



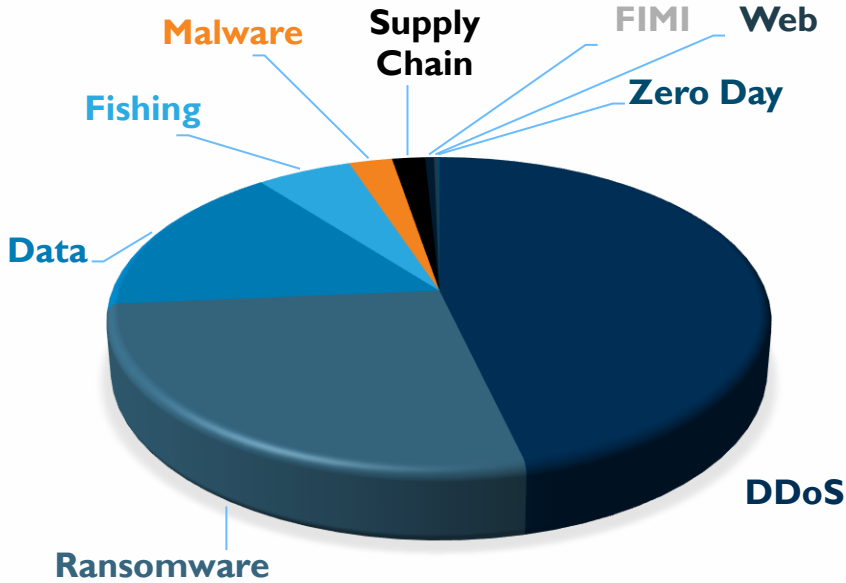
# Cyber Fusion Center as a Shield for Your Business Resilience

---

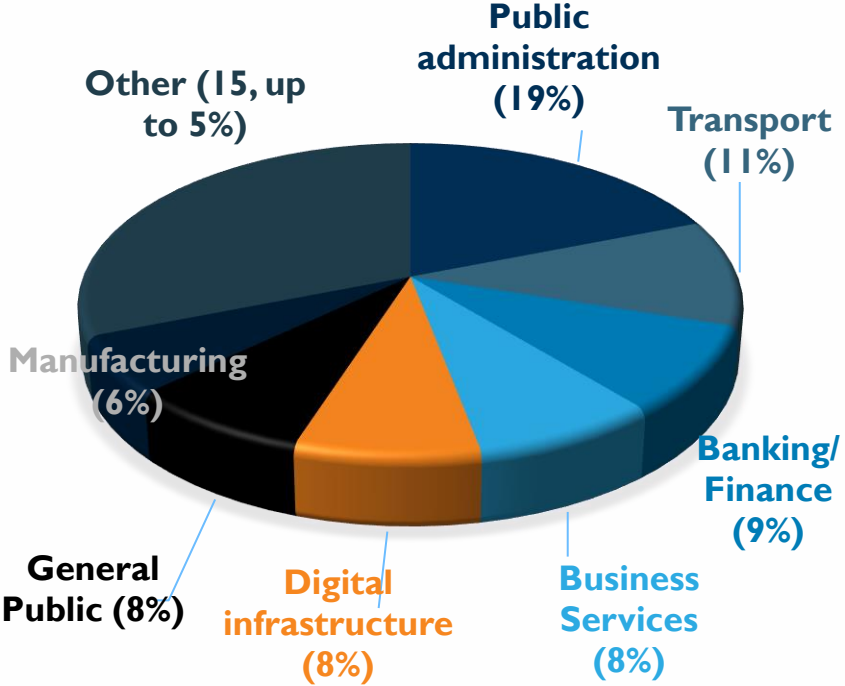
dr. Dovilė Kėrienė

- Threats against availability (DDoS)
- Ransomware
- Threats against data
- Social Engineering
- Malware
- Information manipulation

### THREATS, %



### INCIDENTS, %



Motivation – financial gain, espionage, destruction, ideological

- **Ignitis On** – hybrid attack, **supply chain** incident
- **KTU** – ransomware, data loss

## DDoS

- **Vilnius District Municipality** – DDoS, possibly data leak
- **General Jonas Žemaitis Military Academy of Lithuania** – Moodle system broken authentication

## Ransomware

- **Aibės** – phishing, broken authentication
- **VDU** – phishing, data leak

## Fishing

- **CPVA** – fishing, broken authentication, mail storming
- **Verslo žinios** – fishing, broken authentication, mail storming

## Broken access

- **Schools and kinder garden „bombing“** – hybrid attack, mail storming
- **Tamo** – mail storming, data leak, DDoS



96% – cybersecurity is critical to organizational growth and stability

74% – concerned about their organizations' business continuity

60% – organizations don't include cybersecurity into business strategies

44% – cybersecurity requires episodic intervention rather than ongoing attention

54% – the cost of implementing cybersecurity is higher than the cost of suffering a cyberattack

90% – cybersecurity is a differentiating factor helping them build customer trust

