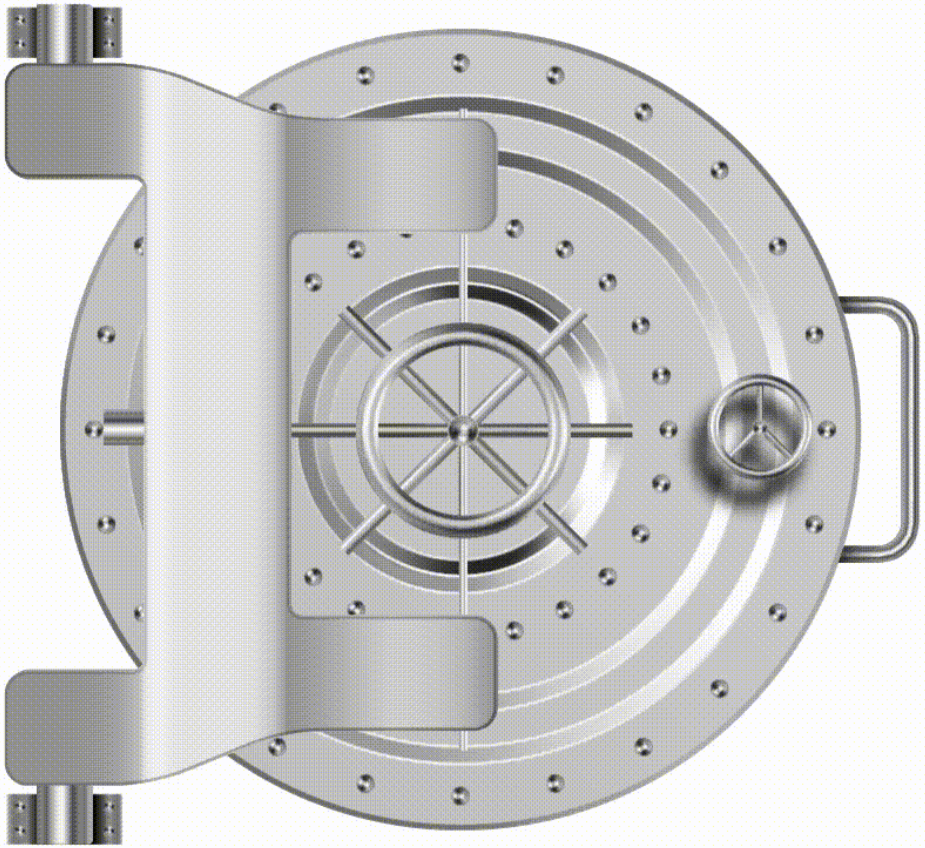
Deloitte.



