



Thomas Murray

Risk Intelligence | Due Diligence | Cyber Security



Cyber Resiliency - Challenges and Responses to Cyber Threats

Risk and Recovery Management Task Force – Central Depository Company of Pakistan Ltd
Breakout Session - ACG25 Da Nang Vietnam



Introduction

The ability to continue carrying out operations in anticipating and adapting to potential cyber threats and withstanding and recovering from any successful cyber attack.

CSDs must maintain their operational capability to ensure fair and orderly markets. Cyber is a Systemic Risk and should be treated as such.

Criminal and Nation State attacks:

- Operational disruption
- Ransomware
- Theft of data

Areas of weakness include: entity itself, participants/members, other FMIs, third parties ('Supply Chain'), new and old technologies, people.



Threat Landscape

Orbit Security

Organisation:
Bourse de Casablanca (MAR)

Universe:
Exchange

Score filter: 0 — 1000
[Slider]

Date filter: 03 Oct, 2023
[Slider]

Network footprint in:
Ireland, Morocco, United States (Total: 3)

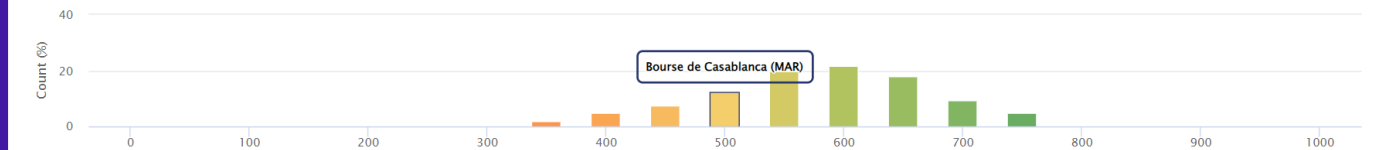
My Organisations Executive Summary Risk Profile Domains & IPs Trend Analysis Alerts Remediation Enquiries Reports

Bourse de Casablanca (MAR)

Cyber Security Score

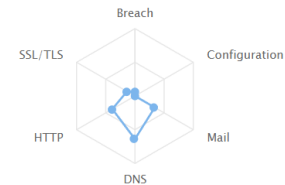


Benchmark of Exchange Scores

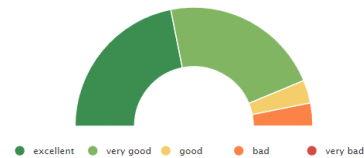


Bourse de Casablanca (MAR) is better than 16.04% of the Exchange Universe.