Only 15% have dedicated board meetings for discussing cybersecurity issues

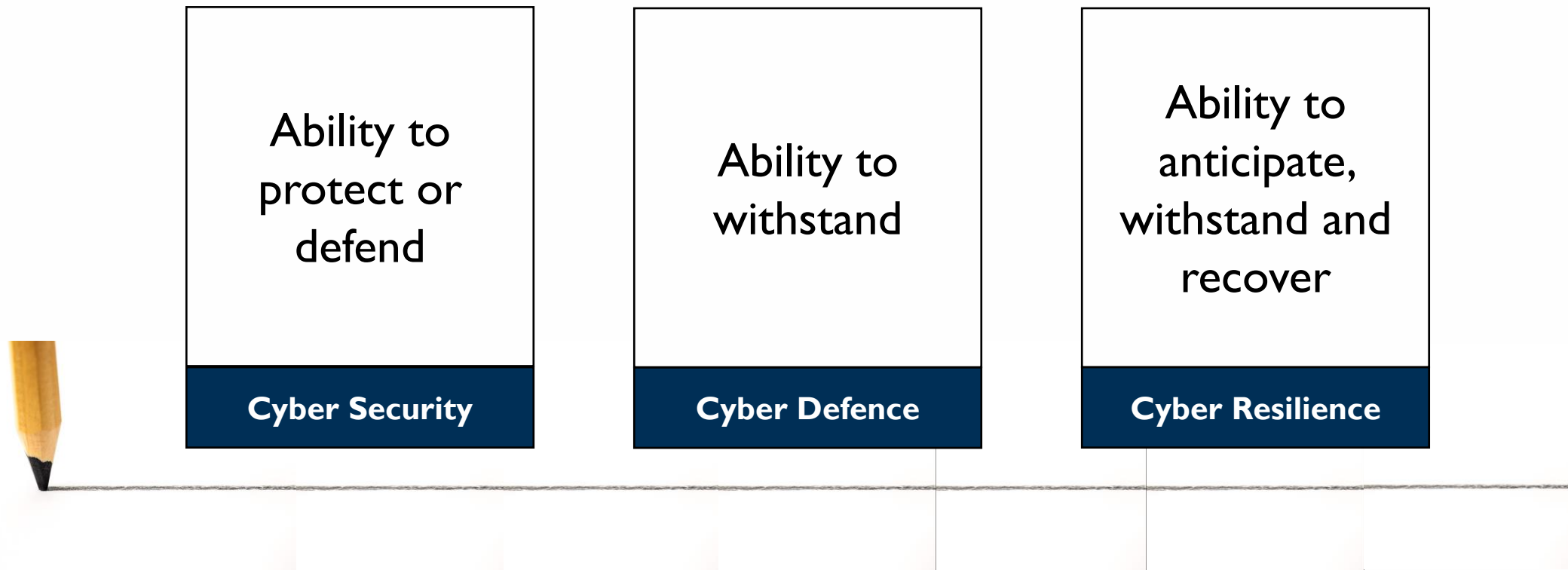
Finally - 91% said cybersecurity is a technical function that is the responsibility of the **CIO** or **CISO**

And **ONLY 5%** excel at cyber resilience \*

\*Accenture research

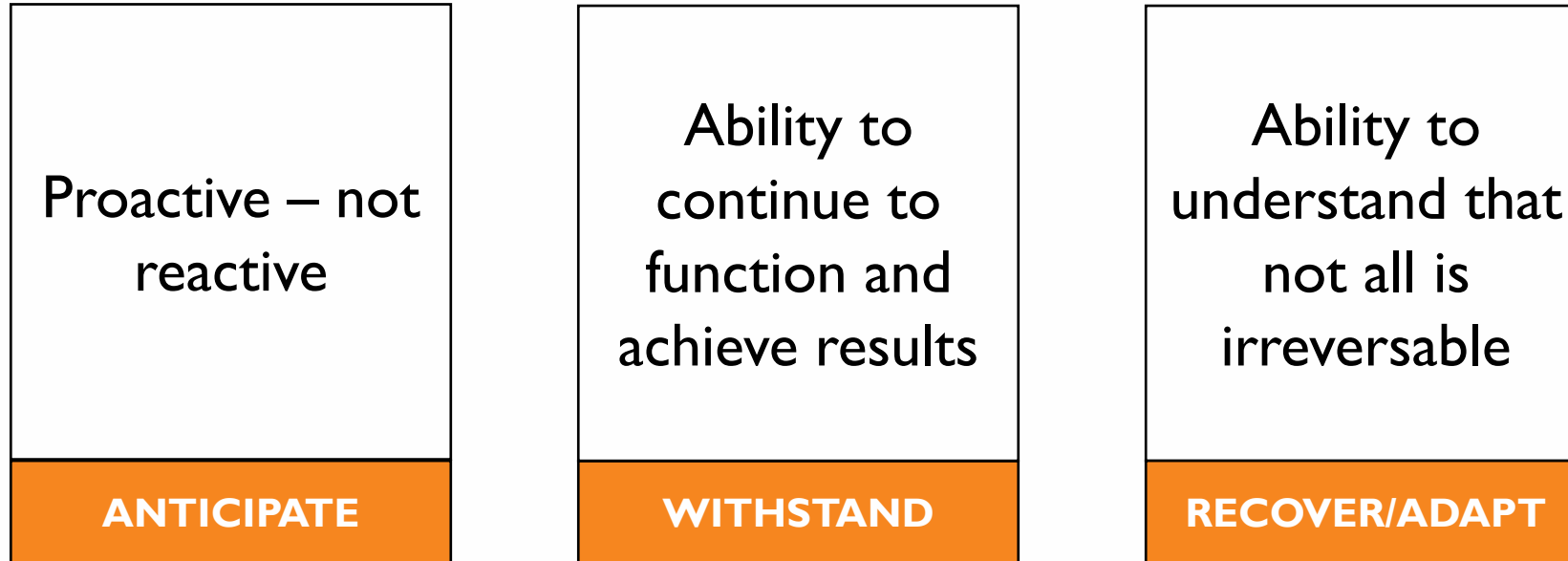
**What keeps the CEO up at night is different from what's causing the CFO to lose sleep...**

Resilience the capacity, not only to survive, but to continue operating through and recover from difficulties



\* According to NIST glossary

**Confidence conquers doubt.**



Cyber Security programs are not only about the process, but also about the **outcomes**.