Cyber Security Risk – Threat landscape, Emerging Trends and Insights

Cyber Security Governance: Updates From The Front Line, February 2023

February 2023

Introduction & Agenda

Vamsi Krishna Meruva

Director, Risk Advisory

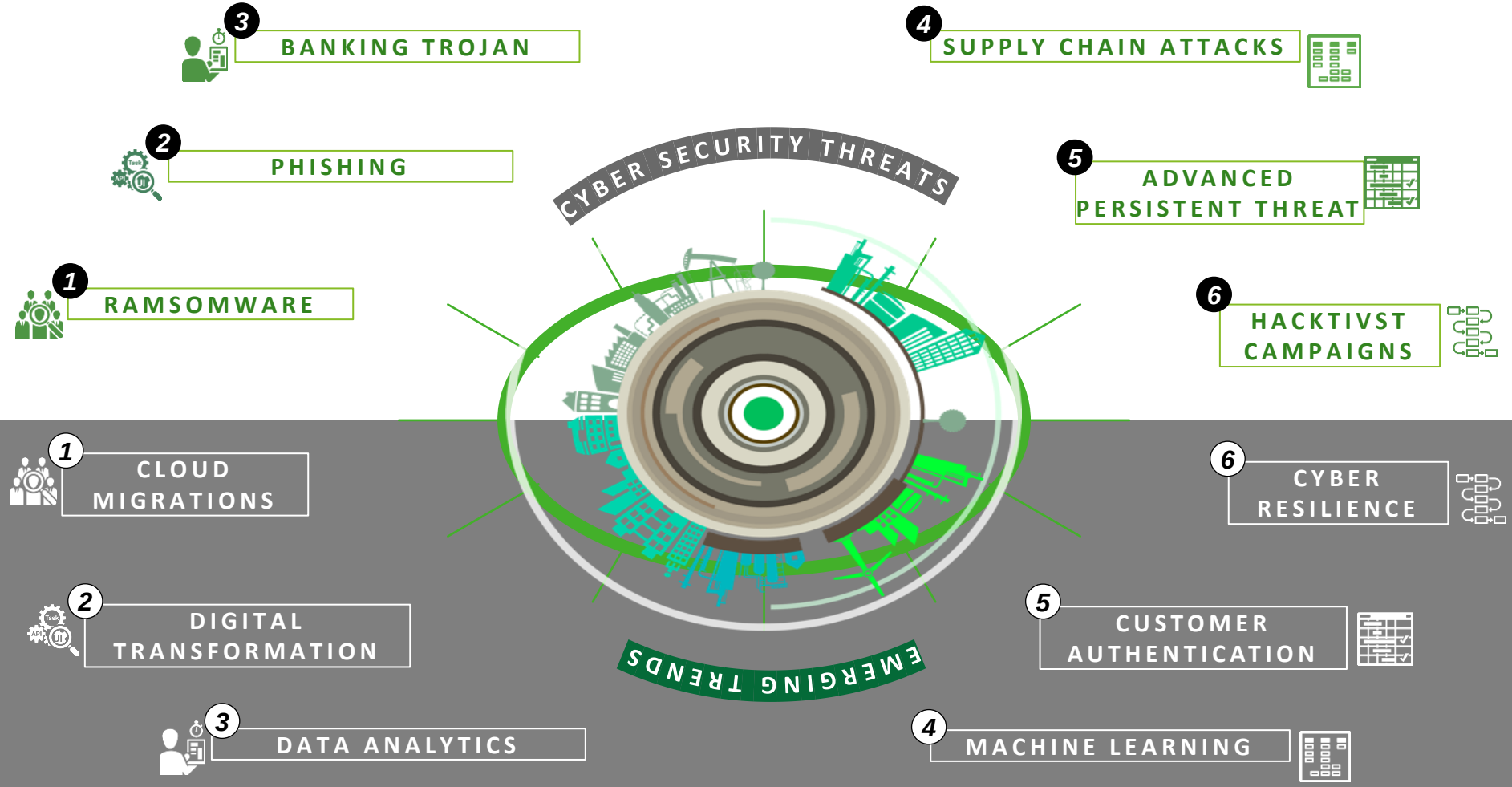
Deloitte UK

Email ID : vmeruva@deloitte.co.uk

What are the prevalent cyber threats and emerging trends in the financial services industry?

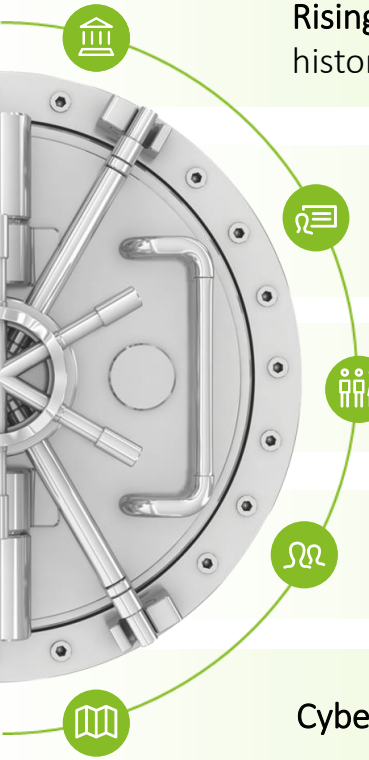
WHAT IT'S ALL ABOUT

The cyber threat landscape evolved significantly over the past decade owing to developments in technology, geopolitical issues, new wave of hacktivism and innovative 'go to market' strategies adopted by organised cyber criminals. 39% of UK businesses reported an attack in 2022 where the most common threat vector was phishing (83%).



