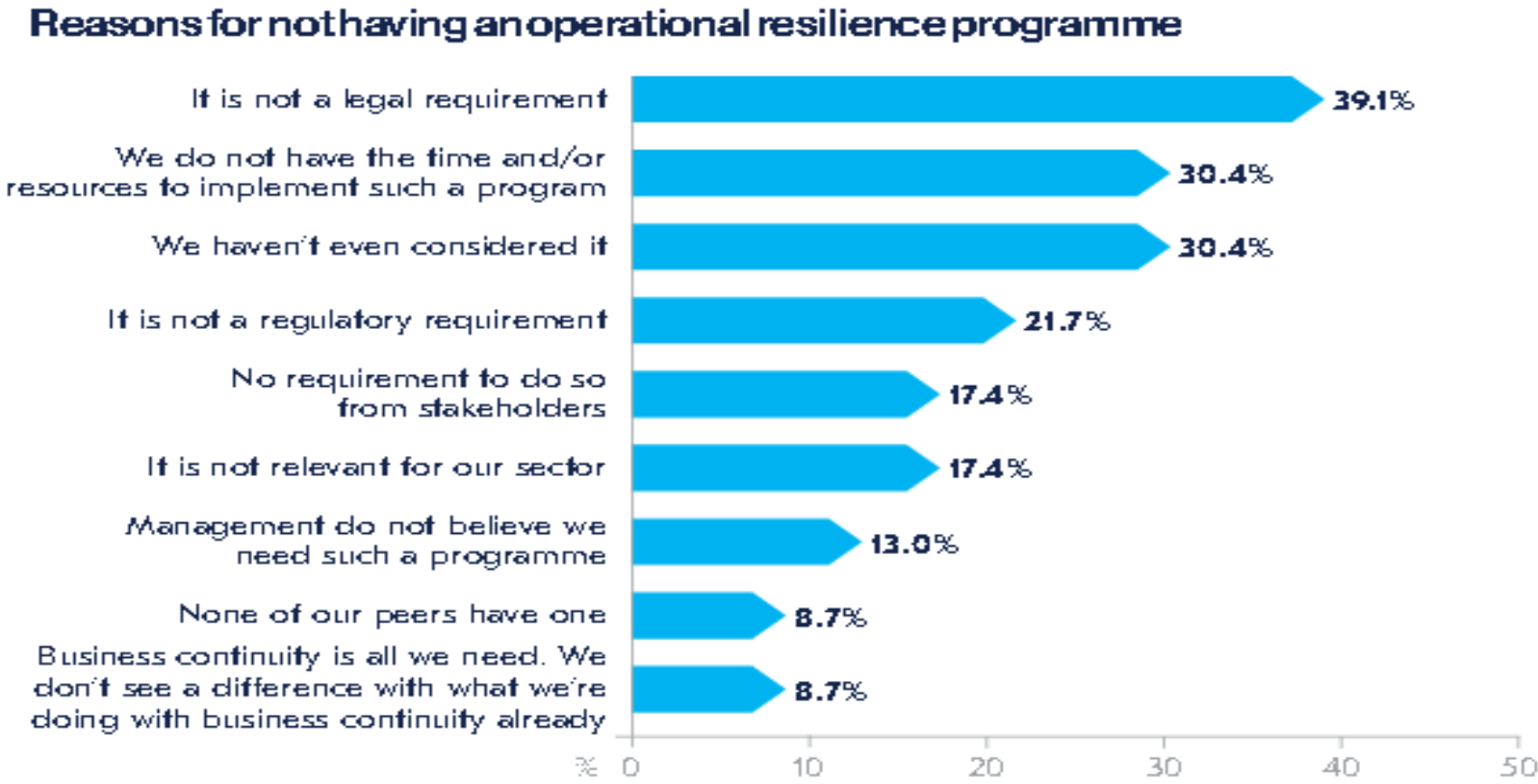
16.0%
We are in the process of developing one

8.8%
No

Top five reasons for the development of an operational resilience programme.

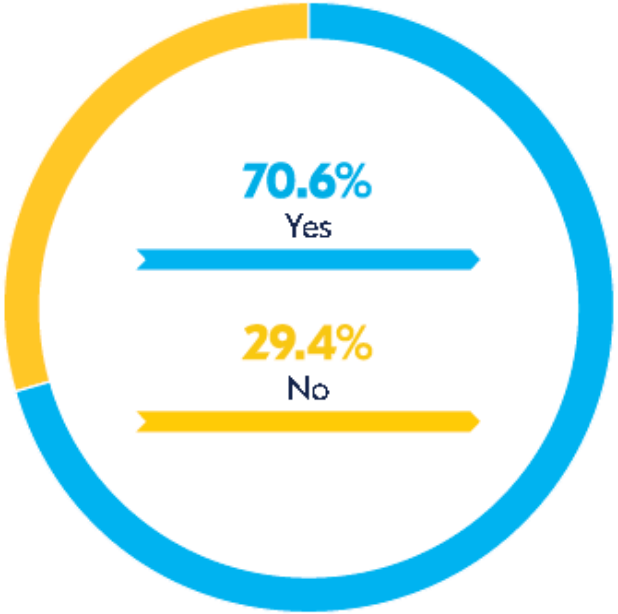
1. **67.0%** Regulatory requirement
2. **58.5%** For good practice purposes
3. **32.1%** Commercial and/or customer benefit
4. **32.1%** Industry requirement
5. **27.4%** To be prepared for incoming regulation

BCI Operational Resilience Report 2024



BCI Operational Resilience Report 2024

Do you have concerns that meeting regulatory requirements/laws will become a tick box exercise?



