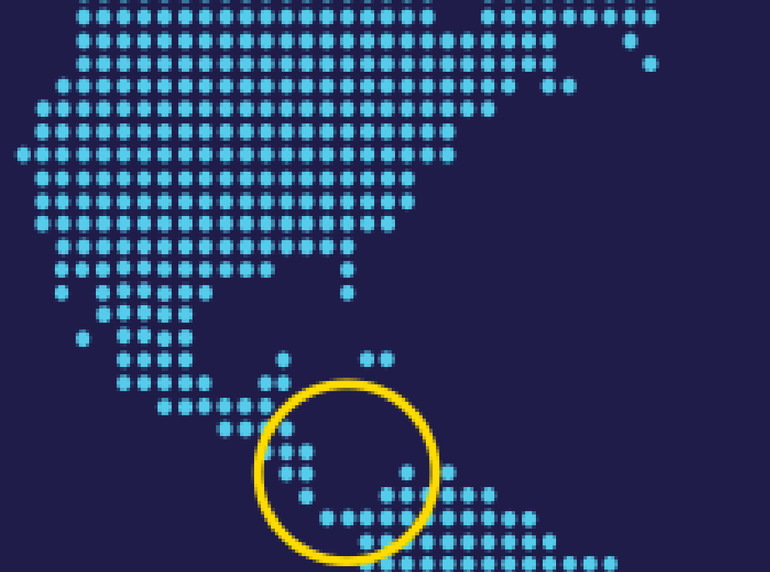
2023 CELAES
Congreso Latinoamericano de Seguridad Bancaria

Ciberresiliencia en un entorno cambiante

Supervivencia en un mundo digitalmente amenazado



ASOCIACION BANCARIA DE PANAMA
ABP

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

Agenda

- Continuidad vs Resiliencia
- Definiendo ciberresiliencia
- El entorno
- El desafio
- Un enfoque
- Un resultado

Continuidad vs Resiliencia

¿Hay debate?

ISO 22301 Continuidad del negocio : «la capacidad de una organización para continuar la entrega de productos y servicios dentro de marcos de tiempo aceptables a una capacidad predefinida durante una interrupción».

ISO 22316 Resiliencia del Negocio como « la capacidad de una organización para absorber los cambios del entorno y adaptarse a ellos, cumpliendo sus objetivos y sobreviviendo y prosperando».

Business Continuity Institute (BCI – UK) «La resiliencia operativa es solo la continuidad del negocio bien hecha»

Definiendo Resiliencia

Literalmente

resiliencia

Del ingl. *resilience*, y este der. del lat. *resiliens, -entis*, part. pres. act. de *resilīre* 'saltar hacia atrás, rebotar', 'replegarse'.

1. f. Capacidad de adaptación de un ser vivo frente a un agente perturbador o un estado o situación adversos.

2. f. Capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido.

REAL ACADEMIA ESPAÑOLA

Nuestra norma BS 65000 define la resiliencia organizacional como “la capacidad de una organización para anticipar, prepararse, responder y adaptarse al cambio exponencial y a las interrupciones repentinas para sobrevivir y prosperar”.

bsi.

Definiendo Resiliencia

Literally

noun: **resiliency**

1. the capacity to withstand or to recover quickly from difficulties; toughness.
   "the remarkable resilience of so many institutions"
2. the ability of a substance or object to spring back into shape; elasticity.
   "nylon is excellent in wearability and resilience"

Oxford Languages

What is the difference between resilience and resiliency?

Resilience and resiliency are different forms of the same word. Both nouns refer to the ability to recover quickly from illness or misfortune. But in today's English, resilience is far more common than resiliency, especially outside the U.S. and Canada.

Definiendo Resiliencia

No hay debate

La continuidad del negocio es la capacidad de una organización de seguir ofreciendo sus productos o servicios dentro de un período de tiempo aceptable después de una interrupción.

Por otro lado, la resiliencia organizacional es la capacidad de anticiparse, prepararse, responder y adaptarse a los cambios con el fin de sobrevivir y crecer.

Definiendo CiberResiliencia

¿Tampoco hay debate?

La **ciberresiliencia** (a veces denominada ciber resiliencia o resiliencia cibernética) describe la capacidad de un sistema u organización para resistir y/o recuperarse ante ataques o incidentes cibernéticos.

El concepto de **ciberresiliencia** aúna los planes de seguridad y las capacidades defensivas de una compañía para proteger sus sistemas e información con la salvaguarda de los intereses empresariales. De tal forma que, en caso de que se produzca un incidente de seguridad, la empresa pueda seguir operando de manera efectiva, evitando la parálisis y las consecuencias económicas y reputaciones derivadas de ella.

Definiendo CiberResiliencia

Tendencia clara

La ciberresiliencia es un concepto que engloba continuidad de negocio, seguridad de los sistemas de información y resiliencia de la organización. Es decir, se trata de un concepto que describe la capacidad de continuar generando los resultados previstos a pesar de experimentar sucesos cibernéticos complejos, como ciberataques, desastres naturales o recesiones económicas. En otras palabras, un nivel moderado de competencia en seguridad de la información y resiliencia influye en el grado de continuidad de las operaciones de negocio que una organización puede ofrecer con un tiempo de inactividad nulo o casi nulo.

IBM

cyber resiliency

Definitions:

The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

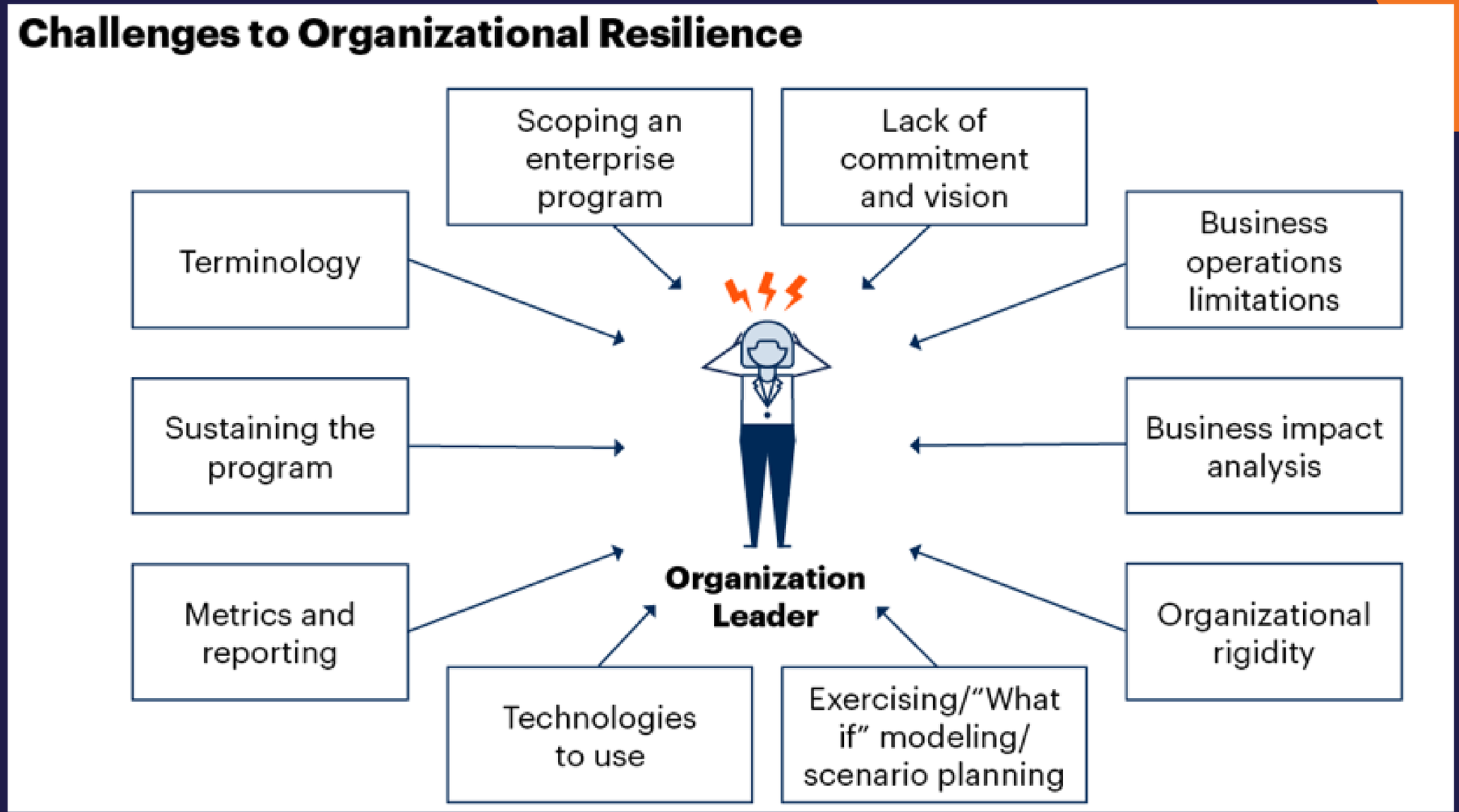
Sources:

