Why incident response preparedness helps improve digital operational resilience, regulatory response and C-Suite support.

DIGITAL RESILIENCE

Prepared for BCS – The Chartered Institute for IT

Bruce Keeble 12 March 2024
4:00pm-5:00pm

AGENDA

- Introduction
- What does cybersecurity mean to non-technical stakeholders?
- What do the statistics say?
- Defining resilience – the different flavours.
- Why I believe, incident response and crisis management helps build resiliency through preparedness.
- Governance – why is it mission critical?
- New legislation is driving the resiliency enforced need.
- Worst case scenario and is there a Plan B?
- Q&A

Note: My own personal perspective

A COMPARISON: NON-TECHNICAL PERSPECTIVE

Cybersecurity and resiliency – Different perspectives

What is cybersecurity, to different people?

I believe it should be more like a garden!

STATISTICS

Should numbers impact how we need to think and approach the journey to true resilience?

Cybereason stated in their true cost to business report:

- **Of those surveyed**, 46% estimate total business losses of USD$1-10 million and 16% estimate total business losses of over USD$10 million.
- **Dwell Time:** 56% didn't detect a breach for 3-12 months.
- **The true cost is staggering** –Not to mention the loss of revenue, brand damage, and layoffs that followed.
- **Attackers are evolving and the supply chain shows weakness** – 41 percent of the attackers getting in, via a supply chain partner.
- **Businesses don't have the right tools** – Less than half said their businesses are adequately prepared for the next attack. Whilst 87 percent of organisations increased spend, only 41 percent feel they have the right people and plans in place to manage the next attack.

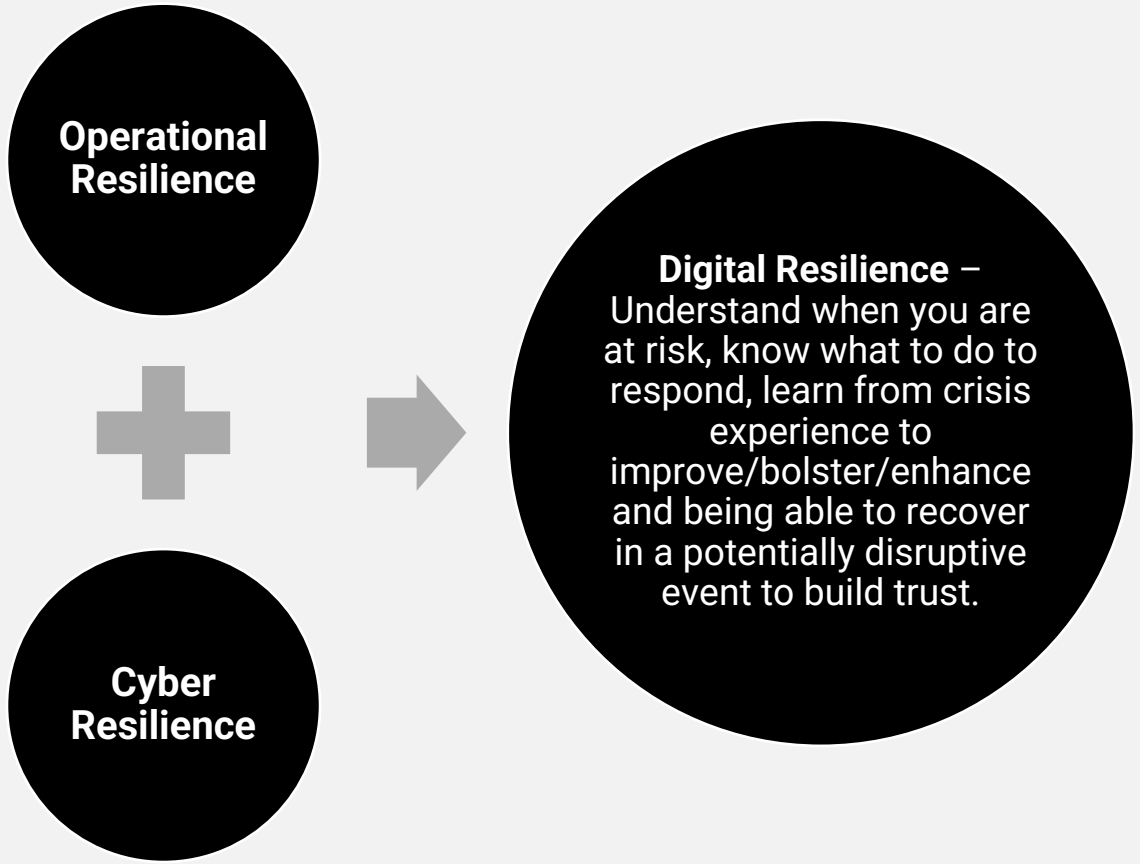
Question: What other information cannot or is not captured?