Risk Breakdown



Domains & IPs Risk Profile

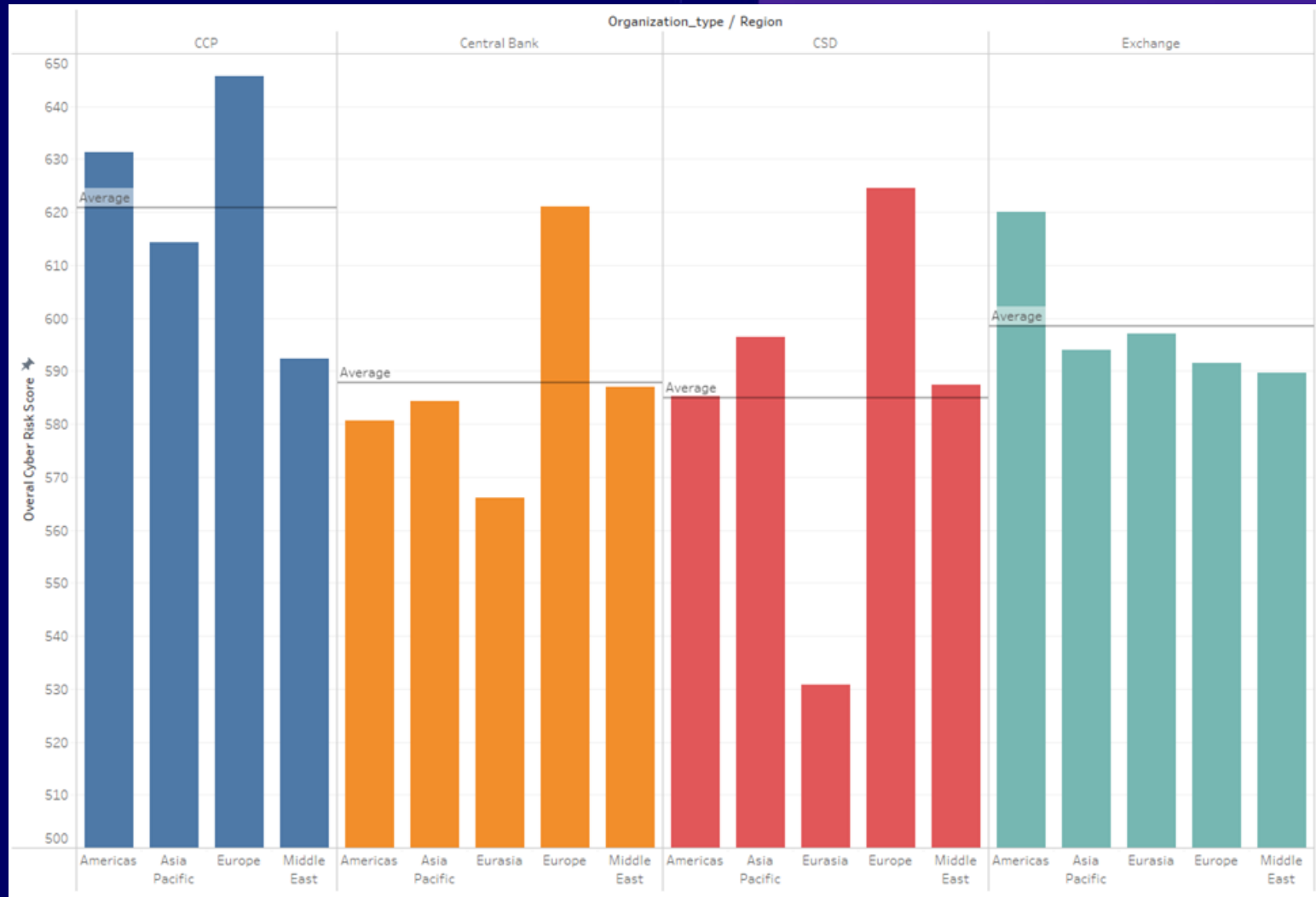


Geolocation of Network Infrastructure