NIST SP 800-172

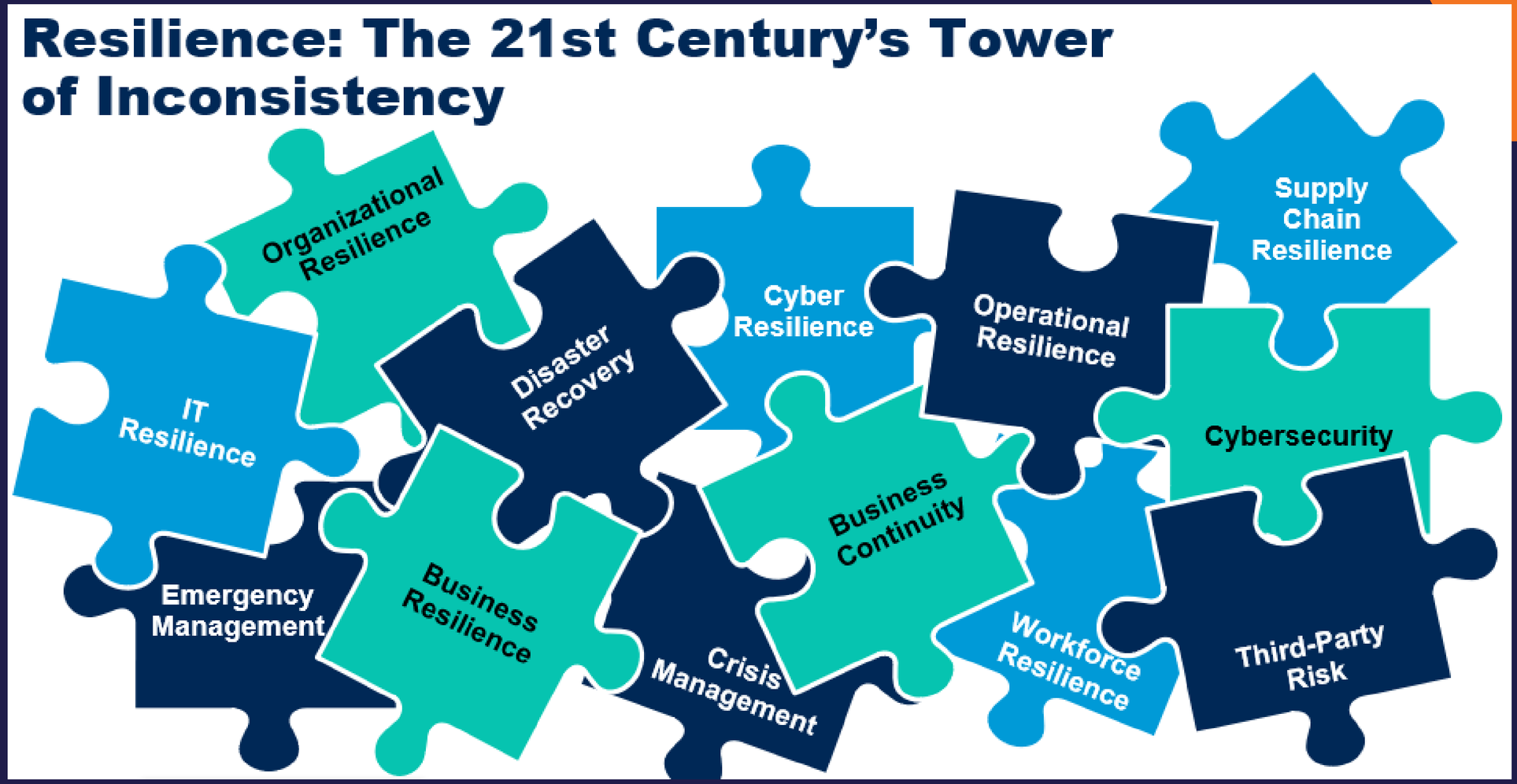
NIST COMPUTER SECURITY RESOURCE CENTER CSRC

2023 CELAES
Congreso Latinoamericano de Seguridad Bancaria

El Entorno



El “caos” del Entorno



El “caos” del Medio

Constant Emerging Threats

Compliance and Regulation

Increased Cyber Attacks and Service Disruptions/Failures

Reputation and Social Media

Increasingly Complex Operations

Maintain or Gain Competive Edge

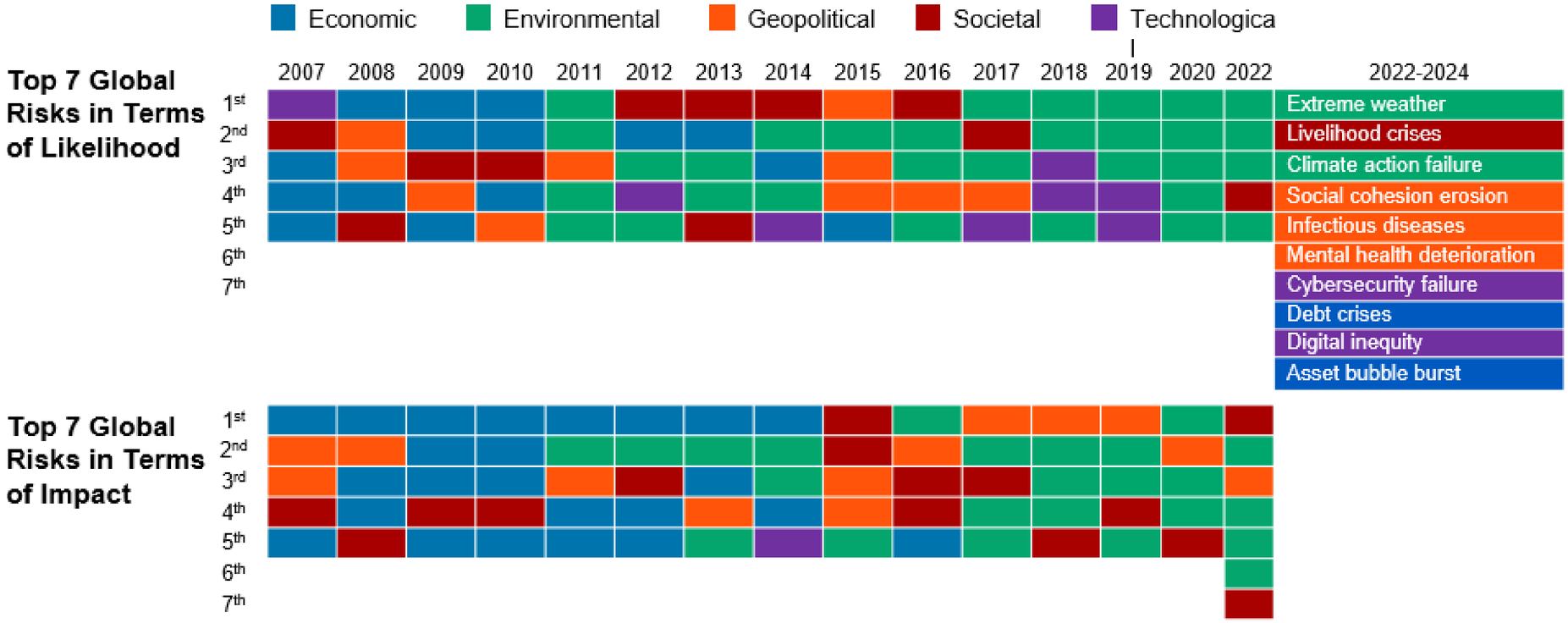
Increased Reliance on IT, Supply Chain, Service Providers