Reference: https://www.cybereason.com/ransomware-the-true-cost-to-business-2024

WHAT IS DIGITAL RESILIENCE

Should this impact what we need to think about what true resilience is?

Digital Resilience / Operational Resilience / Cyber Resilience



How does digital resilience differ from operational and cyber resilience?

Cyber and **Operational resilience** are both core components of adopting **Digital Resilience**.

Digital resilience is vital to maintain your ability to operate in a disruption and evolve to take advantage of new conditions and technology advancements to all kinds of crises to accelerate and innovate.

Building cross-functional crisis management, BCP, and continuous monitoring, to break down siloed digital environments in often, complex and across sophisticated technology teams.

WHAT IS DIGITAL RESILIENCE

Resiliency means the same thing for everyone, right?

Digital Resilience / Operational Resilience / Cyber Resilience

Operational Resilience – the ability of an institution to deliver critical operations through disruption to operate within their impact tolerances (ensuring risk identification and management, adaptive governance, business continuity plan, IT resilience, Crisis Management and Response.)

Cyber Resilience – Focused on protecting the digital assets: the ability of an organisation to prepare, identify, respond and recover from an information security incident. This is underpinned by risk-focus assessments and acknowledging an incident will happen.

How does digital resilience differ from operational and cyber resilience?

Cyber and **Operational resilience** are both core components of adopting **Digital Resilience**, which is where organisations, employees and individuals are in need of strategic alignment with the company.

Adapting to an **all-hazards disruption event** ranging from cyber threats such as ransomware, insider threat, data leakage, business continuity, and **non-cyber events** such as natural disasters.

Why incident response, crisis management capability and preparedness is a primer for enhanced resilience?

Incident response and Crisis Management teaches how to manage a crisis from the Board level down to technical and operational teams.

Expertise in this field, indelibly embeds both technical and soft skill expertise, to input to a variety of internal and external stakeholders. This includes supporting the strategy in different jurisdictions, where self-reporting early on to regulators, is mandatory.

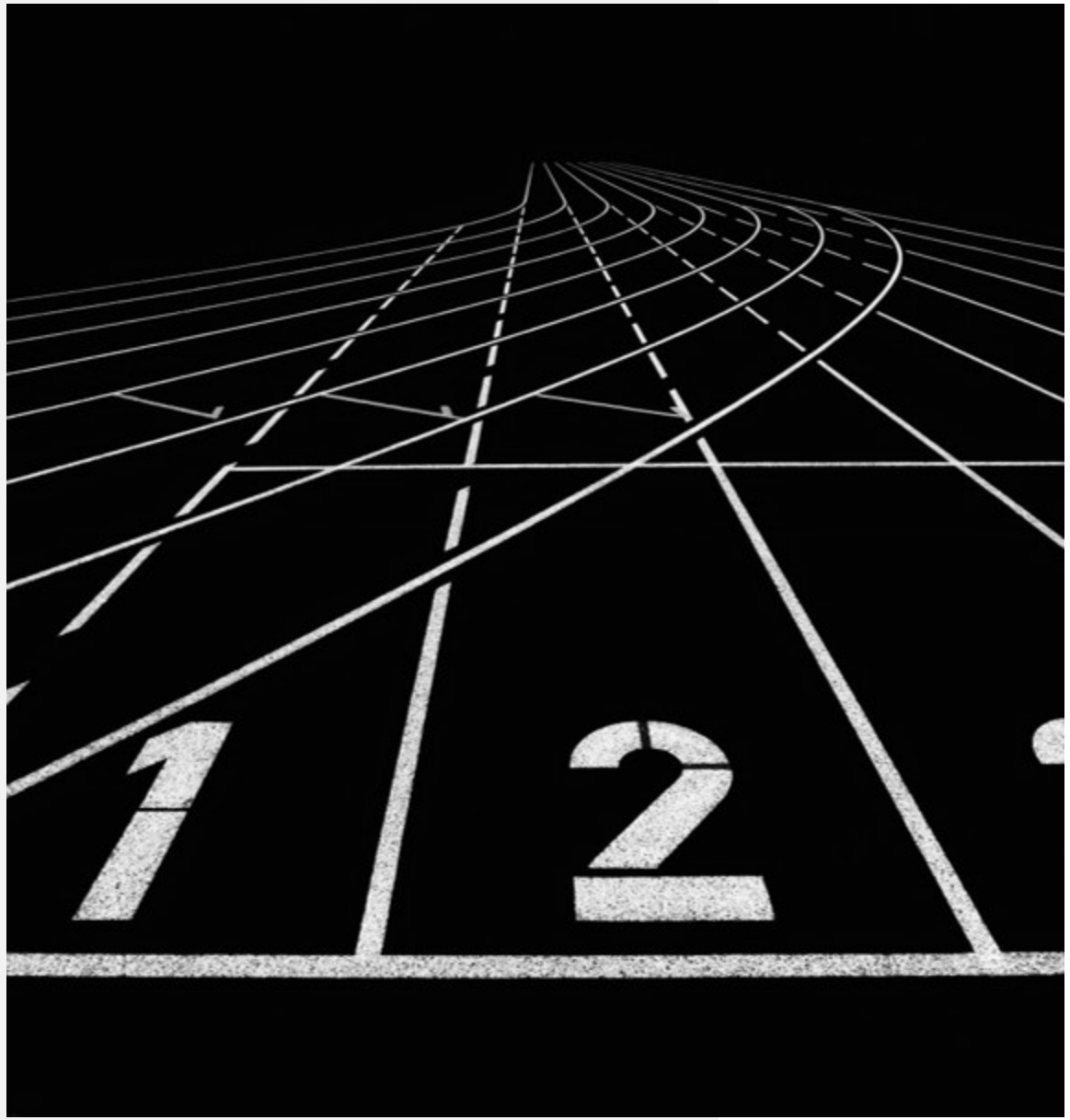
Incorporating the resiliency standards such as **ISO 22301:2019 (BCMP)** with good practice guidelines such as **ISO 22361:2022 (Crisis Management)** which emphasizes an all-hazards approach (and not just a cyber related crisis) can help organisations steer the resiliency program.

