Thomas Murray | Cyber Risk

Stay Ahead of Cyber Threats

4th September 2025

UNDER CYBER ATTACK?

Call our incident response team 24/7 on +44 (0) 207 459 4888 for immediate help from our experts

Thomas Murray | Cyber Risk

Agenda

01. Real world examples of threat actor activity

02. Cyber Threat Landscape

03. Orbit Security Analysis of ACSDA CSD's

04. FMI Risk Assessment Analysis of ACSDA CSDs

05. Approach toward risk management

06. Key Takeaways and Question & Answers

Thomas Murray | Cyber Risk

Speakers

Ana Giraldo

Chief Risk Officer & Director Americas

agiraldo@thomasmurray.com

Shreeji Doshi

Director – Cyber Risk

sdoshi@thomasmurray.com

Thomas Murray | Cyber Risk

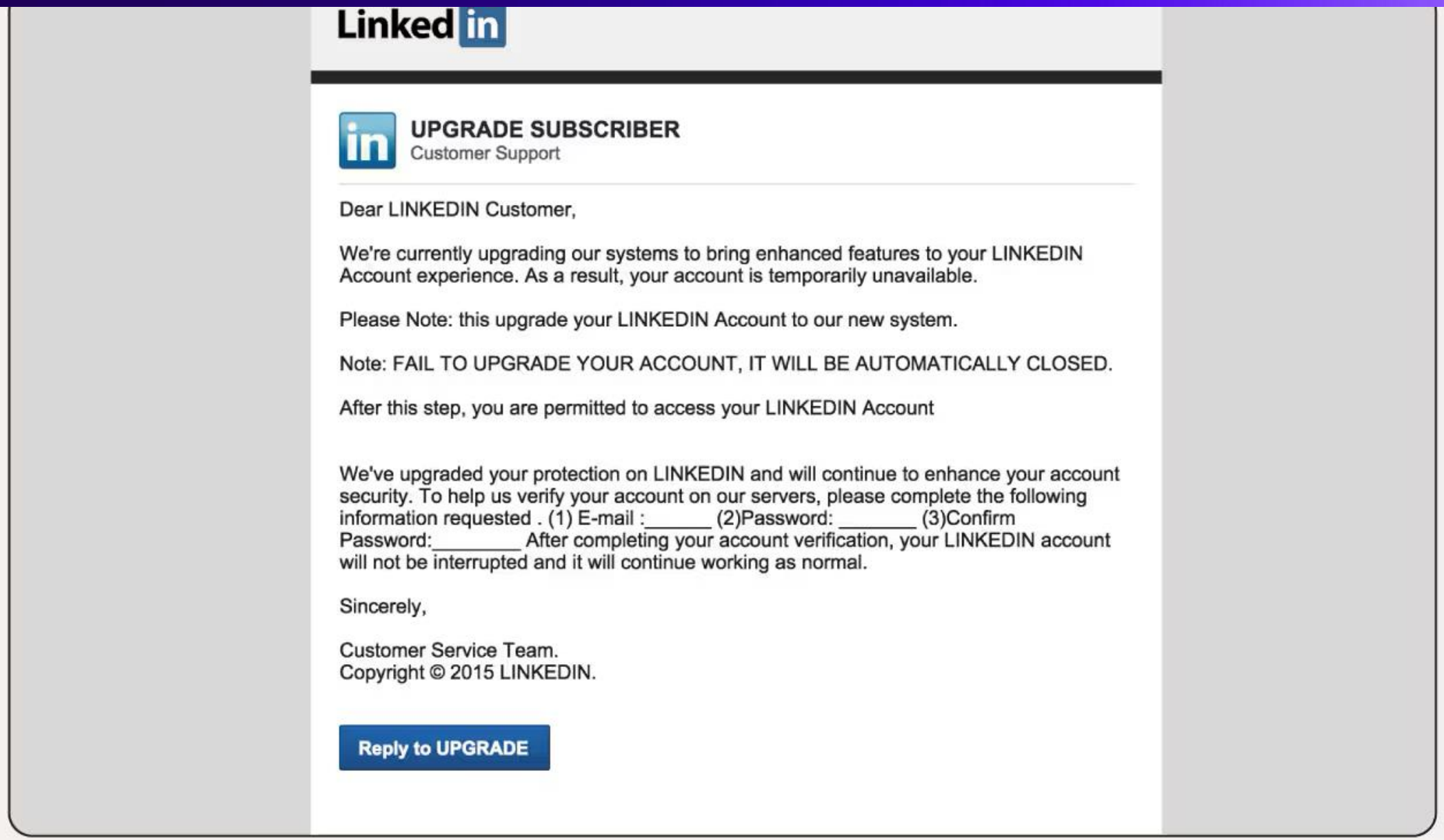
01

Real world examples of Cyber threats

Thomas Murray | Cyber Risk

Question

What is the number one threat?



LinkedIn

UPGRADE SUBSCRIBER
Customer Support

Dear LINKEDIN Customer,

We're currently upgrading our systems to bring enhanced features to your LINKEDIN Account experience. As a result, your account is temporarily unavailable.

Please Note: this upgrade your LINKEDIN Account to our new system.

Note: FAIL TO UPGRADE YOUR ACCOUNT, IT WILL BE AUTOMATICALLY CLOSED.

After this step, you are permitted to access your LINKEDIN Account

We've upgraded your protection on LINKEDIN and will continue to enhance your account security. To help us verify your account on our servers, please complete the following information requested . (1) E-mail :_____ (2)Password: _____ (3)Confirm Password:_____ After completing your account verification, your LINKEDIN account will not be interrupted and it will continue working as normal.

Sincerely,

Customer Service Team.
Copyright © 2015 LINKEDIN.

Reply to UPGRADE

Thomas Murray | Cyber Risk

Question

Why does phishing remain so popular?

All of your files are currently encrypted by no_name_software.

These files cannot be recovered by any means without contacting our team directly.

DON'T TRY TO RECOVER your data by yourselves. Any attempt to recover your data (including the usage of the additional recovery s
if you want to try - we recommend choosing the data of the lowest value.

DON'T TRY TO IGNORE us. We've downloaded a pack of your internal data and are ready to publish it on our news website if you do
So it will be better for both sides if you contact us as soon as possible.

DON'T TRY TO CONTACT feds or any recovery companies.
We have our informants in these structures, so any of your complaints will be immediately directed to us.
So if you will hire any recovery company for negotiations or send requests to the police/FBI/investigators, we will consider thi

DON'T move or rename your files. These parameters can be used for encryption/decryption process.