Pressure/ Expectations From Customers

2023 CELAES
Congreso Latinoamericano
de Seguridad Bancaria

El Entorno: sus amenazas

World Economic Forum: The Evolving Risks Landscape, 2007 to 2024



Source: World Economic Forum, The Global Risks Report 2022, Insight Report 16th Edition, In partnership with Marsh & McLennan, SK Group and Zurich Insurance Group

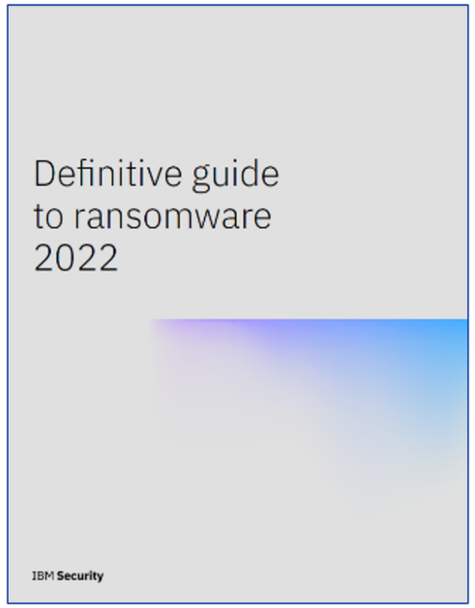
Gartner

2023 CELAES
Congreso Latinoamericano de Seguridad Bancaria

El Entorno: sus ciberamenazas

Data is under constant attack

Advanced threats like ransomware continue and drive the need for better data protection



$40M

Victimized companies pay as much as USD 40-80 million to have data released[1]

81%

of organizations are concerned about the risk of ransomware attacks[2]

86%

of organizations suffered at least one cyber attack in the preceding twelve months; an increase from 76% experienced in the prior year[3]

Ransomware RaaS

- Extracted/stolen critical data
- Locked/Encrypted critical data
- **Backdoor**

Failed Backups

- Infected **backups**
- Deleted files, Wipers
- DR tools – Not sufficient

Targeted Data Attacks

- Know where to cripple
- **Critical** component attacks
- Unknown attack vectors

1. IBM Definitive guide to ransomware 2022
2. Cybereason: Ransomware Research 2021
3. Global Report, Ransomware Trends, 2023 Veeam

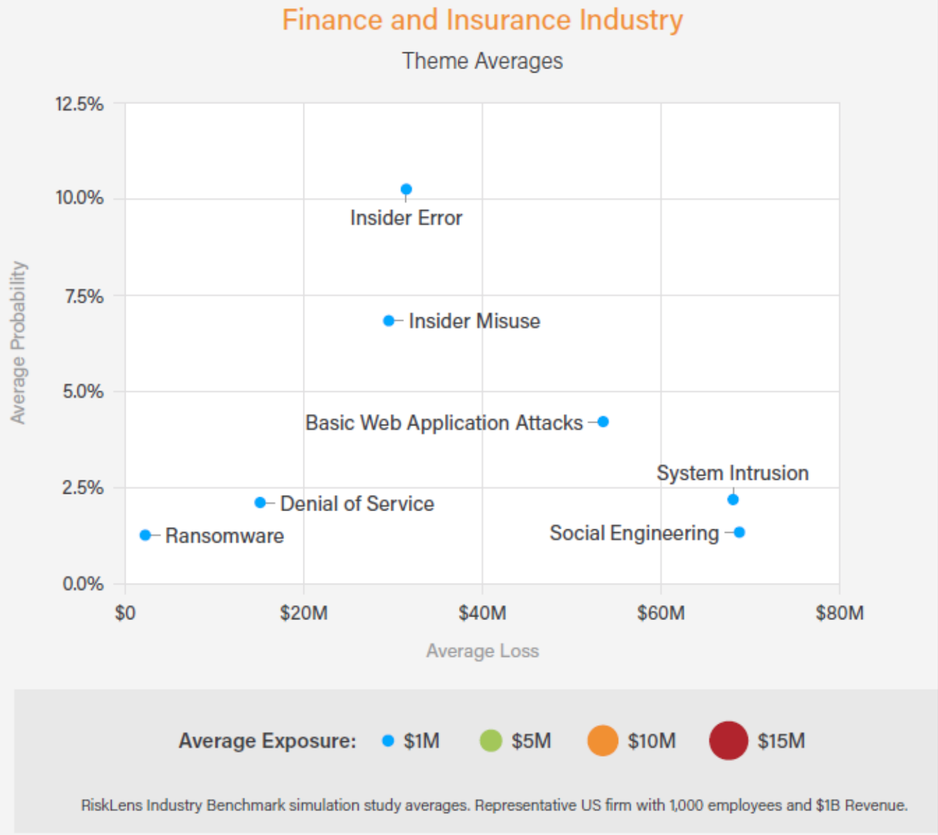
El Entorno: sus ciberamenazas

Finance and Insurance

This industry includes banks, insurers, lenders, investment companies and others involved in financial transactions.

Theme	Loss*	Probability	Exposure
Insider Error	$38.7M	10.4%	$4.5M
Basic Web Application Attacks	$58.7M	4.4%	$3.6M
Insider Misuse	$32.6M	7.0%	$2.4M
System Intrusion	$66.2M	2.1%	$1.9M
Social Engineering	$67.7M	1.6%	$1.7M
Denial of Service	$18.4M	2.1%	$399.9K
Ransomware	$1.1M	1.1%	$13.6K

*Exposure will not equal Probability x Loss due to probabilistic secondary losses.



2023 CELAES
Congreso Latinoamericano
de Seguridad Bancaria

El Entorno: reflexión

¿Porque la resiliencia es un imperativo estratégico?

¿Cómo cambia el escenario de la resiliencia?

Resiliencia

¿Cómo lograr la resiliencia operativa?

¿Cómo creo un marco de resiliencia para mi oprganizacion?

El desafío

1. Establish Organizational Resilience Responsibility, Governance and Accountability
2. Document Your Organizational Resilience Maturity
3. Develop Your Organizational Resilience Program for Where You Want to Be in X Years
4. Establish Risk Mitigation Strategies/ Corrective Actions
5. Develop Organizational Resilience Metrics and Track Progress to Improve Maturity

El desafío: regulatorio?

Organizational/Operational Resilience

- ISO 22316:2017 - Security and resilience — Organizational resilience — Principles and attributes
- Financial Conduct Authority (FCA), Prudential Regulation Authority (PRA), Bank of England (BOE) Operational Resilience
- Federal Reserve, Office of Comptroller, FDIC Interagency Paper – Strengthening Operational Resilience
- FFIEC Operational Resilience
- Digital Operational Resilience Act (DORA)
- APRA Prudential Standard CPS 230 Operational Risk Management
- Office of the Superintendent of Financial Institutions (OSFI): Operational Risk and Resilience
- Basel Committee on Banking Supervision (BCBS): Principles of Operational Resilience
- Vendor & Consulting Services specific frameworks, e.g., PwC, Fusion Risk Management, Protiviti, i3 Australia, ServiceNow, ICOR Organizational Resilience Framework, Carnegie Mellon CERT Resilience Management Model (CERT-RMM)

Business Continuity/Disaster Recovery

- ISO 22301:2019 – Business continuity management systems – Reqs
- ISO 22317- Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)
- ISO 22313 - Security and resilience — business continuity management systems — Guidance on the use of ISO 22301
- ISO 22330 - Security and resilience — Business continuity management systems — Guidelines for people aspects of business continuity
- ISO 27031:2011 Information technology – Guidelines for info & communication technology (ITC) readiness for business continuity
- FFIEC: Business Continuity Management Handbook (Financial Services)
- NIST SP 800-34 – Contingency Planning Guide for Federal Information Systems
- Appendix D: Mandatory Procedures for Business Continuity Management Control (Directive on Security Management)
- NFPA 1600 Standard on Continuity, Emergency, and Crisis Management
- UAE NCEMA7000 Business Continuity Management Standard
- (FS) Saudi Arabian Monetary Authority (SAMA) Business Continuity Management Framework
- BCI: Good Practices Guidelines – Business Continuity
- DRII: Business Continuity Management Professional Practices

Cybersecurity

- NIST SP 800-160 – Developing Cyber Resilient Systems: A Systems Security Engineering Approach
- NIST CyberSecurity Framework (CSF)
- U.S. Cybersecurity Maturity Model CMMC
- Directive on Security Management
- (FS) Monetary Authority of Singapore (MAS) Notice 655 Cyber Hygiene
- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)
- Cyber Resilience Act (CRA) – rules to ensure secure hardware/software products