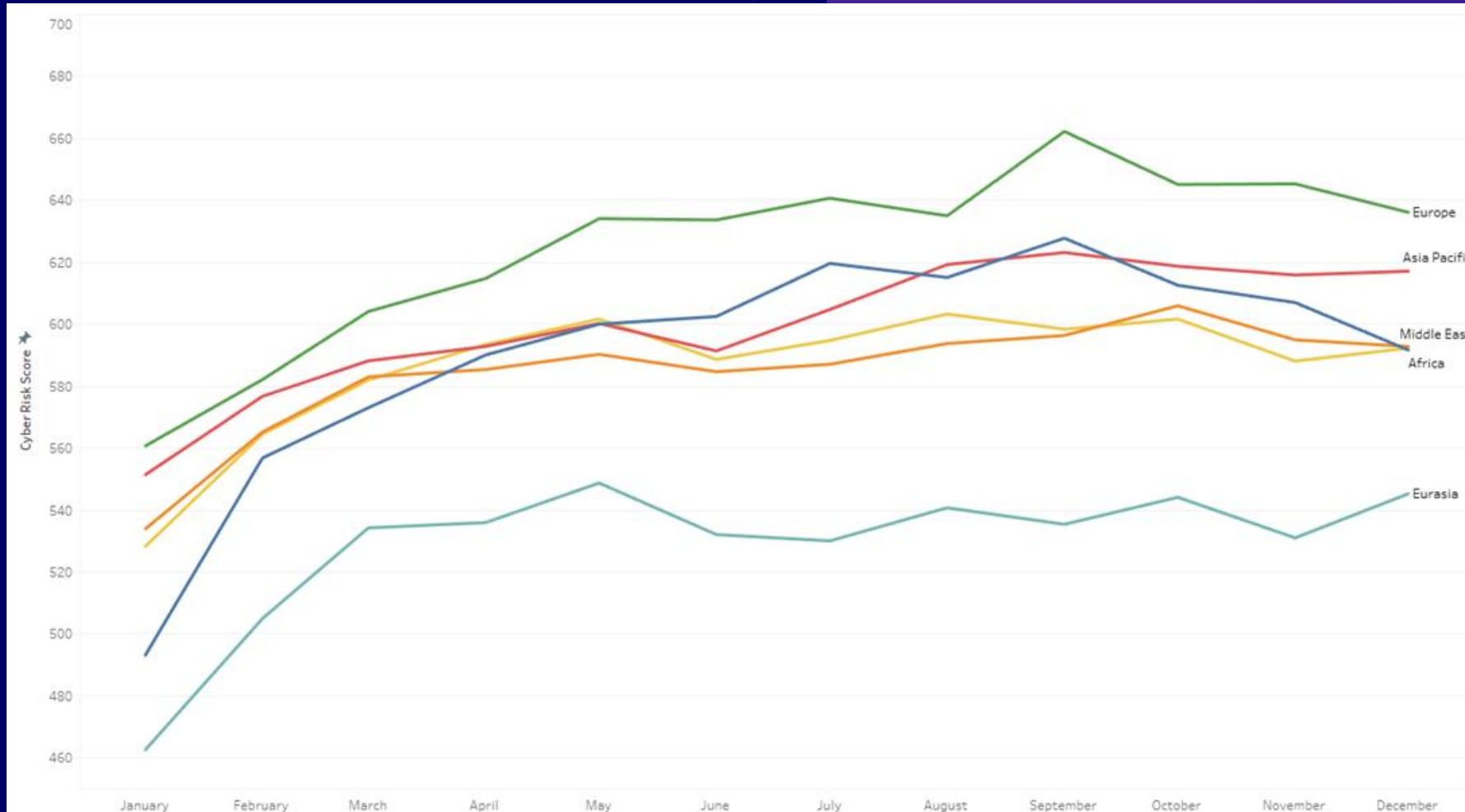


Selected 16 servers of total 16 discovered for Bourse de Casablanca (MAR).