BCI Emergency & Crisis Communications Report 2024

Top four critically essential processes/tools within operational resilience

95.8%
Identifying Important Business Services (IBS)

88.3%
Identifying critical suppliers

83.2%
Prioritising and working vulnerabilities that threaten impact tolerances

81.7%
Establishing impact tolerances

BCI Emergency & Crisis Communications Report 2024

Top 5 major challenges of implementing operational resilience

58.2%
Embedding operational resilience into the fabric of the organization

50.5%
Not having the headcount and/or staff time to implement a realistic policy

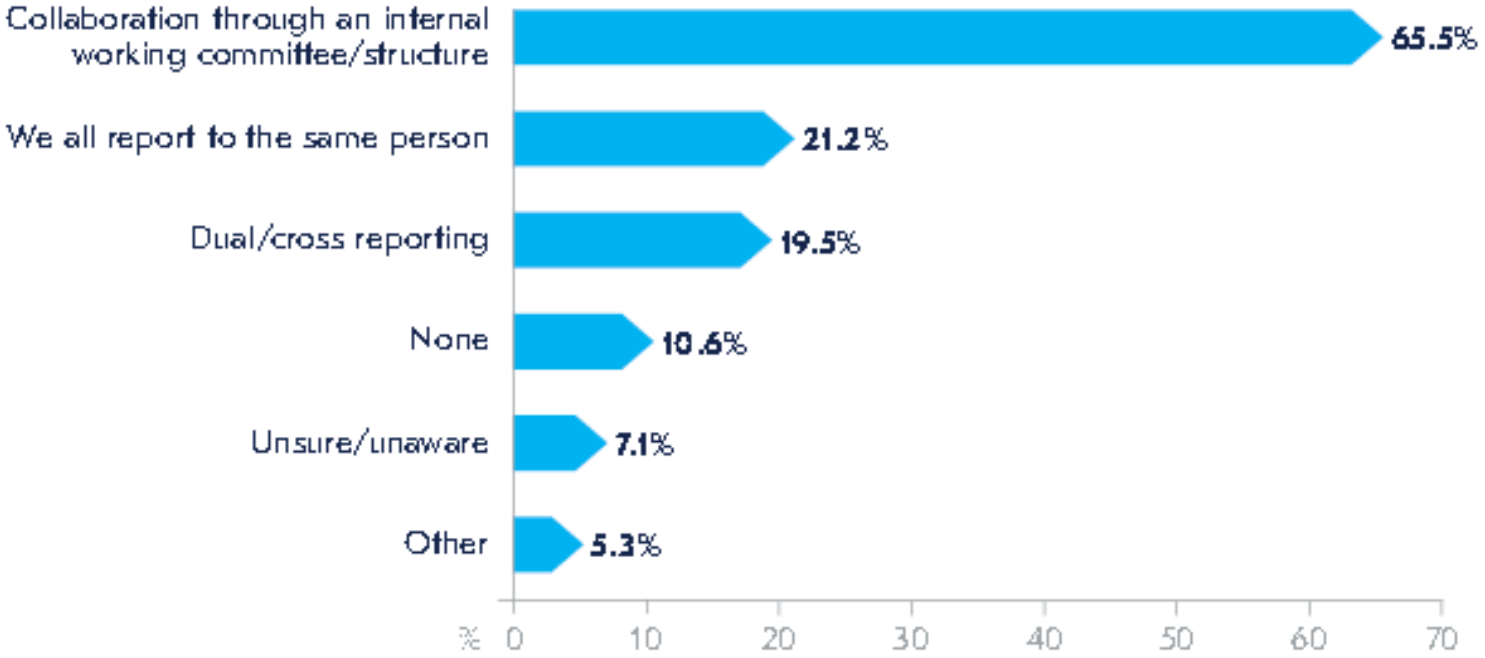
50.5%
Addressing legacy infrastructure

45.9%
Getting critical third-party suppliers to comply with regulations

42.4%
Understanding, monitoring and managing supply chain risks

BCI Operational Resilience Report

What has your organization done to bring together operational resilience and other related functions such as cyber or risk?



Conclusions

- Confusion: Business Continuity → Operational resilience (staff identique)
- Operational resilience:
    - **Préventif (protection, detection, …)**
    - **Réactif (curative, réparation, récupération et reprise des activités)**
- Motivations principales: meilleure cyber-protection (attaques tjrs en hausse) et obligations légales et régulatoires.
- 40% se reposent sur une police d'assurance.
- Beaucoup d'espoirs/d'attentes, mais peu de validations de récupérations.
- Testing à perfectionner (préventif et reprise des activités). L'assurance ne sauve personne.
- Les principaux défis: embarquer/intégrer dans la "chair" de l'entreprise; staffer correctement
- Crainte d'évolution vers une charge administrative sans valeur ajoutée.
- Efficacité en resilience opérationnelle / cyber-résilience = *Collaboration / intégration* transverse.

We are

SYNERGIT.BE

Christian.deboeck@synergit.be
+32 (0)475 26 26 39


bci
Leading the way
to resilience