Crisis/Emergency Management

- U.S. FEMA NIMS/ICS
- ISO 22320:2018 - Security and resilience - Emergency management - Guidelines for incident management
- ISO 22396:2018 – Security and resilience – Community resilience – Guidelines for supporting vulnerable persons in an emergency
- ISO 22361:2022 - Security and resilience — Crisis management — Guidelines to help any organization identify and manage a crisis
- UAE National Emergency and Crisis Management Framework

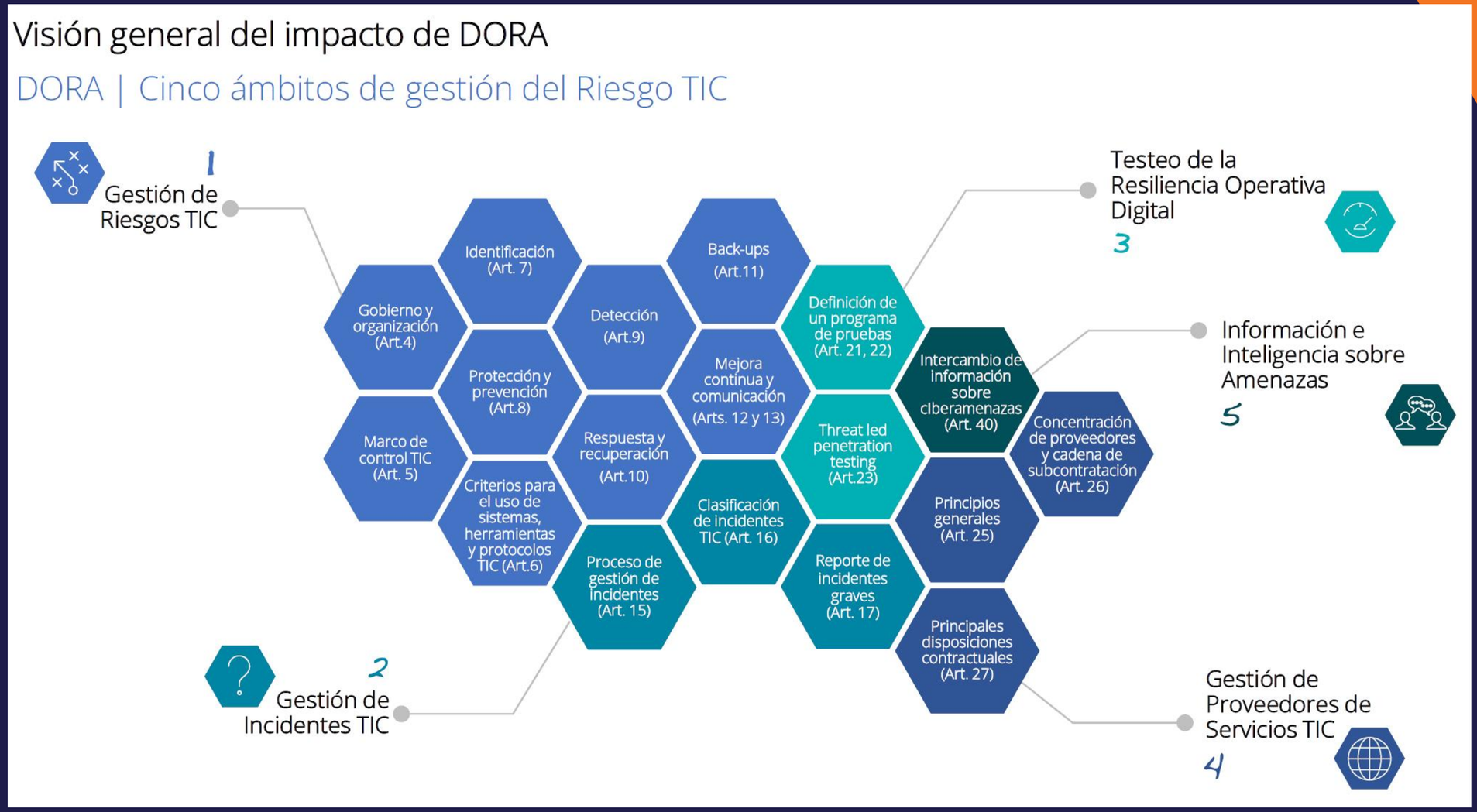
Supply Chain/Third-Party Risk Management

- ISO 22318 – Societal security — Business continuity management systems — Guidelines for supply chain continuity
- (FS) PRA: Outsourcing and Third-Party Risk Management
- Office of the Superintendent of Financial Institutions (OSFI) Guideline B-10 Third Party Risk Management
- EBA: Guidelines on ICT and Security Risk Management (FS)
- EBA: Guidelines on Outsourcing Arrangements (FS)
- ECB: Cyber Resilience Oversight Expectations for Financial Market Infrastructure (FS)
- ECB: TIBER-EU Testing Framework (FS)
- Financial Stability Board (FSB): Effective Practices for Cyber Incident Response and Recovery (FS)
- ENISA: Cyber-Security Certification Framework