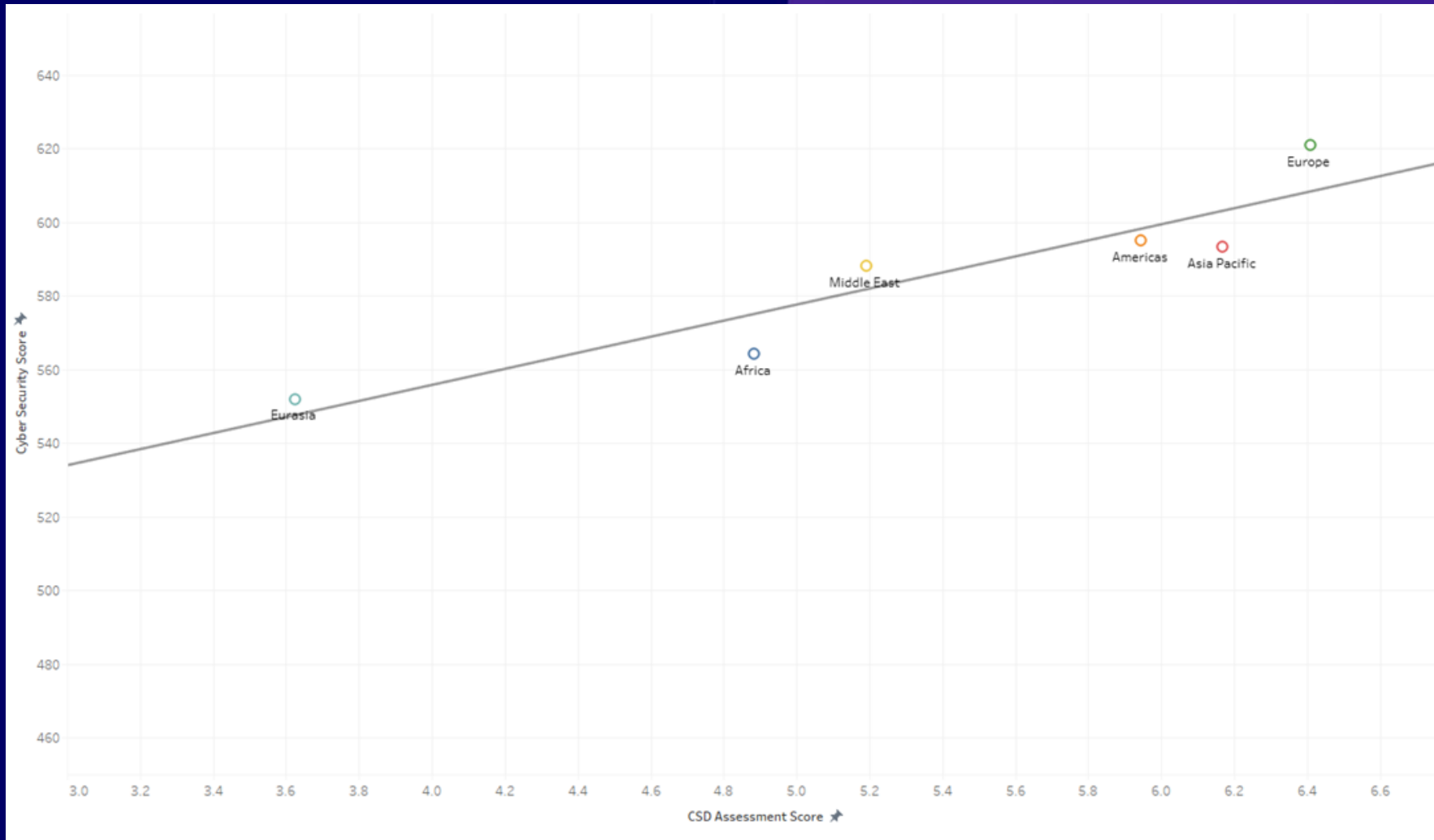
Threat Landscape



Threat Landscape



Threat Landscape



Prevention, Response & Resumption

Holistic approach beyond IT including ERM, Senior Mgmt, members, staff training to be Incident Ready

Tabletop exercises and market-wide threat simulation, systems testing, attack surface and internal security monitoring

Shared Threat intelligence – community approach to monitor threats and share information. Partner with government institutions and community for active Threat Hunting

Incident Response – get professional help and communicate! First responder, incident management, forensics and litigation support.

Resumption – data or system capability recovery, or roll-back across the whole market

Regulatory Response

EU – Cyber Resilience Oversight Expectations (CROE) for Financial Market Infrastructures (2018) – Evolving, Advancing, Innovating levels

Digital Operational Resiliency Act (DORA) – risk mgmt, incident mgmt, testing, third parties, info sharing

CPMI-IOSCO – Guidance on Cyber Resilience for Financial Market Infrastructure (2016)

UK, Singapore, Hong Kong – operational resilience guidelines

Key Takeaways

- Not “If” but “When”.
- Treat Cyber as a Systemic Risk.
- Enterprise-wide issue – not just IT, treatment from the top down and bottom up.
- “You are not alone” – understand the threat as a community, share intelligence, prepare, respond and react together, get in a professional.
- Regulation is rapidly coming – be prepared.

Thank you