Cyber **security** and cyber **defence** are essential components of organisations overall security posture.

The distinction is in their **focus**, **approach** and **outcomes**.

**Hope isn't a strategy! We must expect and prepare for the worst.**

## Why business resilience **needed**:

- Surviving and thriving beyond disaster recovery
- Competitive advantage in a turbulent world
- The assurance of business continuity
- Proactive risk management
- Crisis management in real-time
- Cyber resilience in a digital age
- Resilience across supply chain



## Steps to **achieve**:

- Access vulnerabilities and risks
- Develop a resilience plan
- Invest in organizational resilience
- Embrace technology for resilience
- Test and refine your resilience plan
- Continuously monitor and adapt
- Collaborate and learn from others

- **Continuity:**

- organisations capacity to sustain business activities and restore vital functions
- primary focus on plans and strategies – for acceptable and predefined level service delivery

- **Resilience:**

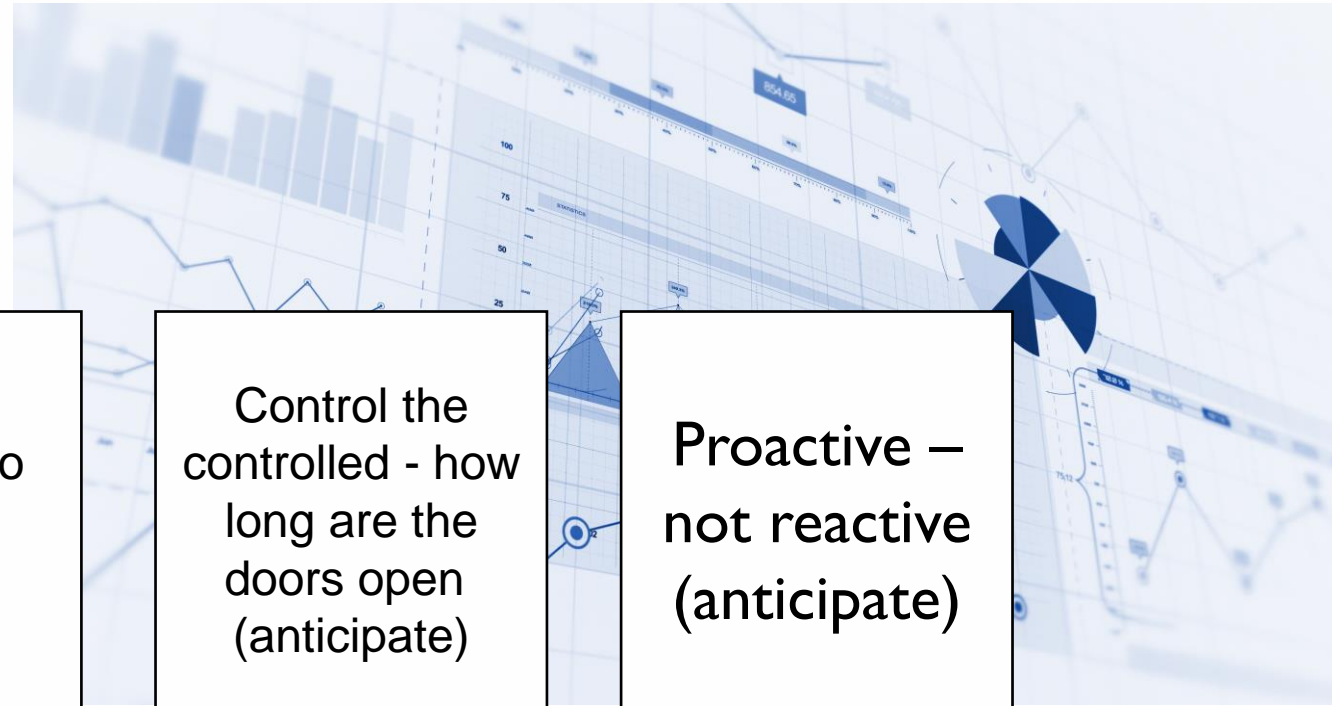
- Ability to withstand unexpected events and emerge stronger
- Extends to incident management, strategic and operational factors
- Ability to absorb and adapt to changing environment





**OLD** – KPI – Key Performance Indicator

**NEW** – KRI – Key Resilience Indicator



Mean time to detect  
(withstand)

**MTTD**

Mean time to respond  
(withstand)

**MTTR**

Control the controlled - how long are the doors open  
(anticipate)