To prove that we REALLY CAN get your data back - we offer you to decrypt two random files completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

https://aazsbsgya565vlu2c6bzy6yfiebkcbtvvcytvolt33s77xypi7nypxyd.onion:80/

Your company id for log in: [snip]
Your company key: 3 of any of your dc through comma. Example: "DC1, DC2, DC3". You can type less if you have no enough

YOU SHOULD BE AWARE!
We will speak only with an authorized person. It can be the CEO, top management, etc.
In case you are not such a person - DON'T CONTACT US! Your decisions and action can result in serious harm to your company!
Inform your supervisors and stay calm!

Your requested files.

18:05

Thank you for providing those. I will have my IT and Leadership team look over these.

12:09

Okay, we'll be in touch.

14:52

Understood. No one is in the office today since it is Sunday. We will reach back out to you on Monday.

14:39

ok, we are in touch.

17:13

We have reviewed the files. How does your decryption process work? Do you send us one decryptor that restores all our systems or do you send decryptors for each system affected?

11:44

I can restore all your systems and data in to the original state. We can easily check it. You send me 3 encrypted files, I decrypt them and send you back to you. But these files should not contain important information.

16:58

After payment you receive one decryptor that restores all your systems.

17:01

Thank you for the information. We will work on getting some files to send you. How long will it take us to restore once we receive your tools?

12:38

Recovery time depends on the size of your system. Usually takes about 1 day.

15:36

Negotiations

We will give you a full support the decryption process if you need it. Chat will be open until we have fully fulfilled our obligations.

07:20

Also, after the payment:

1. You receive decryptors (Windows and Linux OS).
2. Your page will be totally deleted from the blog.
3. ALL your data will be deleted from our server and you will receive the full deletion log.
4. You will get penetration report and recommendations how to avoid such the situations in the future.
5. You receive the guarantee that Black Basta or anyone of our team will not NEVER attack you again.