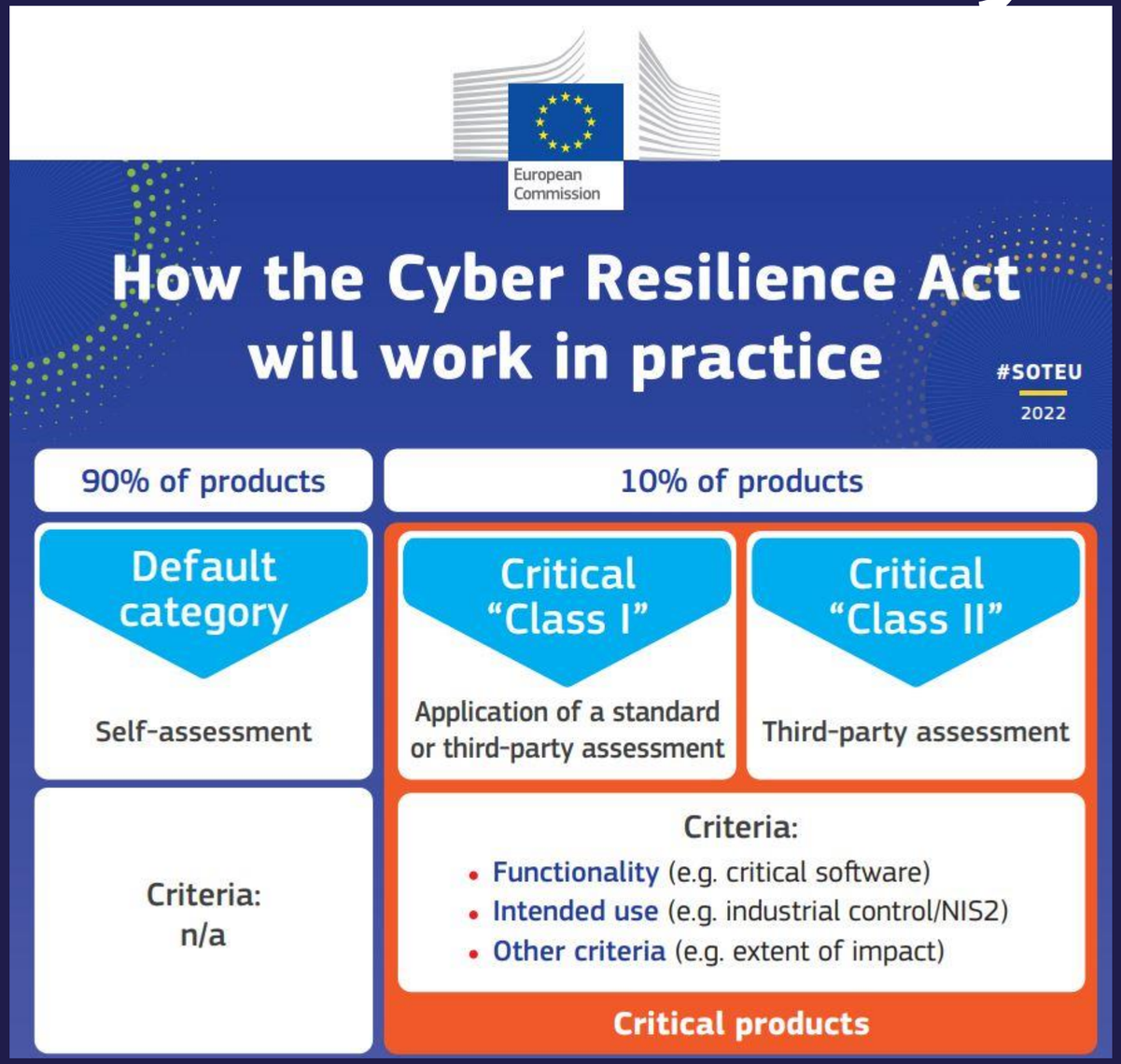
Gartner

ELAES
Congreso Latinoamericano de Seguridad Bancaria

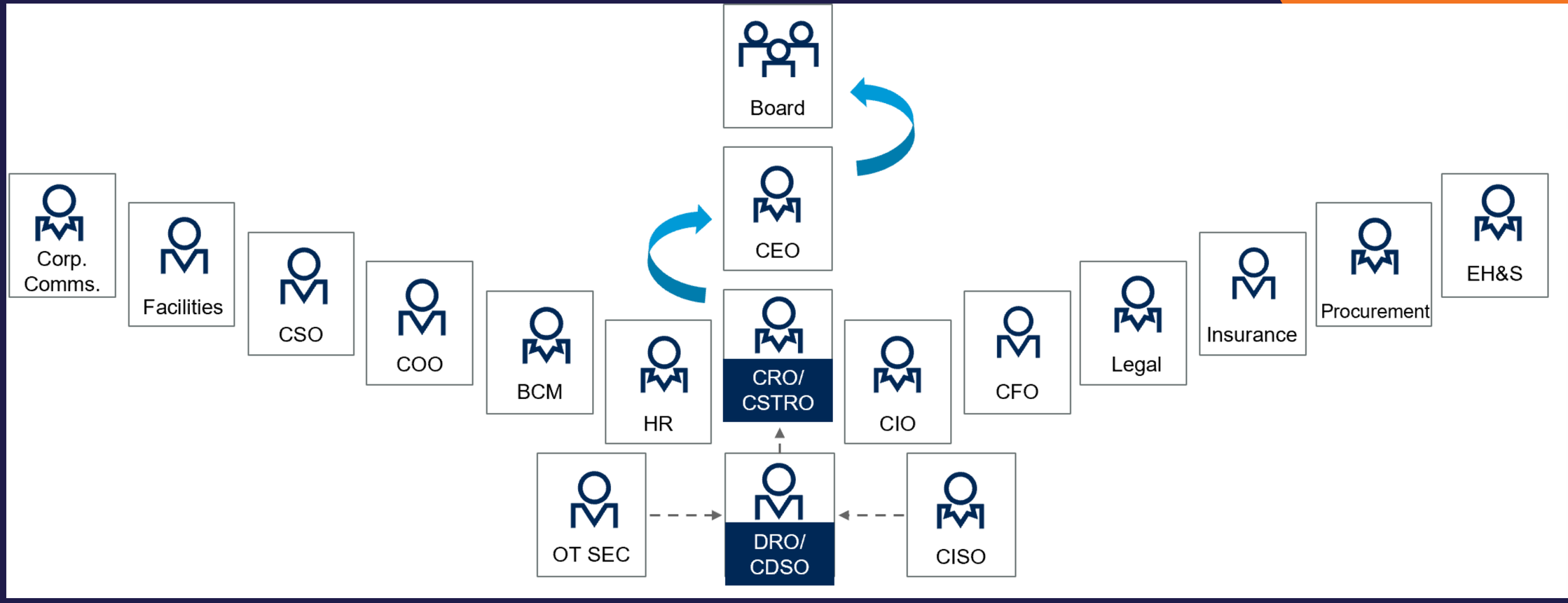
El desafío: UE DORA



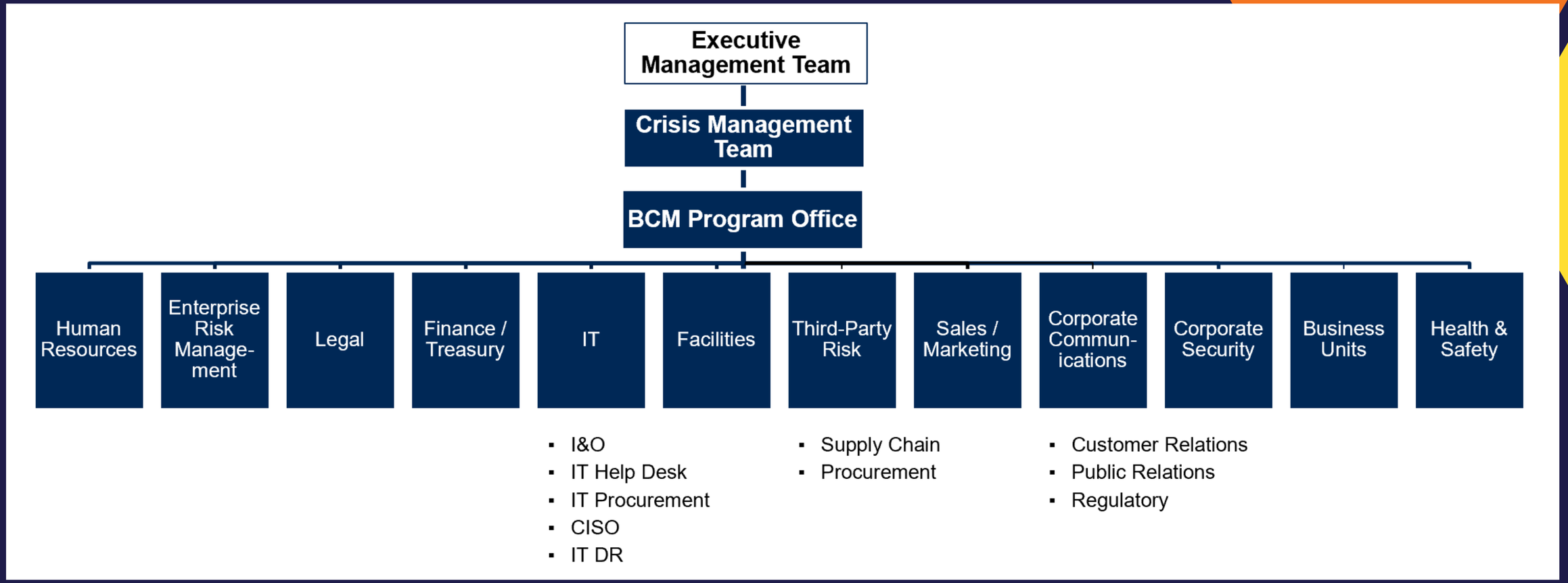
El desafío: UE Cyber Res Act



Un enfoque: hands on (who)