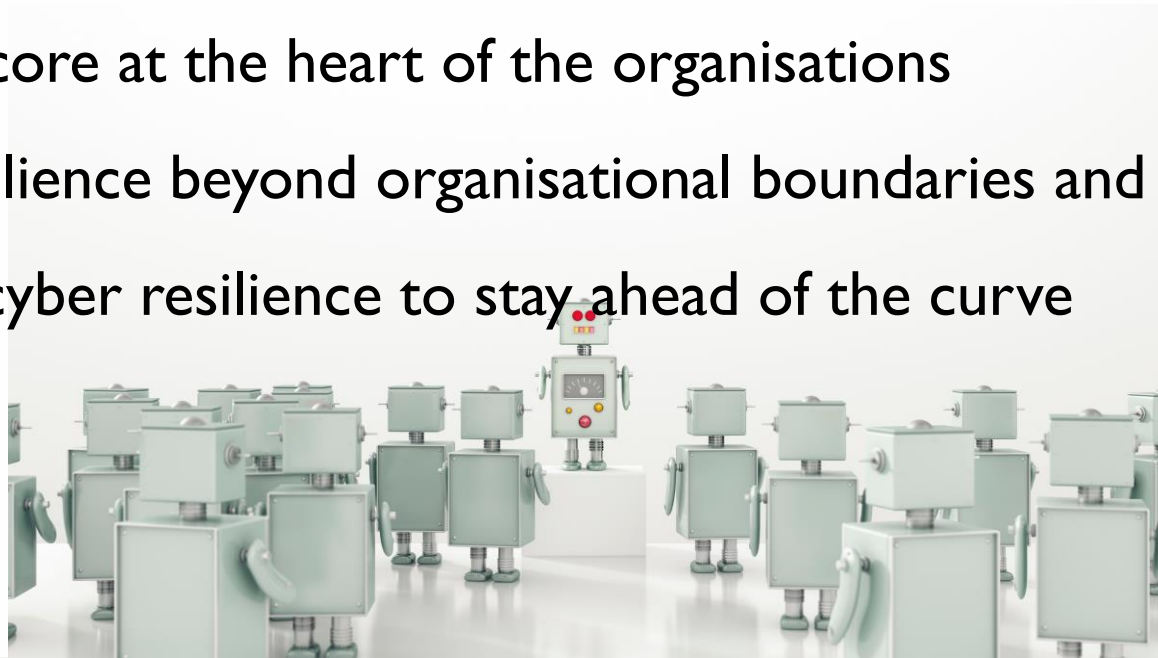
**Patch deployment time**

Proactive – not reactive  
(anticipate)

**System uptime**

**Define it – Measure it – Be accountable for it**

- Embedding cyber resilience in the business strategy from the start
- Establishing shared cybersecurity accountability across the organisations
- Securing the digital core at the heart of the organisations
- Extending cyber resilience beyond organisational boundaries and silos
- Embracing ongoing cyber resilience to stay ahead of the curve



## Cyber Resilient CEO:

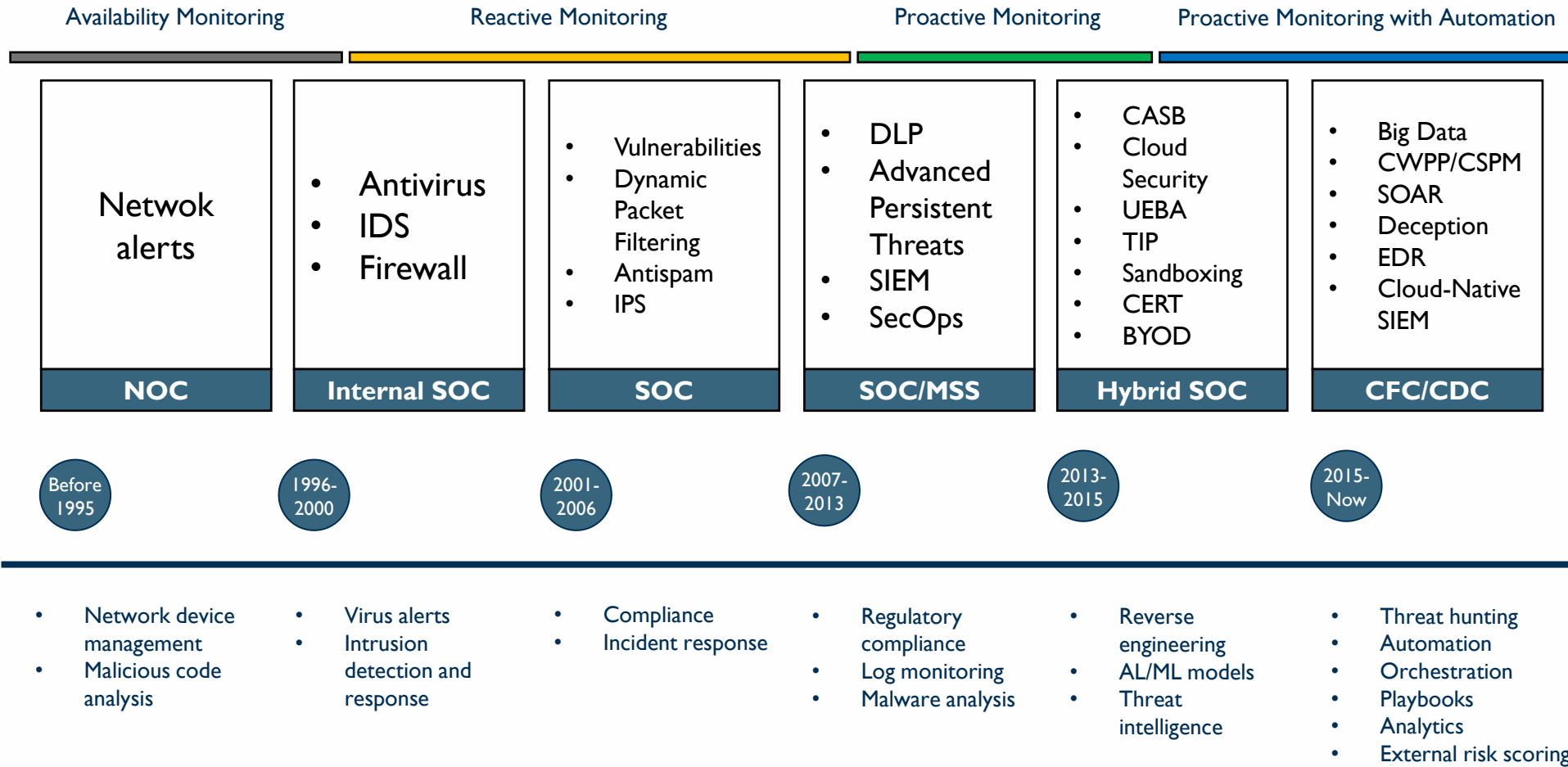
Manages cyber performance as finances 60% vs. 33%