07:20

Thomas Murray | Cyber Risk

Payment

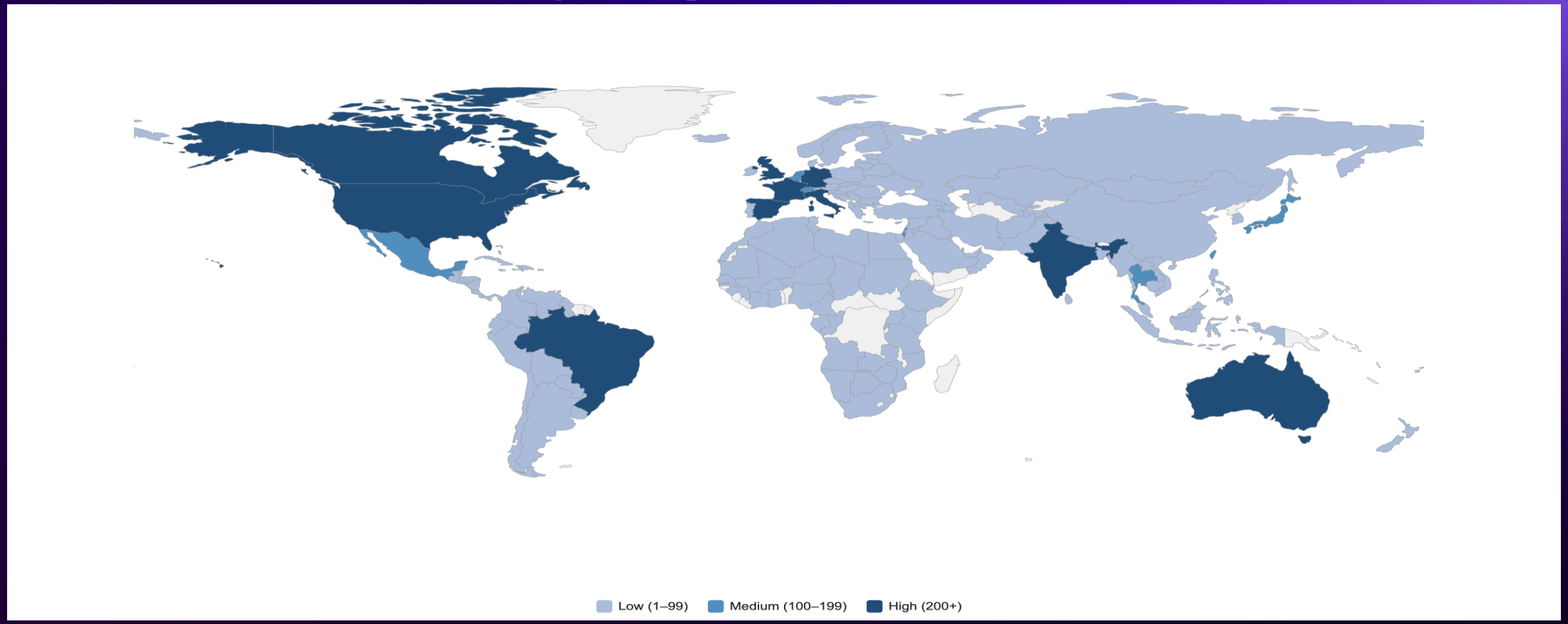
$2,062,500

02

Cyber Threat Landscape

Thomas Murray | Cyber Risk

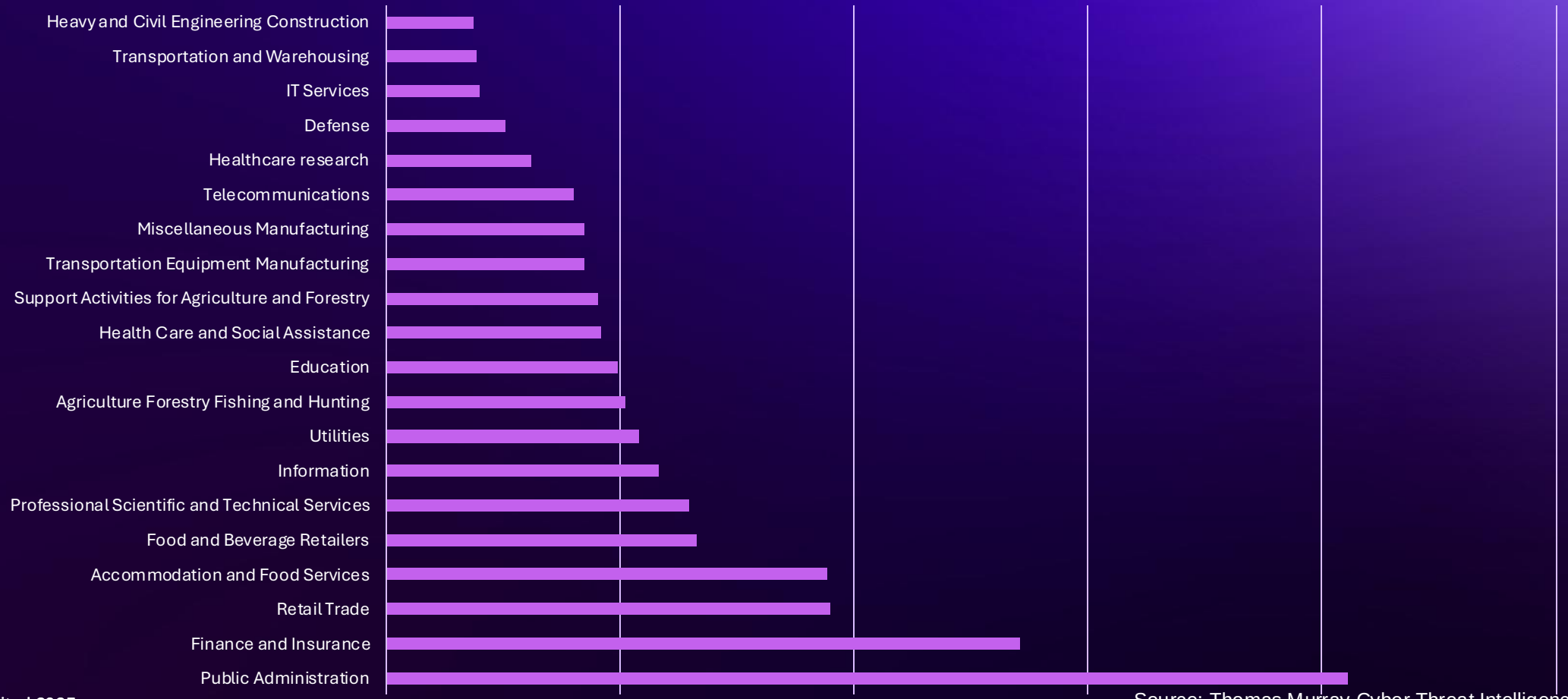
Cyber threats and threat actors correlated to geopolitics



Source: Ransonware.live

Thomas Murray | Cyber Risk

Cyber threats and threat actors correlated to geopolitics



Source: Thomas Murray Cyber Threat Intelligence

Some prominent Cyber attacks on FMI ecosystems

1. Central Depository Services Limited (CDSL), India malware attack, November 18 2022 Disconnect from broader capital market infrastructure, disrupted settlement activities at CDSL, affecting services such as pay-in, pay-out, and pledging of securities

2. Moscow Stock Exchange & Sberbank (Russia) – DDoS disruption (February 28, 2022) | "We can confirm the Moscow Exchange website is down, but we don't have visibility into the incident's root cause or the extent of the disruption," a spokesperson for NetBlocks

3. Ion Markets (Dublin) – Ransomware on derivatives platform (2023)) | The U.S. Commodity Futures Trading Commission delayed publication of weekly trading statistics Two base metal traders said they had experienced some delays in matching deals transacted on the London Metal Exchange.

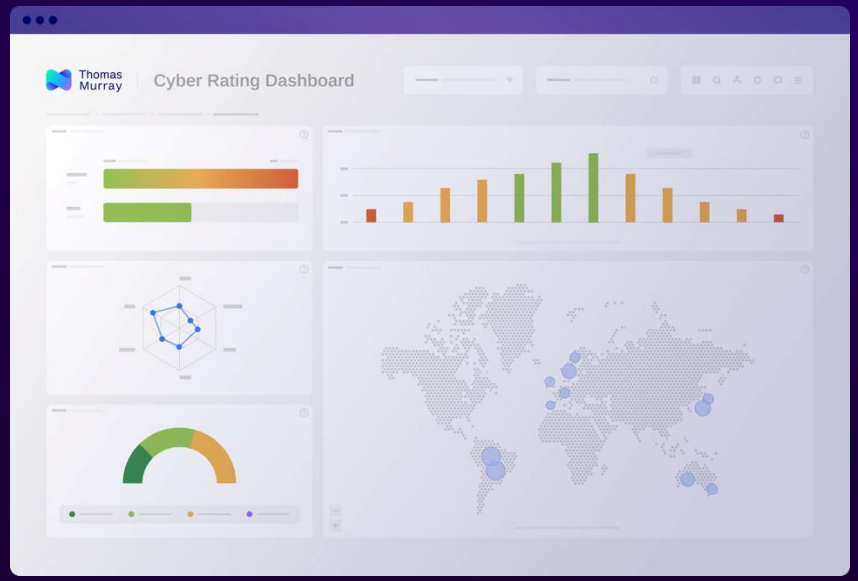
4. Mexico – SPEI Interbank System Breach – In 2018, hackers manipulated Mexico's SPEI instant payment system, creating phony transfer orders across multiple banks (e.g. Banorte), resulting in losses of approximately 300 million MXN (~US $15 million).

03

Orbit Security Analysis of ACSDA CSD's

Orbit Security

How it works



01. Provide Thomas Murray with your Root Domain(s)

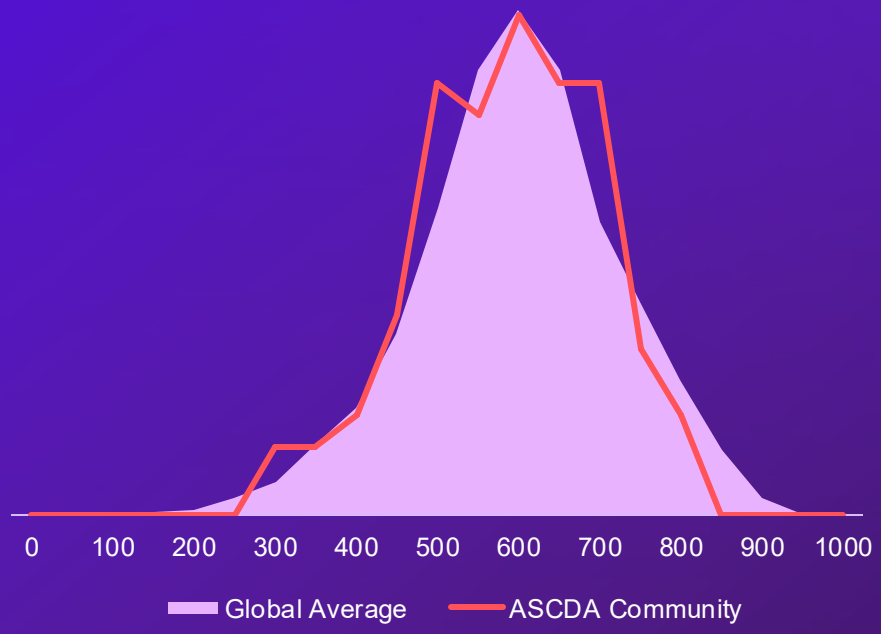
02. Discover your exposed attack surface