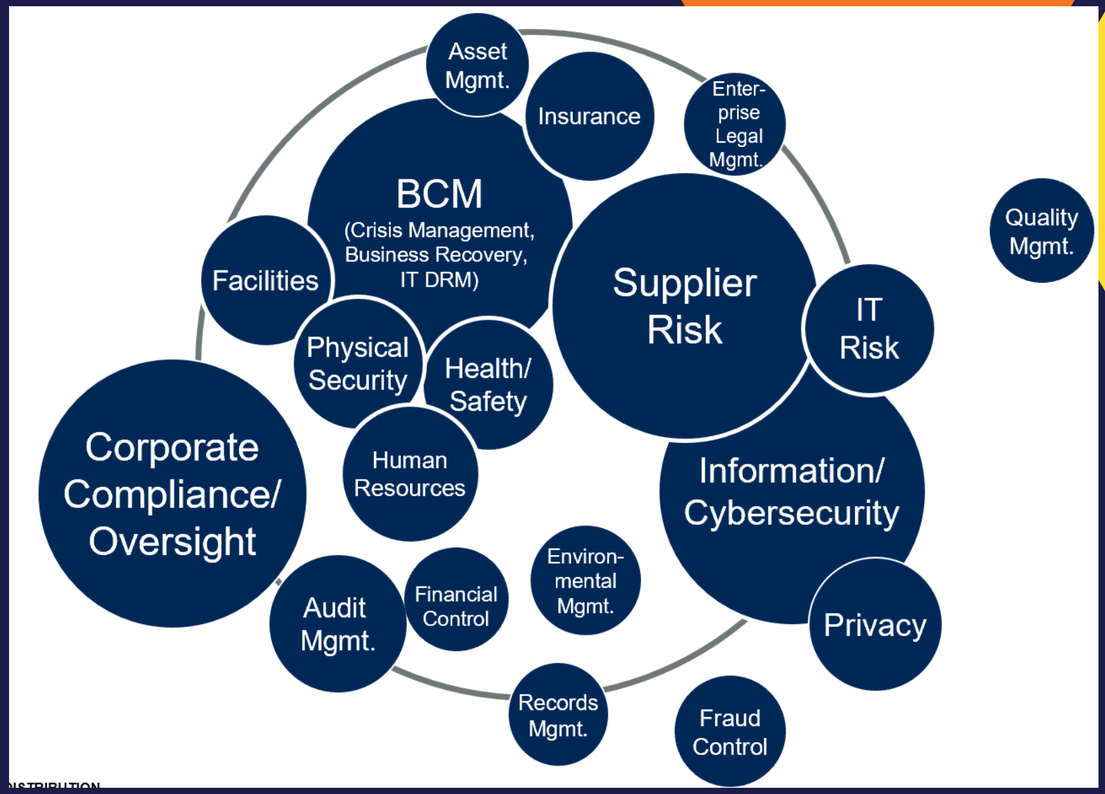


Un enfoque: hands on (where)

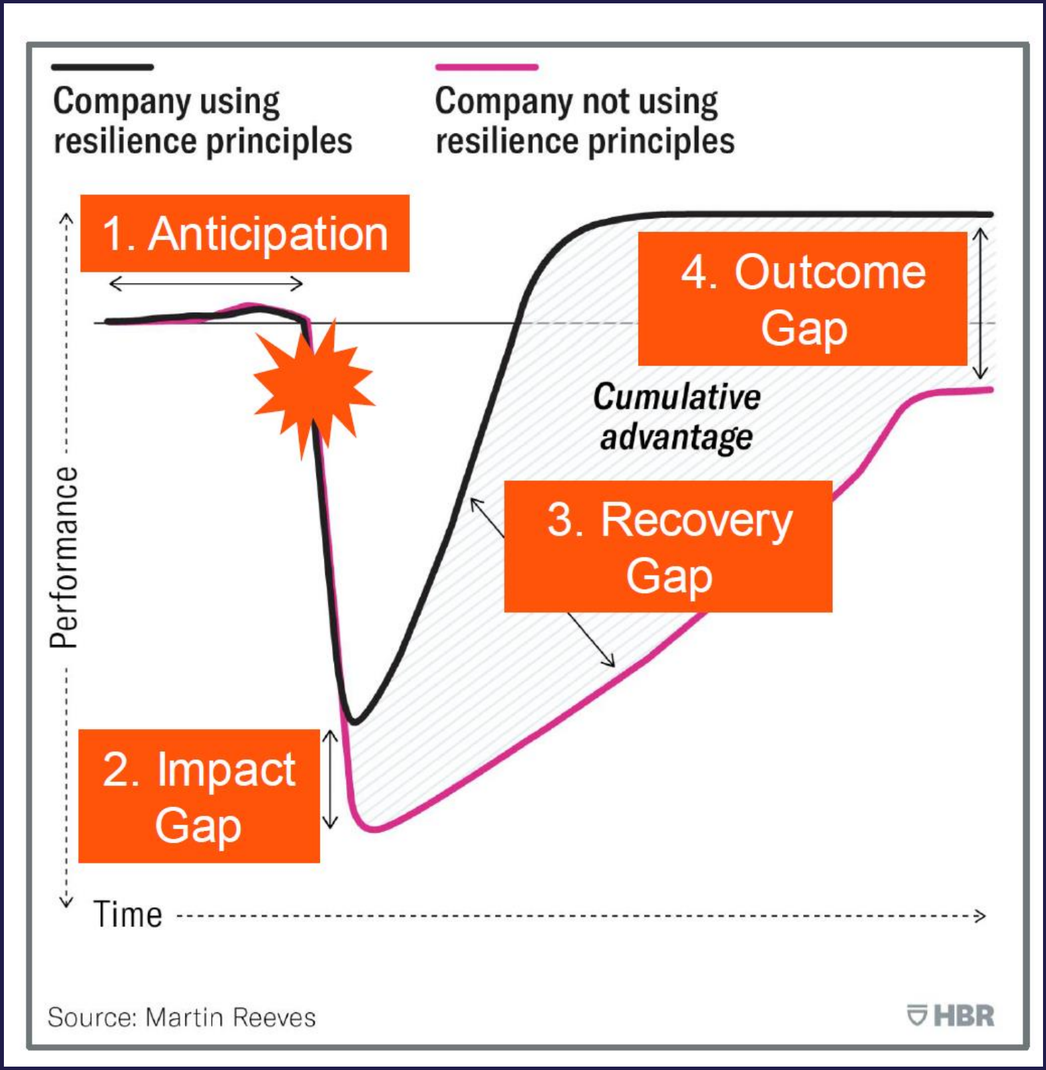


Un enfoque: hands on (how)

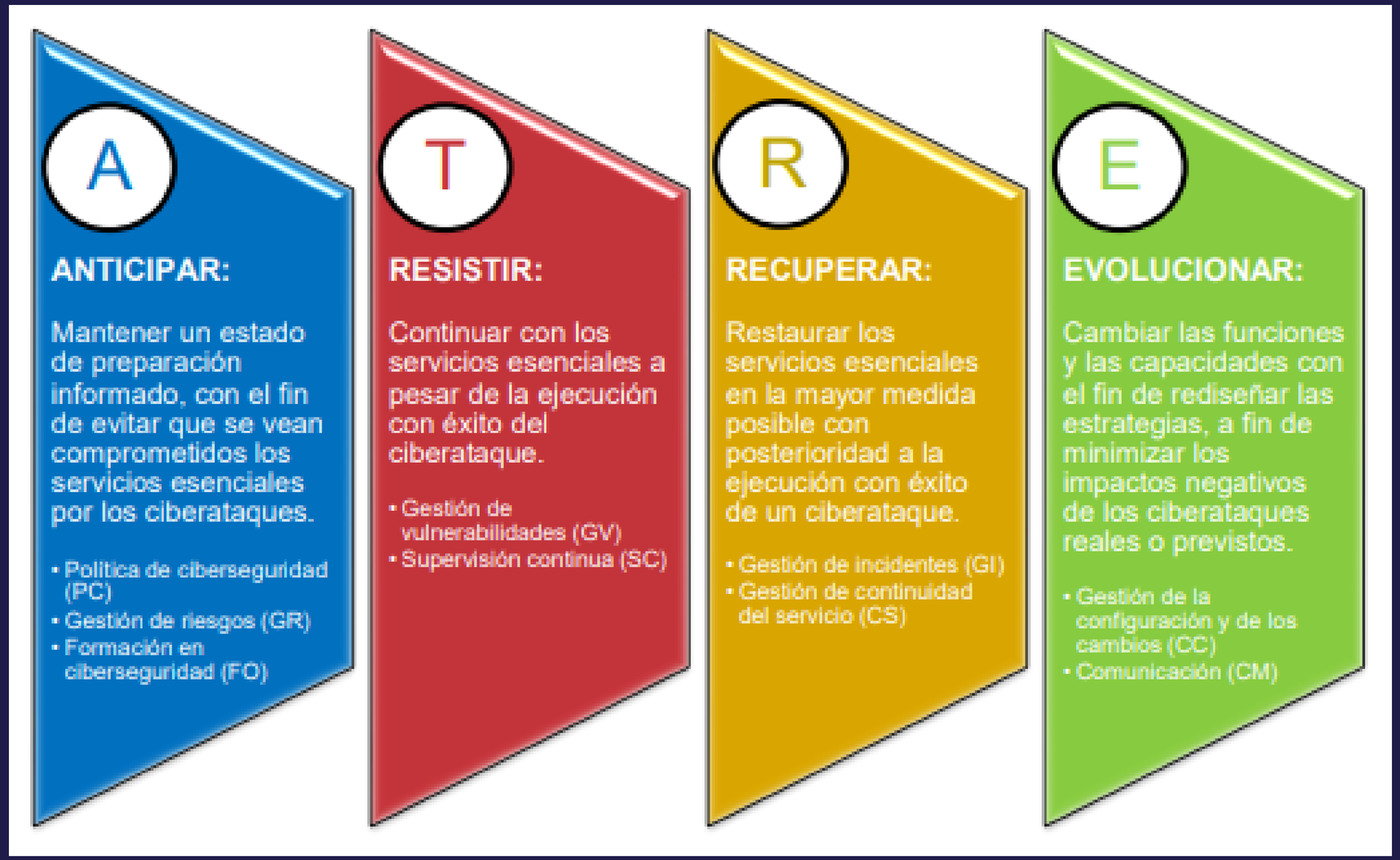
Business Domain	At Risk	Effective	Resilient
Strategy / Business Model			
Current State			
Future State			
Leadership			
Current State			
Future State			
Culture			
Current State			
Future State			
Workforce			
Current State			
Future State			
Business Process			
Current State			
Future State			
IT			
Current State			
Future State			
Facilities			
Current State			
Future State			
Third Parties / Supply Chain			
Current State			
Future State			