Adopts shared accountability 68% vs. 37%, manages AI risks 54% vs. 33%

Boosts cyber security budget 76% vs. 35%

Third-party and enterprise-wide risk assessment 64% vs. 41%

Commit to continuous measure improvement; detect and respond to cyberattacks 6% vs. 34%



- ISO Standard was released in 2005 – compliance was added to the SOC's objectives
- The era between 2007 and 2013 was the golden age for SOC evolution – DLP and SIEM, APTs significantly increased
- 2015 – TIP – threat intelligence platforms, OSINT
- TTP – Tactics, Techniques and Procedures

Since 2015: Cyber Defence Center (CDC), Cyber Fusion Center (CFC), Cyber Security Operation Center (CSOC), Cyber Security Incident Response Team (CSIRT) and Joint Operations Center (JOC)

- Initial SOC role was to detect, identify, investigate and respond to security incidents
- Detect and contain attacks or intrusions in the shortest time frame possible
- Reduce the impact, damage and recovery costs of the incident



### How?:

- Using combinations of technologies and streamlined processes
- For real-time monitoring and analysis of potentially suspicious behaviour

SOCs were created to address specific issues that existed at a specific time in the organization's history

- A shift to MDR
- The rise of SOAR
- SIEM, NDR and EDR as a front line of SOC
- Automation and AI
- Increasing popularity of managed SOC service



The measure of intelligence is the ability to change – Albert Einstein

## Reactive

- The primary focus of SOC is the security of the organization's people, assets, and ideas
- SOC is composed of selected experts, processes and technologies to fulfil its mission, BUT
- SOC mission is rigid and inflexible and cannot easily adapt to new security scenarios and extraordinary situations
- **Problem** – SOC is not integrated with Facilities, Crisis Response, HR, Operations, Cybersecurity Operations, or other departments that either:

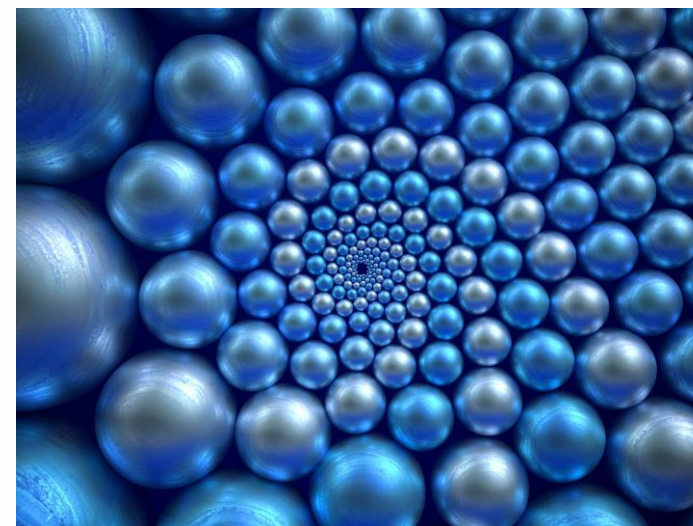
## Not integrated

- identify additional threats to the organization
- or are impacted by those threats

## Security-Centric

The result is that most security operations are not equipped to:

- Scale to the current level of threat volume or types
- Adapt to emerging threats
- Contribute to the organization's overall strategy, growth efforts, or specific initiatives



## DEFINITION

Cyber Fusion Center is a **strategic** SOC that combines

- threat intelligence
- security automation
- incident response
- threat detection
- other security functions,



bringing multiple **teams** and **resources** together to improve an organization's ability to **identify, prevent, and respond** to cyber threats

## GOAL

Cyber Fusion Centers are designed to accelerate **collaboration** and **communication** between teams engaging in

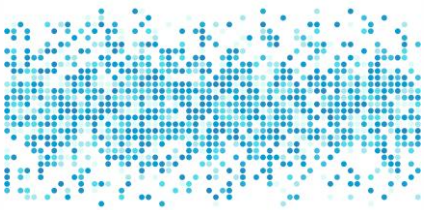
- cybersecurity and IT operations
- to reduce risk and **improve** the organization's **overall security posture**





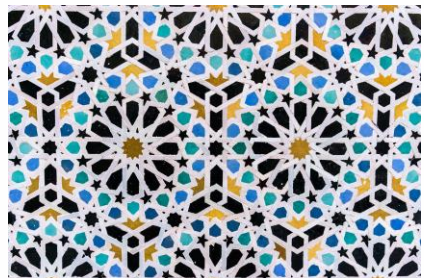
## Fusion Center goes beyond just cybersecurity

- cross-functional hub that brings together various teams together - IT, cybersecurity, risk management, fraud detection
- goal is to foster collaboration and information sharing across different domains
- aim to provide a holistic view of an organization's risk landscape
- helping in making informed decisions that align with business objectives



## Successful Cyber Fusion Center requires

- deep understanding of current SOC operations
- evaluate several domains to assess the maturity of a SOC – from its business drivers, to people, technology, services and processes



## Cyber Fusion Center is the unification of

- all security and related functions - orchestration/automation, data analysis, incident response and threat intelligence
- better integrate threat detection, management, and response processes
- facilitate security collaboration between people, teams, and devices