03. Continuously monitor risks, vulnerabilities, and actionable remediation information

Thomas Murray | Cyber Risk

ACSDA Community vs Global Benchmark

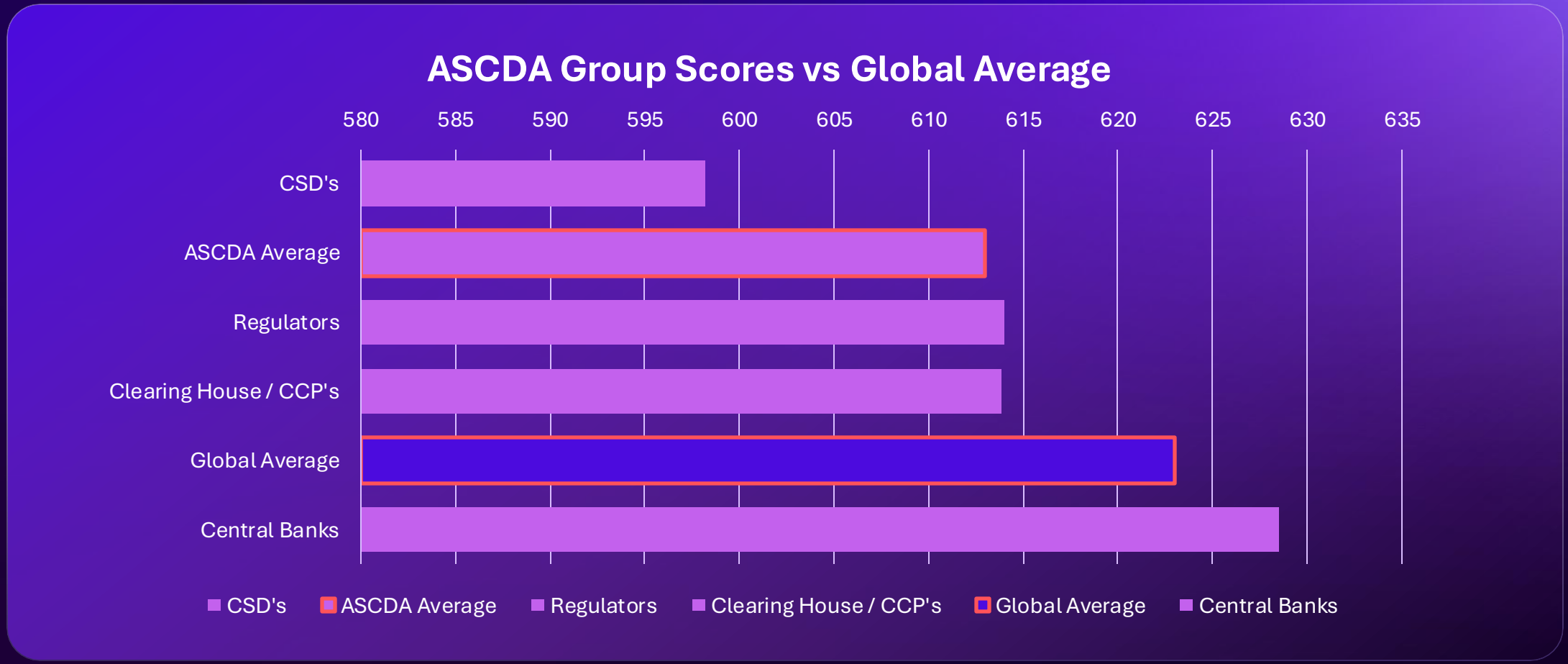
The distribution shows the number of companies at each Orbit Risk score level. The filled area represents the Global distribution of scores across all entities monitored by Thomas Murray, and the red line indicates the scores in this Community (n.92).



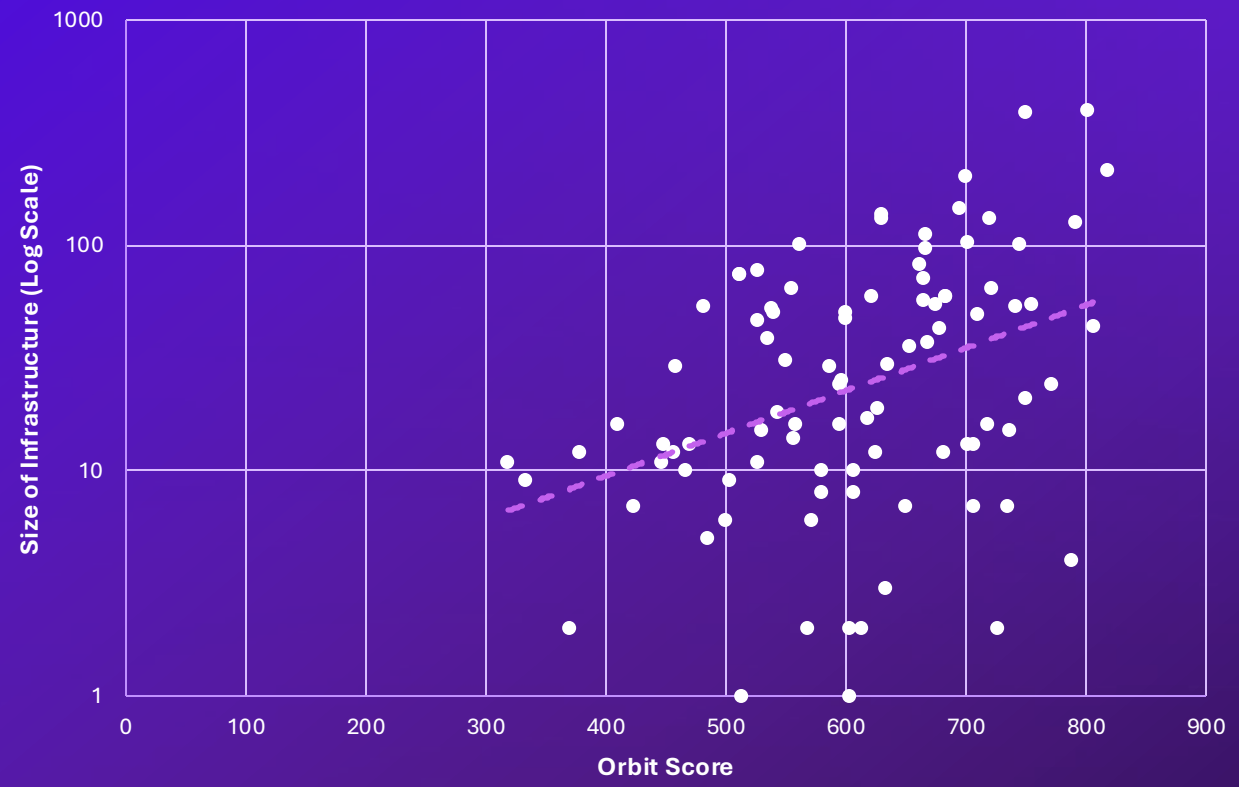
Key Takeaways:

- On average, the entities contained within the ASCDA community have performed **slightly below par** as compared with the global average.
- 13 entities (~16% of the community) stand out as having significant room for improvement (scores below 500)
- 4 entities (~5% of the community) scored below 400, which is considered a very low score.
- 3 entities (~3% of the community) have a score over 800 which is considered an exceptional score, including 2 with a score over 900

ASCDA Community Group Performance



Size of Organisation vs Orbit Score



Organisations with fewer assets open to the internet generally present lower scores, as expected.

Generally, more infrastructure implies more security maturity

Geographic Distribution of Servers

High-Risk Issues

Entities Affected by Issue		*Total Issues in Community*
35%	**Vulnerable Service** Services out of date and may require patching	135
37%	**Open Service** Services likely to not be purposely exposed	112
2%	**Compromised Server** Servers may be port-scanning or part of a botnet – **Further investigation required**	9

Summary of Findings

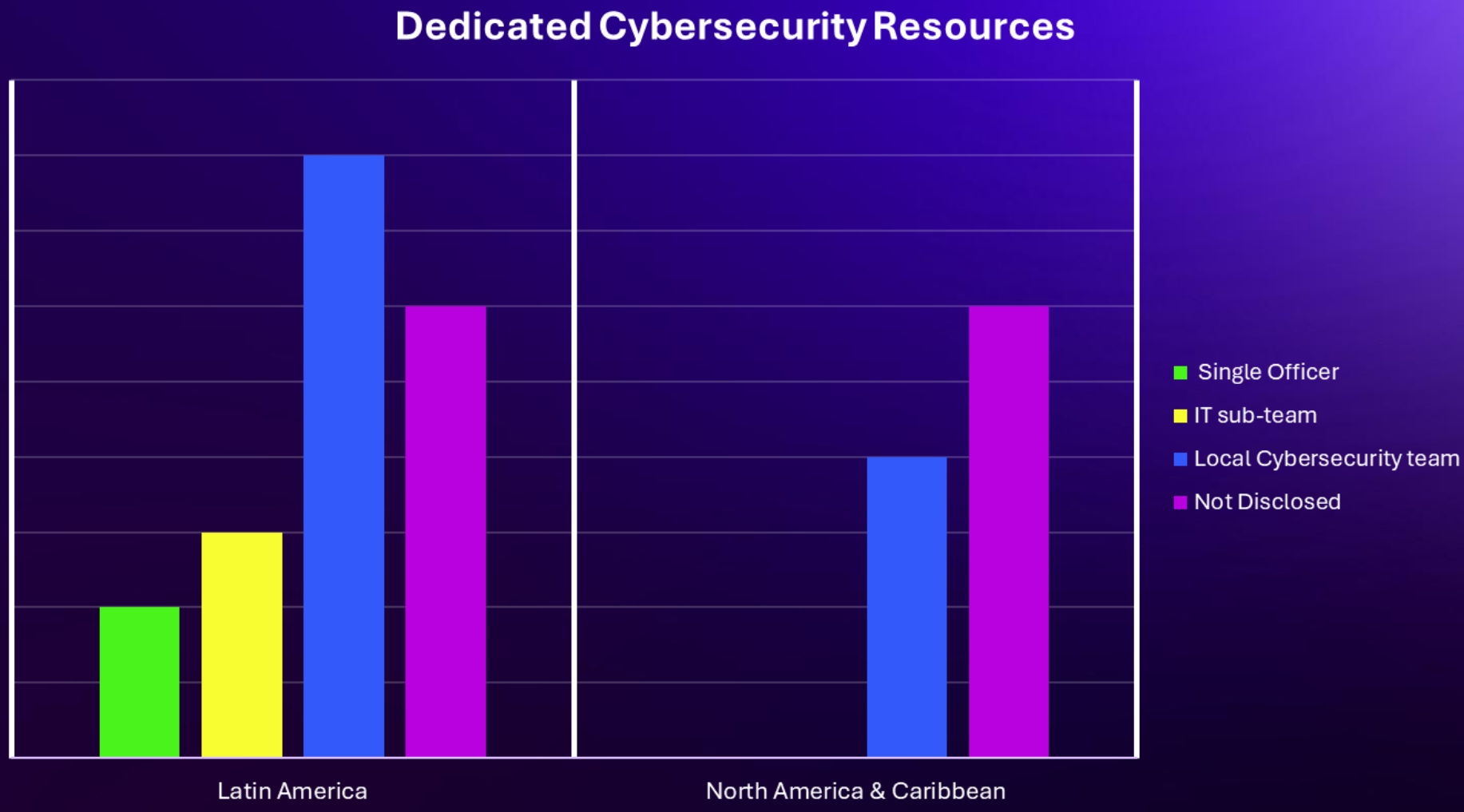
- On average, the entities contained within the ASCDA community have performed **slightly below par** as compared with the global average (Scoring 613 vs 623).
- CSDs are performing under the global average (Scoring 598 vs 623).
- The vast majority of the infrastructure in the community is within the borders of the Americas (~95%)
- There are significant vulnerabilities identified in the community, many of which should be considered to be of Critical Severity. The most severe of which could allow for Denial of Service (DoS) attacks, Authentication Bypasses, and even Command Execution