Cyber Insurance Service Providers – Market Overview and Challenges

The market for cyber insurance is rapidly expanding with Gross Written Premiums expected to grow from c. $7bn in 2020 to c. $21bn by 2025. This increase is driven by rising cyber risk to firms particularly due to growing risk of ransomware attacks.



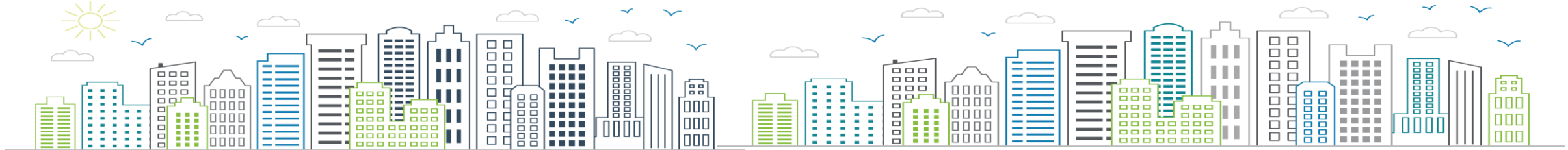
Rising premiums and increasing loss ratios – substantial increase of premiums post pandemic. Loss ratios are significantly above historic averages at 67%.

Cyber catastrophic incidents – a growing concern.

Lack of common standards- no overarching framework or agreed set of principles on best practises.

Challenges to measuring risk - no common yard stick to measure risk and limited historic data.

Cyber insurance – a potential strategic partner



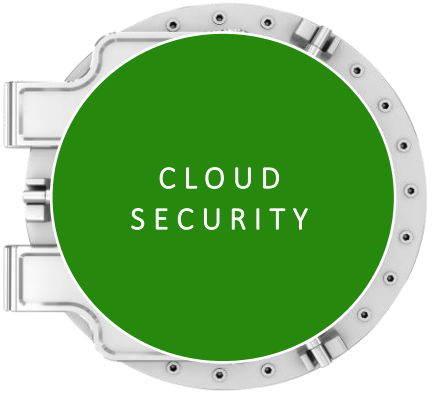
What are the emerging cyber risk mitigating controls that financial service organizations are exploring or investing in?

WHAT IT'S ALL ABOUT

As organisations embrace new technologies and cyber threats evolve the security approach should also change to equip businesses meet new challenges.

- Over 60% organisations likely to adopt zero trust strategy by 2025.
- Key drivers in FS include improving customer authentication, enabling rapid cloud adoption, reducing audit and compliance costs.

- Increasing focus on 'shift left' and 'secure by design'.
- Closely aligned to digital transformation and cloud migrations.
- Product aligned operating models with cyber integrated horizontally for success.



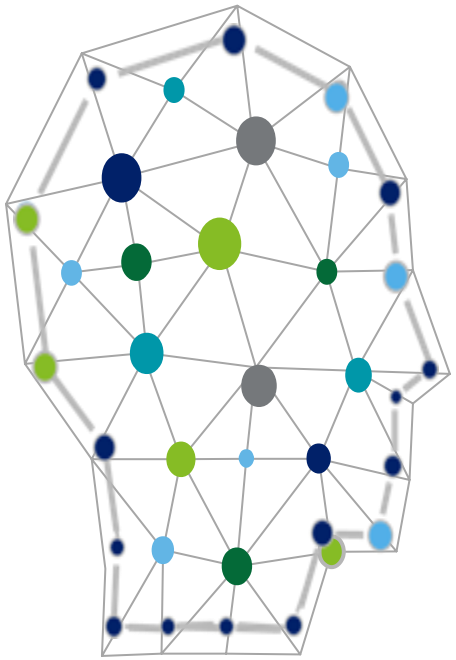
- Major shift in security model to embed Infrastructure as Code (IaC), supported by architectural patterns and tooling such as Cloud Security Posture Management (CSPM).
- Increased focus to drive continuous monitoring for drift and improvement.