## Design of security roadmaps

- Security event monitoring, detecting, investigating, triaging and response
- Malware analysis, reverse engineering, digital forensics, insider threats, cyberfraud
- Threat intelligence platform management

## Assesment of security processes

- Threat hunting
- Content management
- Threat and vulnerability management

## Staff augmentation

- Compliance
- Reporting and notifications
- Training

## Operational support

- Identity and access governance
- Analytics



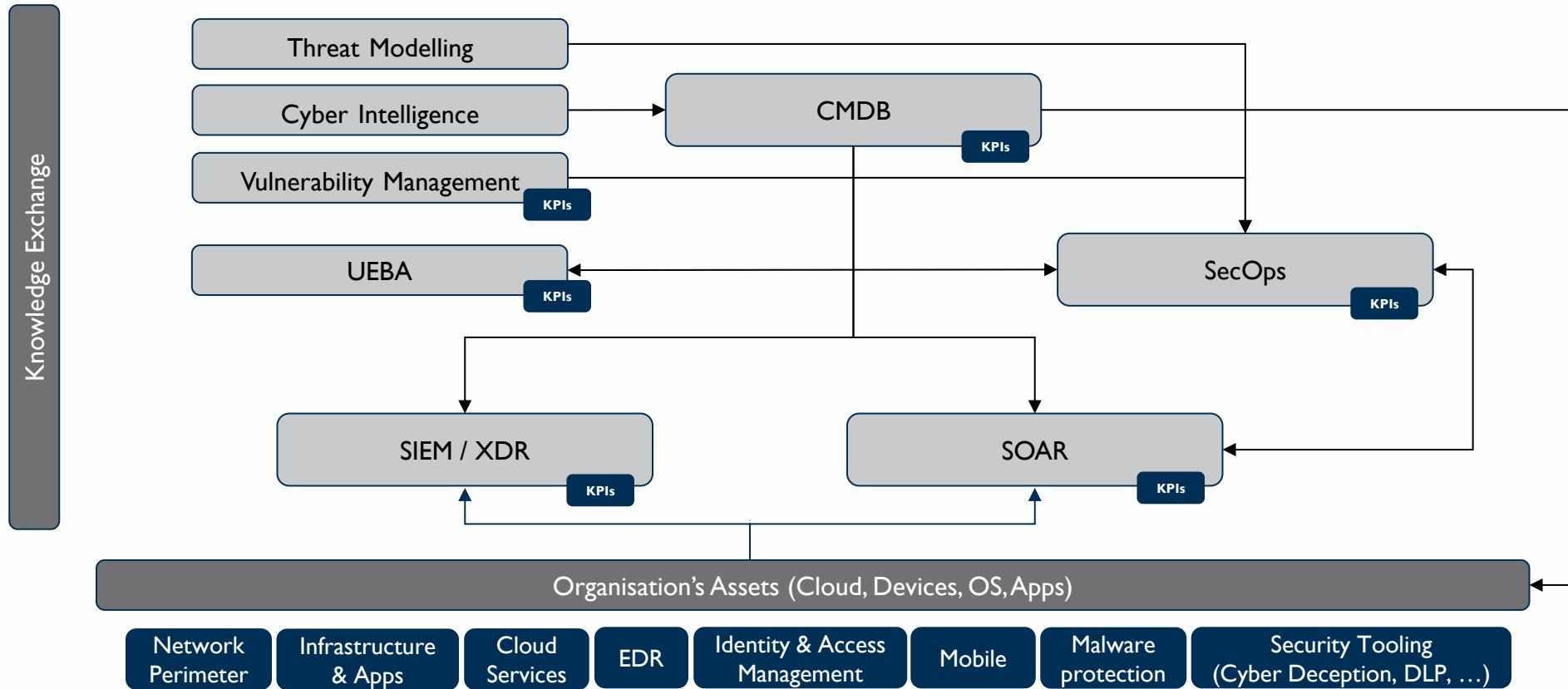
It's not about the numbers – it's about the stories they tell



Contextual Awareness



Incident Detection & Response



— A well-managed CFC offers the security tools and knowledge needed to keep your IT environment safe and resilient.

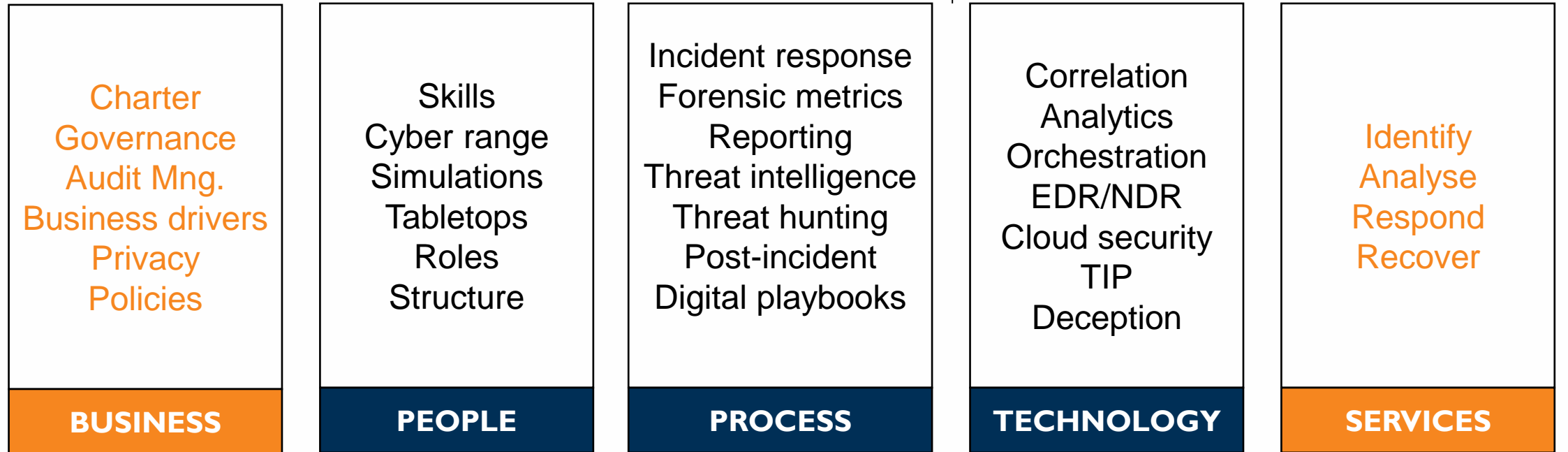
- CFC – more **unified** and **proactive** approach to threat management
  - by integrating different but related teams via collaboration and knowledge sharing
- SOC's role is focused on **detecting, identifying, investigating, and responding** to security incidents
- CFC is one step further by enhancing organization's overall security profile and capabilities
  - by integrating functions, intelligence, and teams
  - using real-time information and operating under shared goals,
  - CFC can operate more effectively in today's threat landscape