04

FMI Risk Assessment Analysis of ACSDA CSD

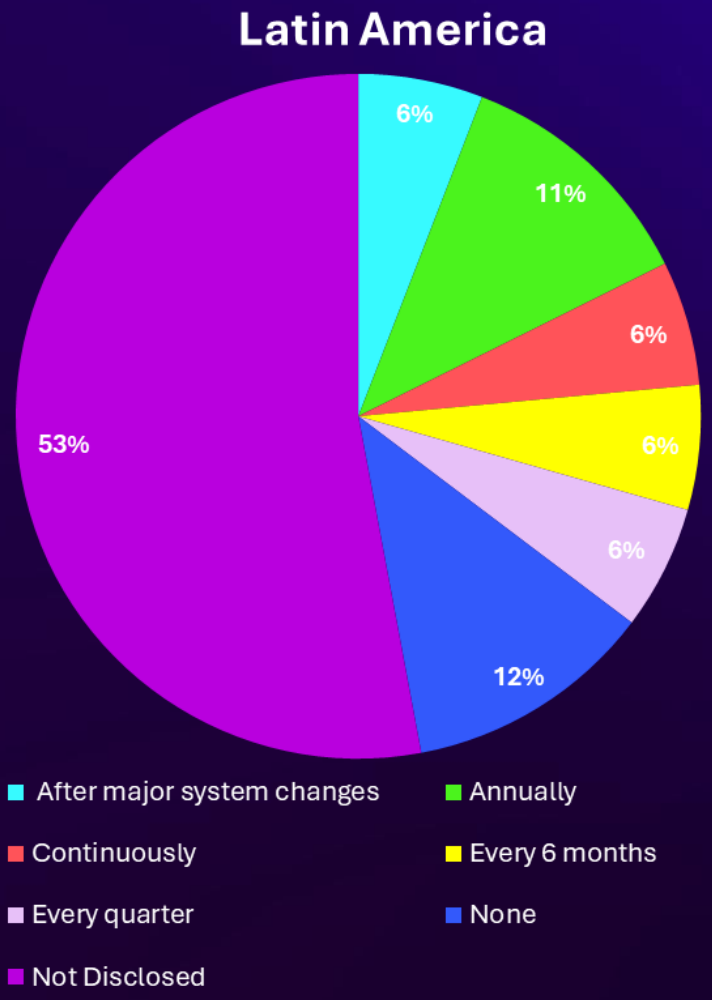
Thomas Murray | Cyber Risk

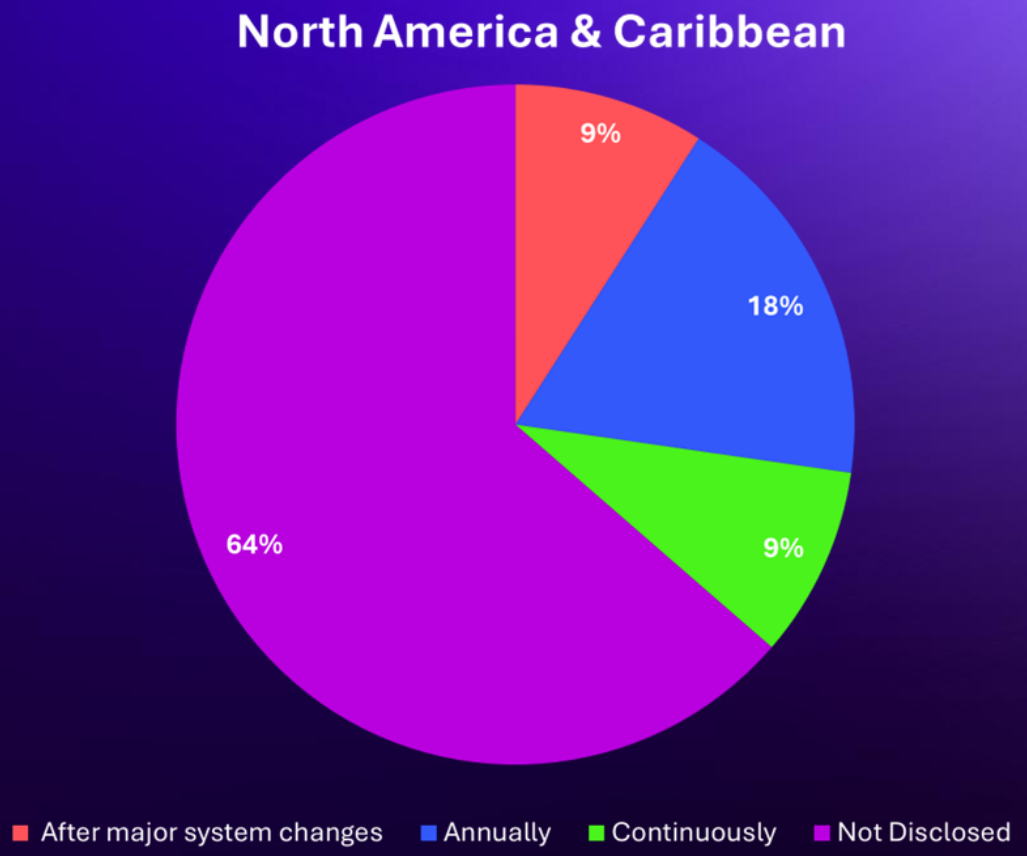
Key trends in Cyber resourcing



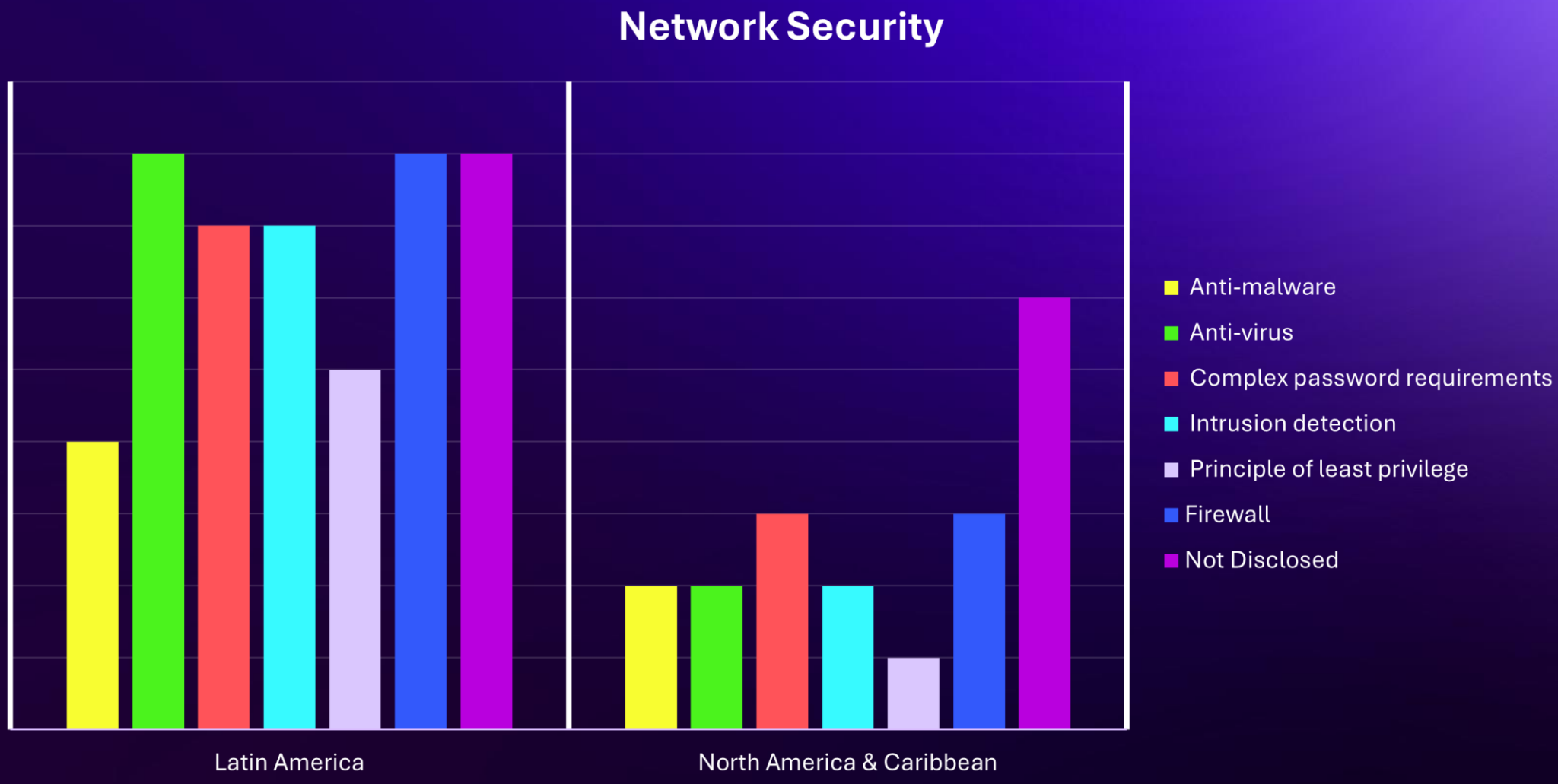
Thomas Murray | Cyber Risk

Key trends in Penetration testing - Frequency





Key trends in Preventive controls



05

Approach toward risk management

Cyber Risk Scenarios within CSD's

CSD's risk scenarios are quite unique as they have common cyber risk scenarios any organisations faces like data leakage, ransomware, service disruption, etc. Disruption and inability to settle remain the highest inherent cyber risk scenarios for a CSD.

Addittionally, CSD's IT environment has multiple interconnection with external stakeholders which bring along new threat vector and associated scenarios. Some of them are illustrated below

Typical CSD Stakeholders	Function	Risk Scenarios
Broker/Market Maker	Clearing/Settlement	Settlement instruction corruption or leakage
Custodian	Clearing/Settlement	Settlement instruction corruption or leakage
Payment Banks	Clearing/Settlement	Payment instruction corruption
Exchange	Clearing/Settlement	Trade data corruption or leakage
Boursa Kuwait	Asset Servicing	Primary CoAc info corruption or leakage
Issuers	Asset Servicing	CoAc info corruption or leakage; dividend funding corruption or leakage