- Significant investment and prioritisation on cyber vault, playbooks and rehearsing them in order to respond to ransomware attacks.
- Regulators expectation on FS increased especially to identify and prioritise recovery of important business services.

Deloitte's 2023 Global Future of Cyber Survey Insights

WHAT IT'S ALL ABOUT

Deloitte conducted a Global Future of Cyber Survey to obtain insights from 1,000 cyber decision-makers at the director level or higher, across 20 countries and limited to organizations with at least 1,000 employees and US$500 million in annual revenue.



CYBER BEYOND

- Cyber is evolving into a distinct functional area of the business.
- Transcending traditional IT roots and becoming an essential part of the framework for delivering business outcomes.

SAAVY BOARDS

- Cyber as a business priority is becoming more evident at the board level.
- 70% of respondents reported that cyber was on their board's agenda on a regular basis, either monthly or quarterly.

DIGITAL TRANSFORMATION

- Executives see cyber playing a crucial role in all digital transformation priorities.
- Secure design, execution and operation of these change initiatives is essential to counter cyber threats.

INVESTING IN TALENT

- Organisations embarking on major transformation programs facing talent challenge.
- Cyber teams and capabilities are stretched to maximum.

DIVERSE ECO SYSTEMS

- Whilst deploying tools and services from different vendors increases cyber readiness the complexity that can come with it could provide an entrée to new risks, including breaches.

Negative consequences resulting from cyber incidents and breaches	2021 (Rank)	2023 (Rank)	2023 (Percent)
Operational disruption *(including supply chain/or partner ecosystem)*	1	1	58%
Loss of revenue	9	2	56%
Loss of customer trust/negative brand impact	4	3	56%
Reputational loss	5	4	55%
Defunding of a strategic initiative	N/A	5	55%
Loss of confidence in tech integrity	N/A	6	55%
Negative talent recruitment/retention impact	8	7	54%
Intellectual property theft	2	8	54%
Drop in share price	3	9	52%
Regulatory fines	7	10	52%
Change in leadership	5	N/A	N/A

Key Takeaway Questions

As cyber threats increase and firms worldwide bolster their cybersecurity budgets, the regulatory community is advancing new requirements and increasing their scrutiny on how Boards and C-suite execs managing cyber risks of their organisations.

Takeaway Questions

01 Does the firm have **ownership**, and **effective management** of Cyber risk? Are the critical assets and services identified?

02 What are the **current and emerging cyber threats** to the firm?

03 Did the firm establish an appropriate **Cyber risk escalation framework** that includes **Cyber risk appetite** and reporting thresholds?

04 How do the **Cyber risk capabilities** align to **industry standards** and **peer organisations?**

05 Is the firm focused on, and **investing** in, the right **Cyber risk mitigating controls**? How are the results evaluated?

06 Is there **Cyber-focused mindset** and **Cyber-conscious culture** organisation wide?

07 What has the firm done to protect the organisation against **3rd party Cyber risks**?

08 Can the firm **rapidly contain damages and mobilise diverse response resources** when a Cyber incident occurs?

09 How does the firm evaluate the effectiveness of its **Cyber risk programme?**

10 Are there **resilience measures** in place to **swiftly recover critical services** from a catastrophic cyber incident?

The End

Contact Details:

Vamsi Krishna Meruva

Director, Risk Advisory

Deloitte UK

Email ID : vmeruva@deloitte.co.uk

Deloitte.