Why are the IR skillsets supportive of digital resiliency?

1) Have a plan
2) Practice and learn the plan
3) Implement the plan
4) Lessons learned and after-action-review

These reactive IR skillsets, can be used proactively, to address and mitigate risk before an operational or cyber crisis occurs.

Arguably, they are essential skills with supporting the Board and regulatory response in a crisis, but coming out of a crisis, building trust in peace time.



References:
https://www.iso.org/standard/50267.html
https://www.iso.org/standard/75106.html

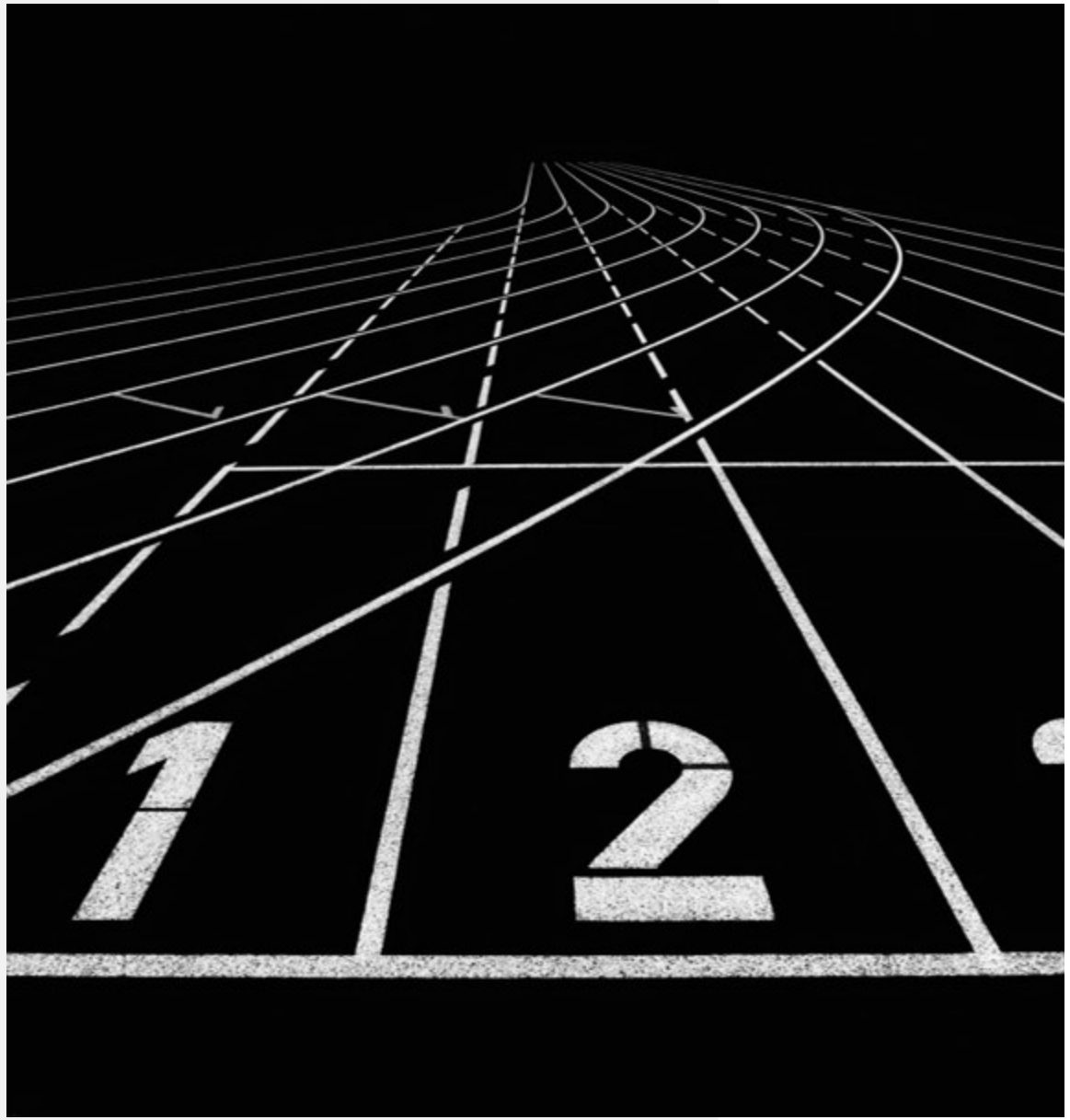
Why is governance, mission critical?

The National Institute of Standards and Technology (NIST) released their 'draft' Cybersecurity Framework (CSF) with version 2.0.

Governance is important to cybersecurity by integration into the business operations to reduce the potential impact and sharpness felt following interruption due to a root cause cyber related threat and the impact that follows.

The Board, senior stakeholders, and heads of product teams (and more) are responsible!