Custodians	Asset Servicing	Elective event instructions corruption or leakage
Asset Managers/Investors	Asset Servicing	Elective event instructions corruption or leakage

Regulators have appreciated the uniqueness of Cyber Risk in CSD

- Regulatory landscape for managing Cyber Risk has evolved.
- Regulations and frameworks in EU (DORA), Australia, Canada, Brazil (Resolution CMN 4,893 of 2021), USA, UK, Singapore, Hong Kong and others covering local financial institutions.
- CPMI-IOSCO 2016 guidance: 2hr RTO

Risk management	Incident response, Testing and Timely incident reporting	Technical Assessments	Business continuity and disaster recovery	Governance and oversight	Data protection and privacy

Thomas Murray | Cyber Risk

Standard approaches to dealing with Cyber threats

Adding new technical capabilities like EDR, MFA, Zero Trust, etc.

Improve Governance, Awareness and Competencies

Process Improvement Vulnerability management, Patching, Third Party Assessments, etc.

Align control to regulatory requirements and CPMI IOSOCO guidelines.

Adopt Control Framework like ISO 27001, NIST CSF, MITRE, NIST 800-53, CIS Top 18

Cyber Threat Intelligence drive Risk Management

The "What"

Threat intelligence sources
Vendor reports
TTPs

ATT&CK®

Business context:
Technology, data, product, services.
Industry

The "So what"

Cyber security risk:

Articulated within the context of the Business.

The "Now what"