Un resultado: mitigar



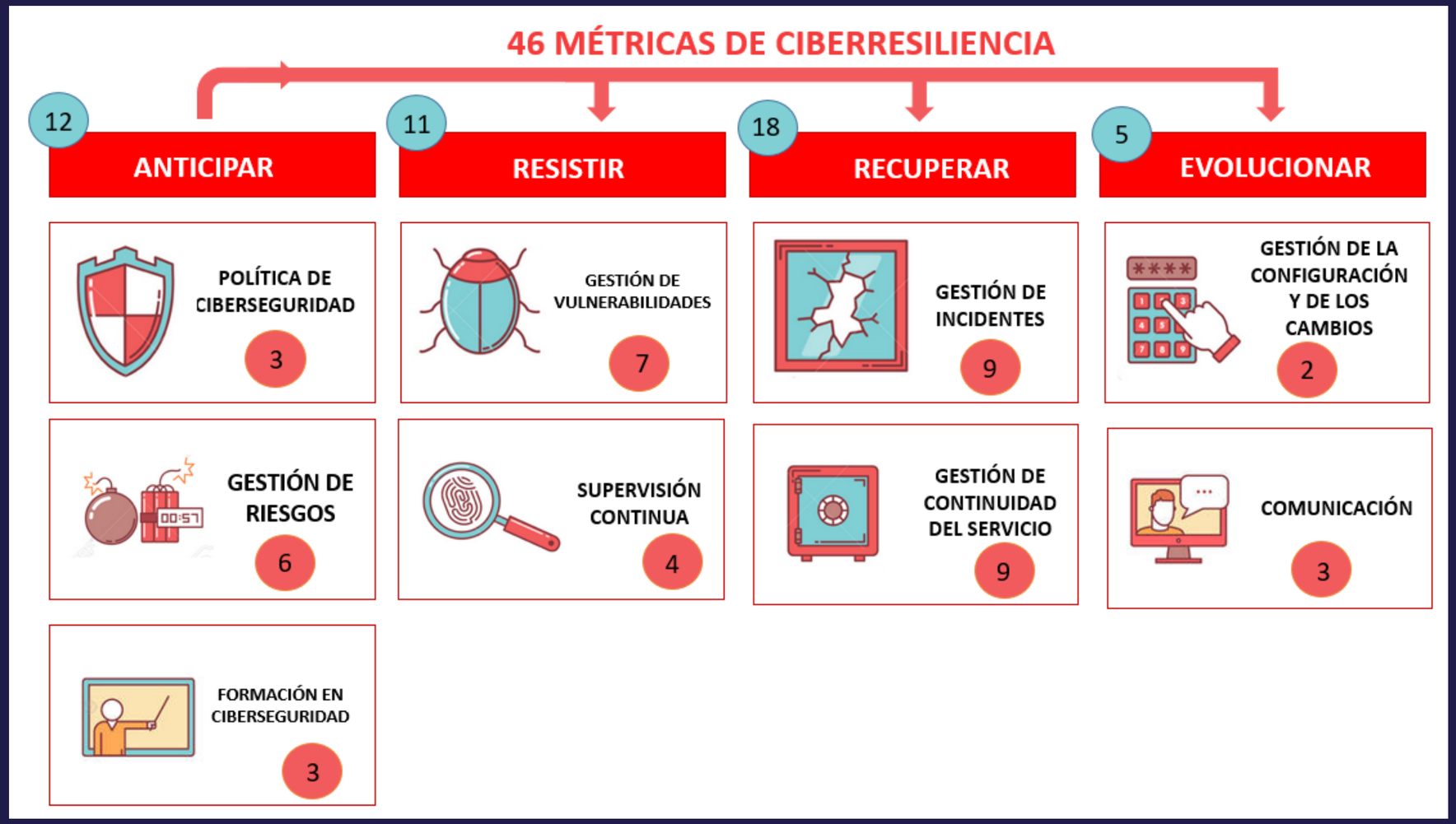
Un resultado: proceso



incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

2023 CELAES
Congreso Latinoamericano
de Seguridad Bancaria

Un resultado: medir



MITRE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

El modelo IMC, basado entre otros en el marco de indicadores de ciberresiliencia **del MITRE**, escoge 46 indicadores para representar los distintos aspectos de la ciberresiliencia. Estos servirán para obtener una visión de las cuatro metas de la ciberresiliencia

Ciberresiliencia: ransomware

IT Resilience and Cybersecurity Resilience: Ransomware

Recovering from a ransomware attack is different than traditional disaster recovery

DR vs. Ransomware Recovery

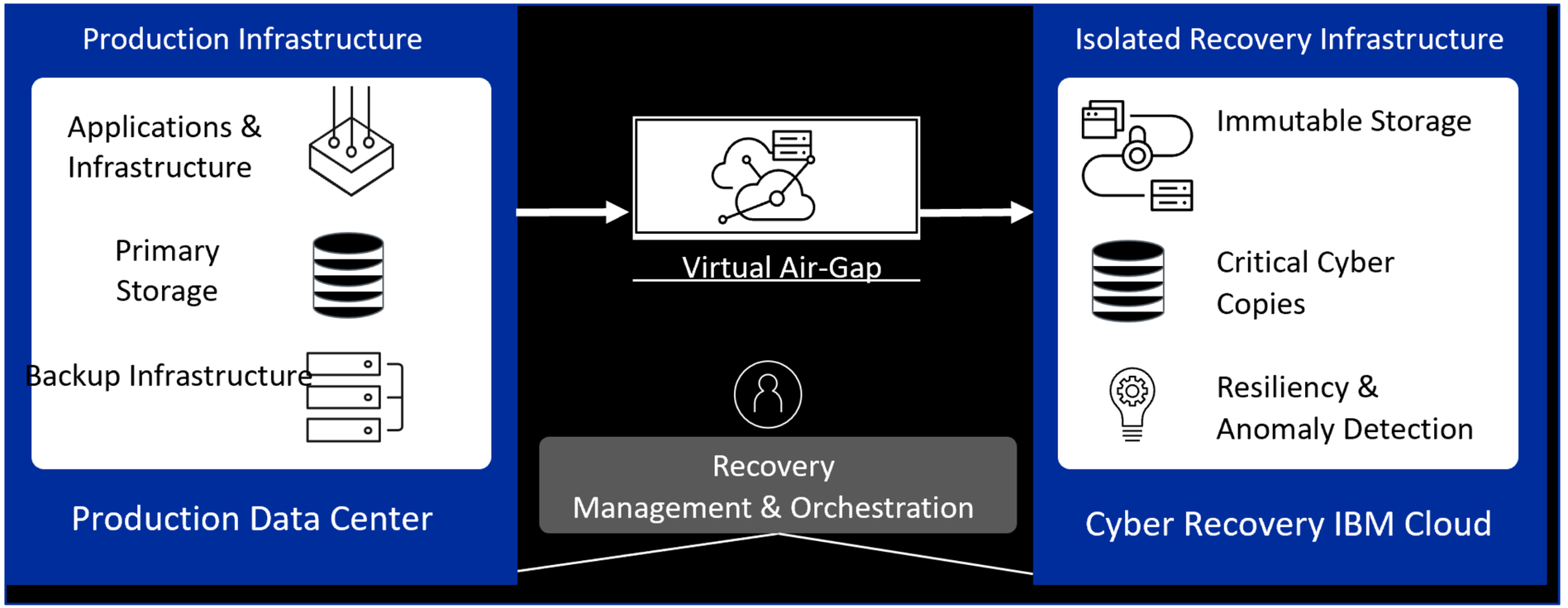
- Meeting RTO/RPOs are most likely not achievable.
- Recovery timeline will be prolonged due to the need to first determine the extent of the damage and what the “go forward” plan will be.
- DR and cybersecurity teams cannot act alone.
- DR is typically IT’s decision versus ransomware where the entire enterprise must be involved.