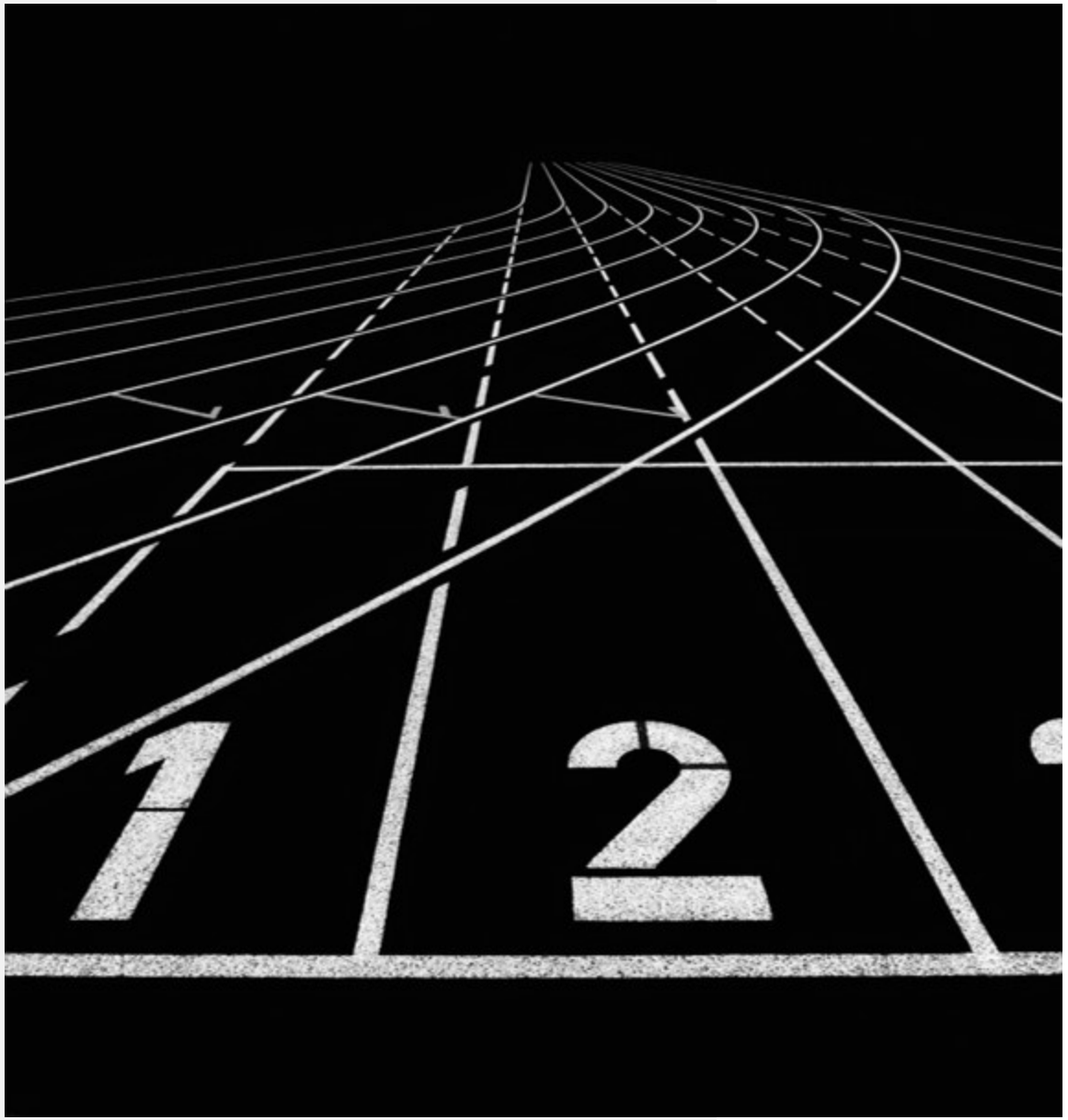
The addition of a "Govern" function to the pillars of a successful and holistic cybersecurity program. "Govern" represents the sixth function, along with "Identify," "Protect," "Detect," "Respond," and "Recover."



Reference: https://www.nist.gov/news-events/news/2023/08/nist-drafts-major-update-its-widely-used-cybersecurity-framework

Why is governance, mission critical?

- There are many frameworks and policies, but the complexity of budgets, across the work force geographies, means there are nuances and evolving changes in risk.
- The aim (in my opinion) is to complement cybersecurity needs and activities that support the business strategic goals. This often means honest and upfront discussions to debate, ensuring self-challenge and independence (also from a different vendor perspective so no marking your own homework).
- Cybersecurity governance requires:
  - Strategic view of how you control its security
  - Define risk tolerance, threshold and appetite
  - What about accountability?
  - Who is responsible and who can make mission critical (even brutally tough) decisions?
- The Board, senior stakeholders, and heads of product teams (and more) are responsible!



Why is legislation forcing resilience to be addressed?

UK and EU legislation is driving the need for resiliency. The requirements for business entities include, particular with financial service entities:

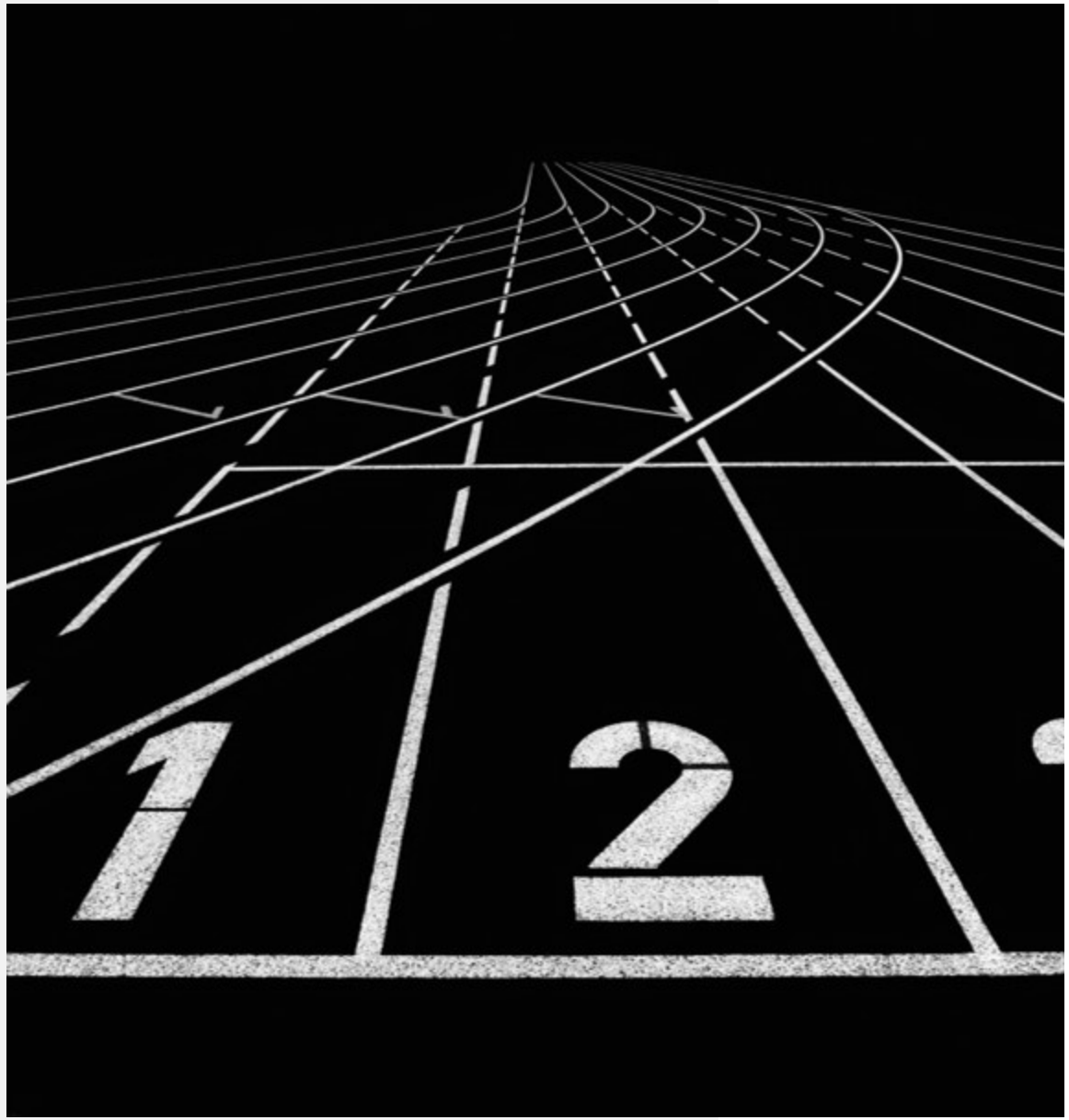
•identification of important business services that, if disrupted, could cause intolerable harm to consumers of your firm or risk to market integrity, threaten the viability of firms or cause instability in the financial system

•set impact tolerances for the maximum tolerable disruption to these services

•perform mapping and testing to a level of sophistication necessary to identify important business services, set impact tolerances and identify any vulnerabilities in your operational resilience

•perform and include processes that encompass a lessons learnt exercise to identify, prioritise, and invest in your ability to respond and recover from disruptions as effectively as possible

•develop internal and external communication plans for when important business services are disrupted



Reference: www.fca.org.uk/firms/operational-resilience

WORST CASE SCENARIOS?

Just how bad can it get and what pragmatic approaches are potentially needed?

Example 1 – Threats of old!

What happens if an at scale, global cyber crisis occurs?

- In 2018, the **Trickbot, Ryuk and Emotet** (dropper, exfiltration and ransomware extort model) event impacted US entities. After a few months, UK and EU entities faced the same onslaught of impact, many victim organisations were simply **not prepared for the scale of impact** across borders.
- **Why was this important?** Existing vendors and internal information security teams were overwhelmed globally, and it was common place for vendors to decline or unable to accept incoming (well paid) engagements simply from being inundated.
- Then during lockdowns, came **Kasaya** (Independence Day) and **Log4j** (Thanksgiving)

Example 2 – Threats ahead?

What about the impact of innovative technology?

- **Cloud** – perhaps not the resiliency saviour if not strategically and intentionally deployed?
- **Weaponised AI** – malware/social engineering
- Quantum computing (and encryption) requiring more GPU power (Graphics Processing Unit)
- **Supply chain** – entities are not having strong enough and fail-safe backup plans to a strategic vendor, if they have to sever B2B connections, leading to increased digital resilience and operational impact. **Exit strategies** are crucial!
- Data privacy impacts – software, personnel, new technology!

Q&A

THANK YOU

Find out more about BCS (The Chartered Institute for IT) here: https://www.bcs.org/about-us/