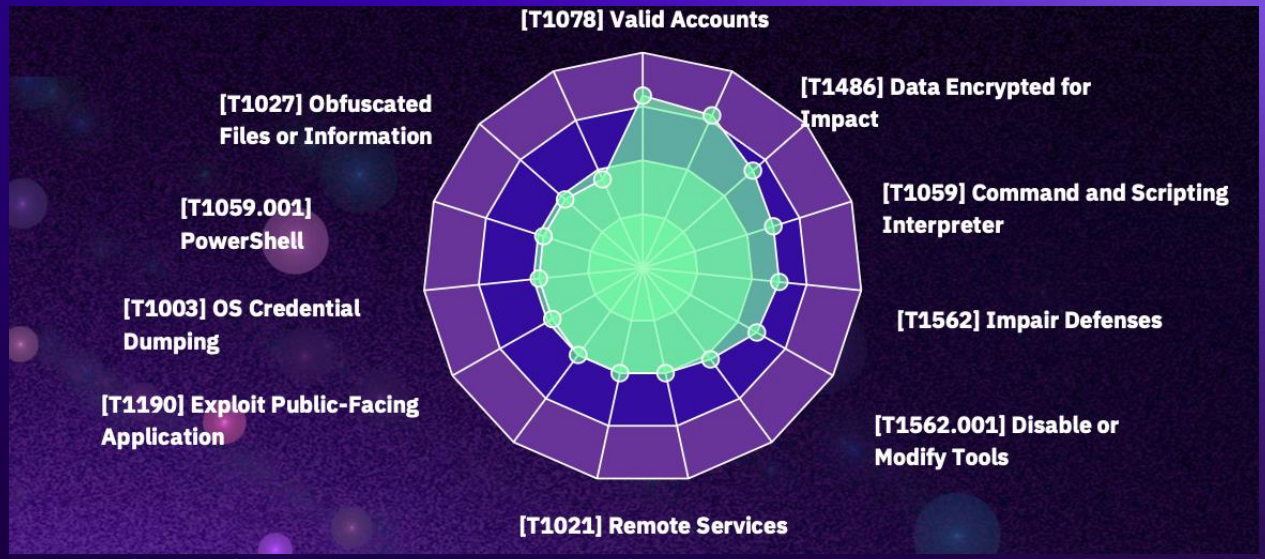
MITRE ATT&CK to NIST 800-53

TI data drives best Course of Action

Cyber Threat Intelligence drive Risk Management

With limited time and resources answer the **following:**

- Who might want to attack your organisation?
- Which attacks are most relevant to your organisation?
- Which attacks will cause the biggest impact?
- How might they do it?



And therefore, **what** what controls should the organisation prioritise based on MITRE and NIST .....

Baseline recommendations

Technical

- Multi-factor authentication
- Endpoint Detection and Response
- Patching and vulnerability Management
- Encryption, rest, transit, use
- Segmentation of networks

Human

- Engaging and topical training
- Policies, procedures (SoPs)
- 4eyes
- Employee vetting

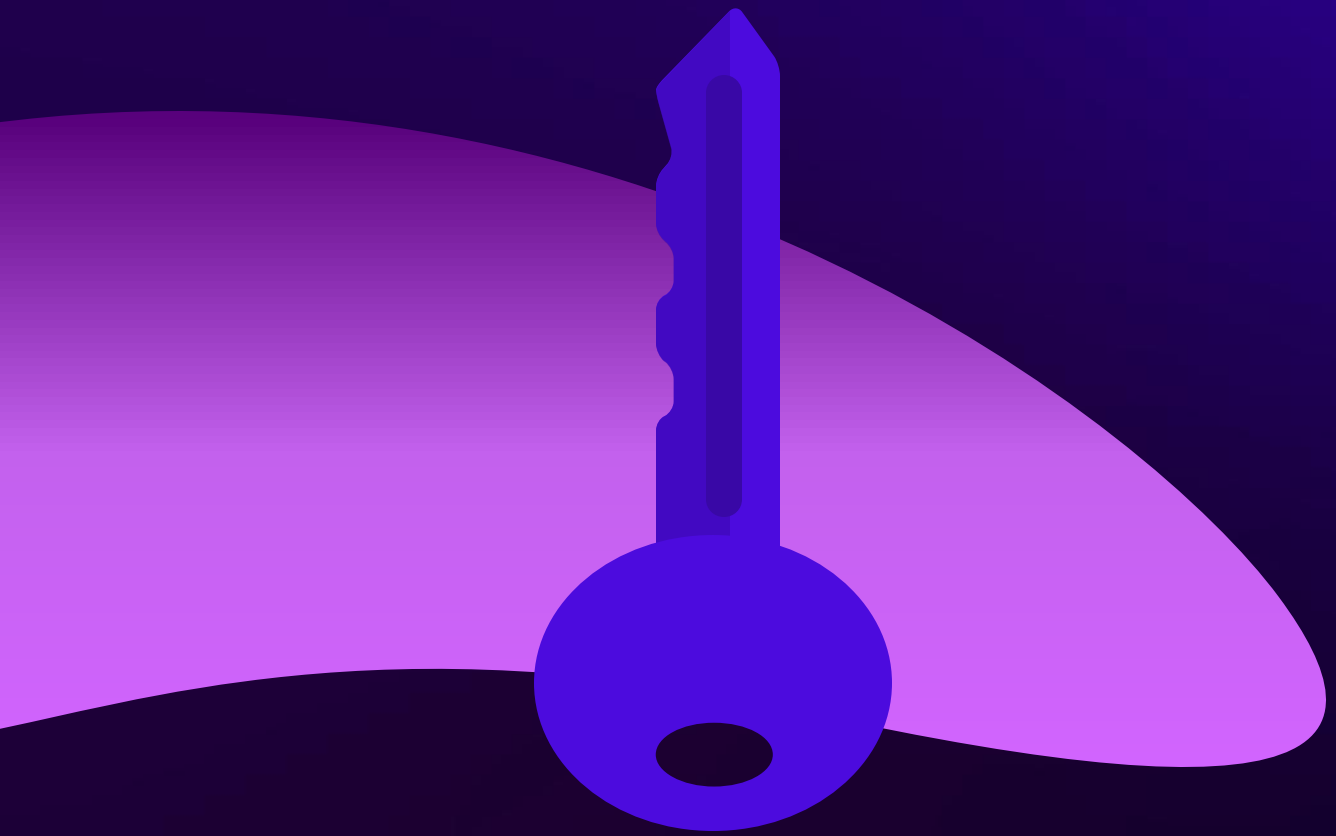
Information Sharing

- Latest tactics, techniques and procedures (TTPs)
- Within an organisation, industry, or wider body of trust.
- Ability to ingest, information as well as share appropriately.

06

Key Takeaways

Key takeaways



Evolving Threat Landscape: Cybersecurity threats are continuously evolving, with new attack methods like ransomware, phishing, and AI-driven attacks becoming more prevalent and sophisticated.

Increased Risk in a Digital World: As FMI rely more on digital infrastructure, the risks associated with data breaches, system vulnerabilities, and insider threats have intensified, making robust cybersecurity measures more critical than ever

Cyber Threat Intelligence based Protection and Detection Measures: Transition standard approach of cyber security into Cyber Threat Intelligence driven which is understanding historic victimology that enables proactive planning

Questions and Answers

Thank You

Thomas Murray | Cyber Risk

For more information:

agiraldo@thomasmurray.com

sdoshi@thomasmurray.com