Ransomware Recovery Best Practices

- Obtain enterprise agreement on what business functions and resources are critical.
- Educate businesses about missed RTOs and RPOs.
- Backup data to an immutable vault.
- Establish an isolated recovery environment and test it.
- Design recovery for every layer of the application and infrastructure.
- Develop a ransomware recovery plan.
- Conduct cross-functional tabletop exercises with all key stakeholders.

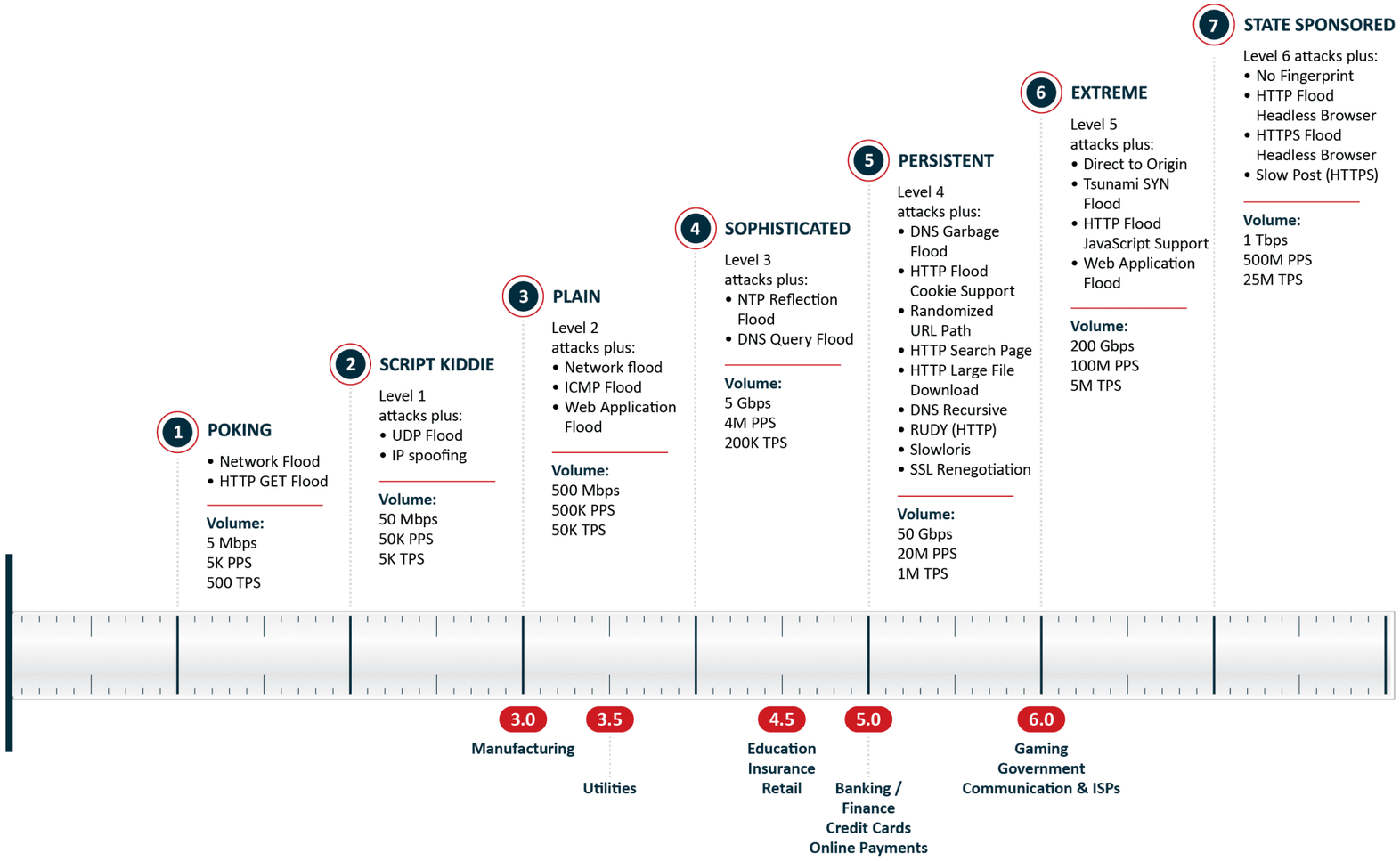
Gartner

Ciberresiliencia: ejemplos



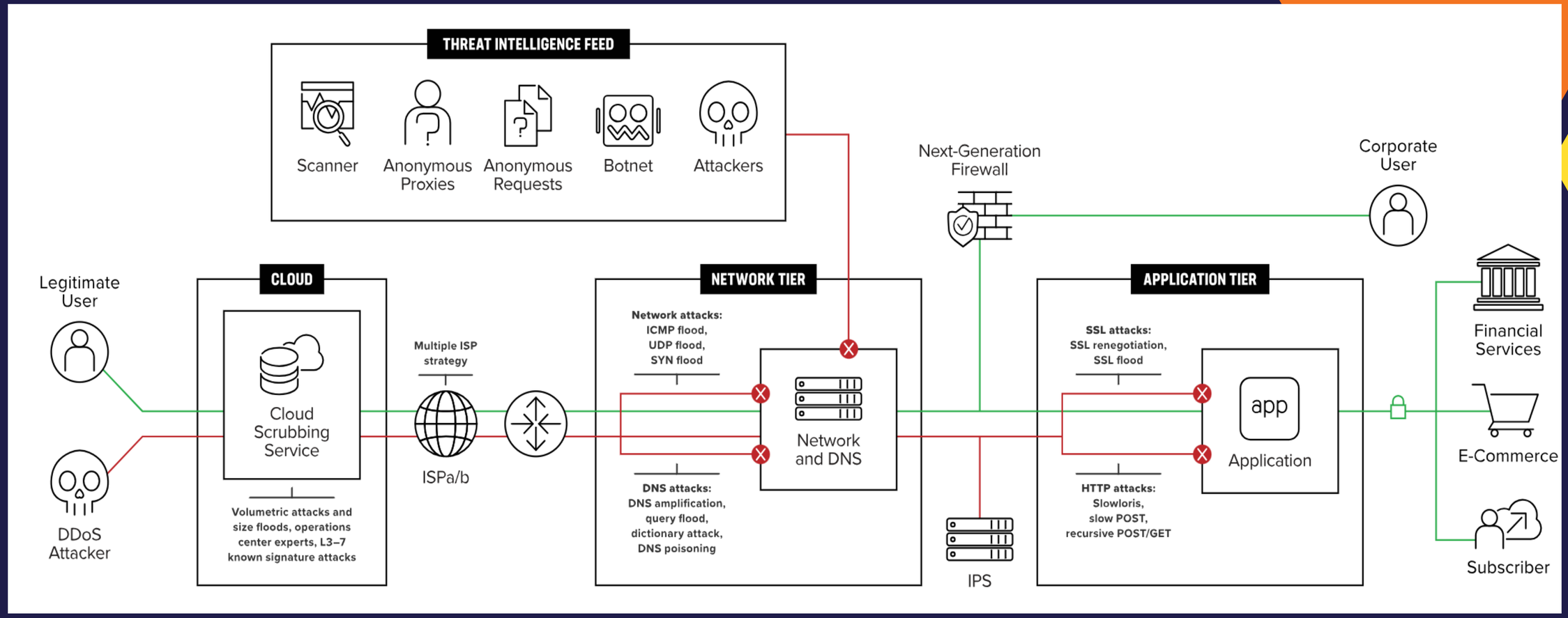
Delivering engineered automation, air-gapped protection, immutable storage, rapid isolated recovery of applications, and ransomware protection

Ciberresiliencia: DDoS



CELAES 2023
Congreso Latinoamericano de Seguridad Bancaria

Ciberresiliencia: ejemplos



Gracias por su resiliente atención.

CELAES 2023
Congreso Latinoamericano
de Seguridad Bancaria