Attack Lifecycle Management

Vulnerability Lifecycle Management

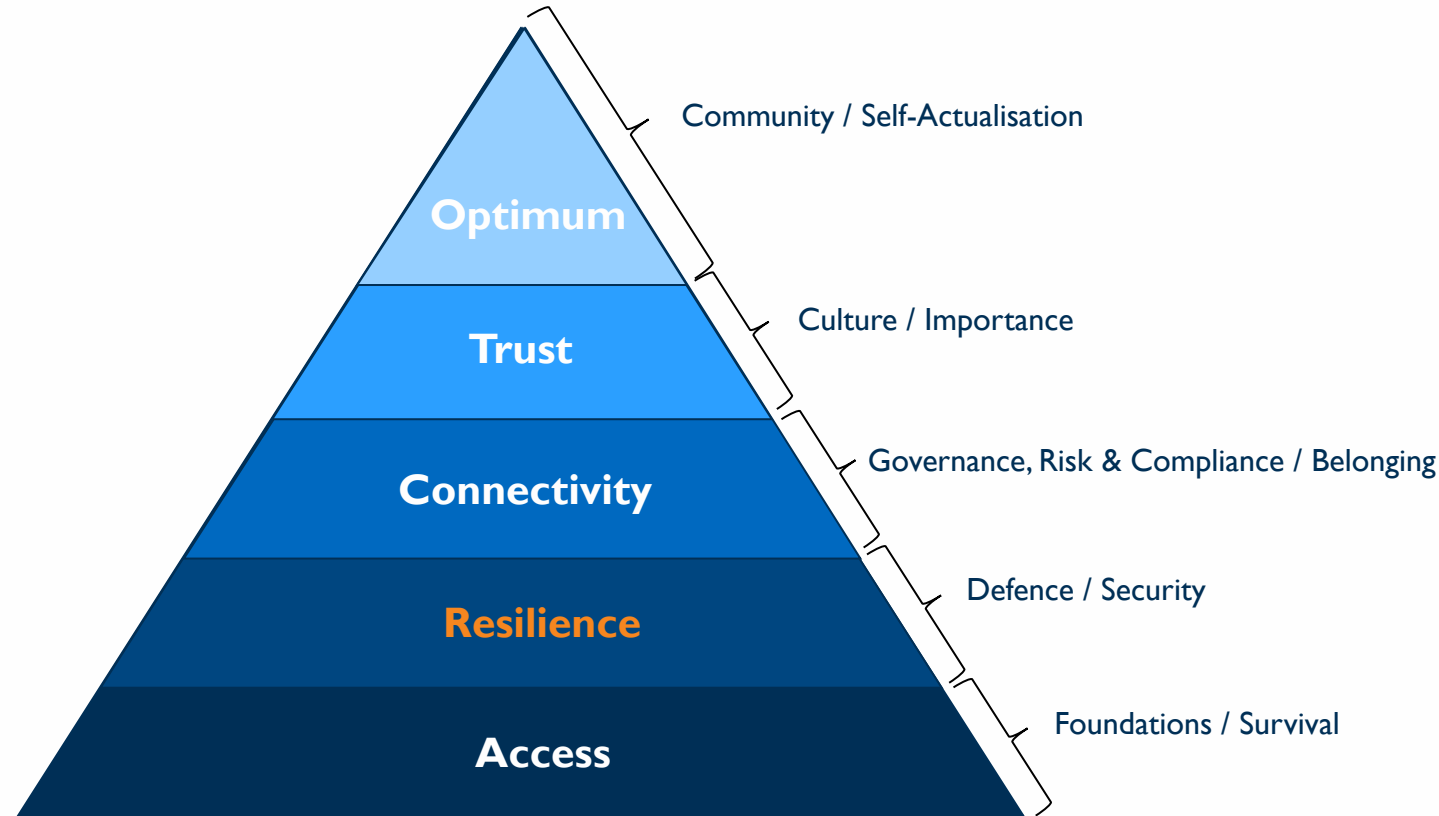
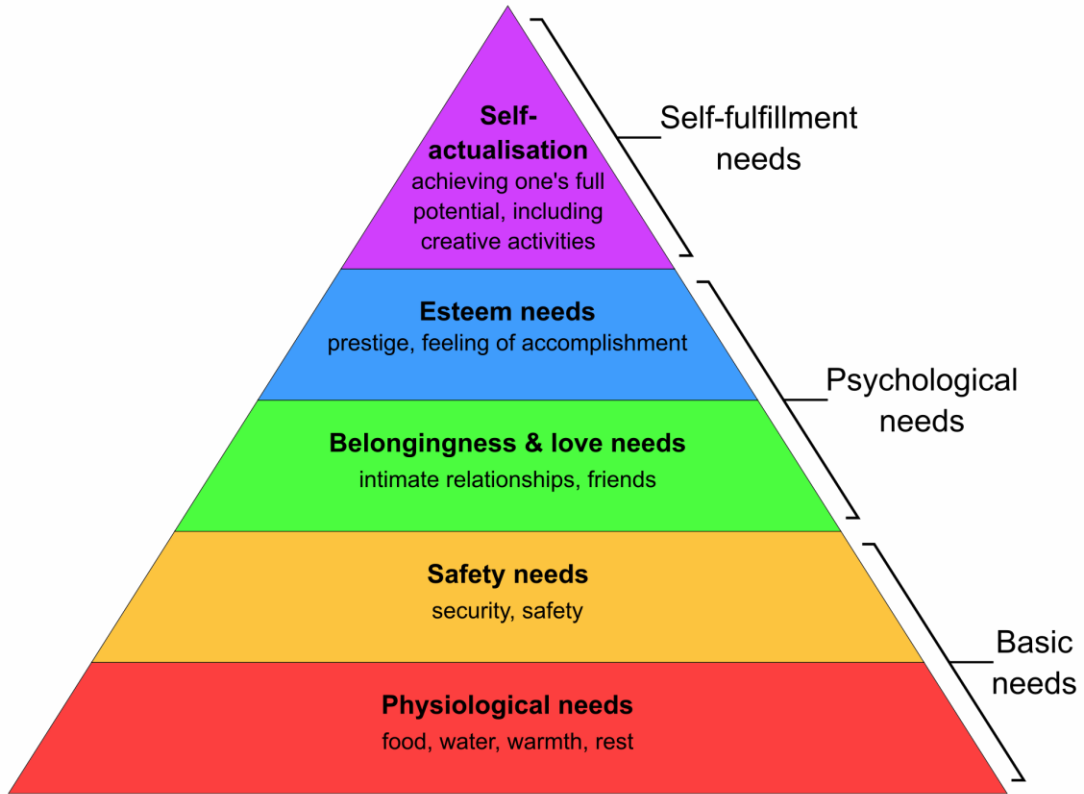
Threat Lifecycle Management



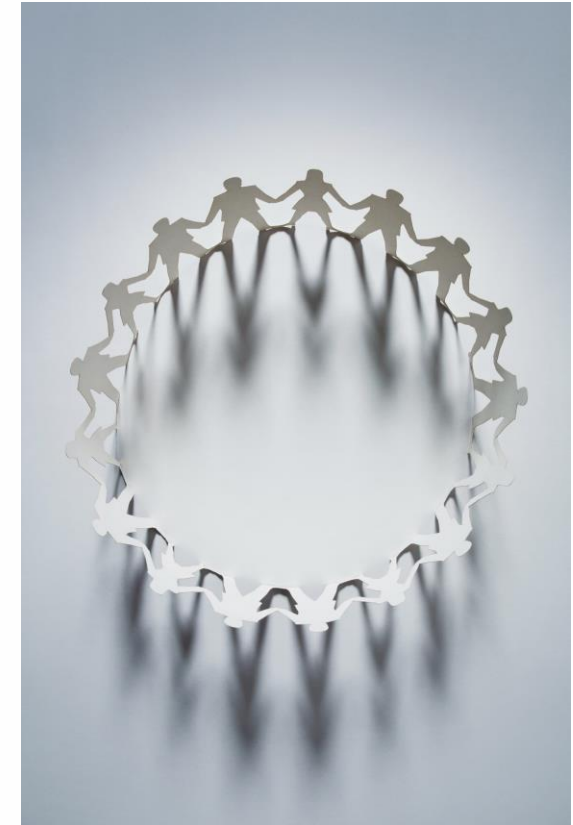
The **Key** is not preparedness, but the possibility to **Recover & Continue**

- According to Gartner, by 2025:
  - **70%** of CEOs will have mandated a culture of organizational resilience to withstand concurrent risks such as cybercrime, catastrophic weather events, civil unrest, and political instability
  - **60%** of enterprises will have adopted Zero Trust as a security starting point. However, more than half will not recognize the benefits
  - **60%** of C-level executives will have performance requirements related to risk built into their contracts with third parties and other business engagements
  - **30%** of countries globally will have enacted legislation governing ransomware payments, fines, and negotiations





- Always have:
  - **Logs** to analyse and rebuild historic chain
  - **Backups** – to restore/rollback
  - Required **competence** to deal with crisis
  - Required **skills** to apply
  - A **team** in all levels
  - Undeniable management **support** and involvement



**Take the lead from the Top**

- Data is a precious asset that must be protected accordingly
  - Reputation is crucial, especially in crisis management
  - Cybersecurity continuous monitoring allows for early detection
  - Vulnerability management buys precious time
  - Disaster recovery and business continuity planning is essential
  - Ability to adapt to changing environment is a key to resilience
  - Employee cyber resilience improvement is always a payback
- 
- CFC can be skilled partner in all of it

83% breaches involves external actors driven by financial factors



74% breaches features human element

**Moving from “Trust Me” to “Show Me”**





Thank You!