

# Security Dashboards, Metrics and Data

Management Insights to see  
through the Maze



The Security Transformation  
Research Foundation



Security Dashboards,  
Metrics and Data

Communicating and driving real engagement with senior stakeholders around cyber security has always been one of the most complex aspects of the CISO role

# Seeing through the Maze

- As digital estates become increasingly complex, attack surfaces are multiplied and most organisations face the same challenge:
- How do we make sense of the data we have to protect ourselves from cyber threats and drive real action around cyber security?



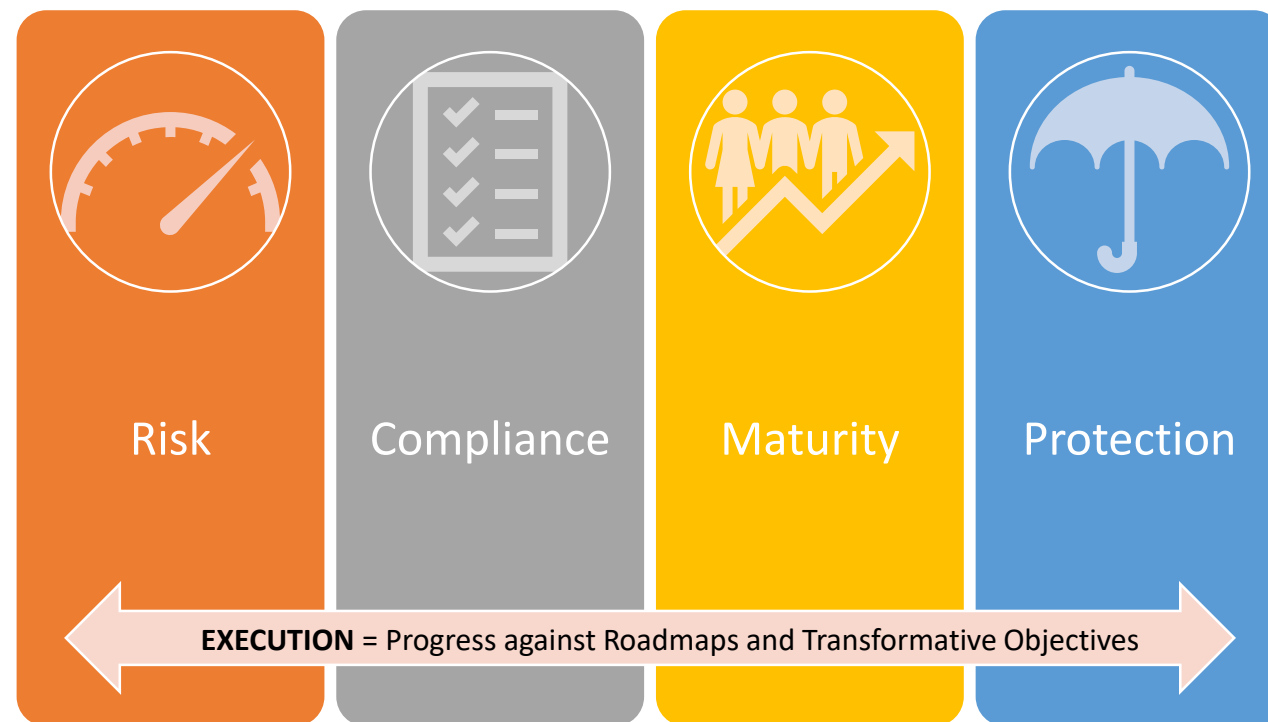
# Dashboards

At least 5 different angles

## Security Dashboards, Metrics and Data

### Dashboards

- Dashboards are essential to communicate around security with senior stakeholders
- Their focus, format and content will vary depending on the degree of security **literacy** and the expectations of each audience, but they can only work as long as they are rooted in the **management and governance culture** of each firm
- Each approach will require a relevant **narrative** to be provided by Security leaders to the target audience supported by relevant data





# Audiences

## 3 broad groups of interests



## Security Dashboards, Metrics and Data

### Audiences

- The audiences for each Dashboard will have diverse key interests – each requiring a specific narrative – but all are faced with a common problem: A constant deluge of management data
- For the Security message to be heard, each audience must be addressed in their own language and in **clear and relevant** terms
- There cannot be a single approach e.g. a metric on patch deployment (on its own) may be irrelevant to ARC members but useful to security management

Security Dashboards,  
Metrics and Data

Key  
Takeaways  
from our  
Focus Groups

# Dashboards & Audiences



## **1- Don't over-simplify**

Security cannot be reduced to a simplistic list of black and white “do’s and don’ts”: Use the dashboards to educate stakeholders where necessary

## **2- Don't window-dress**

Avoid the “watermelon syndrome” (green on the outside; red on the inside): Paint things as they are to build credibility and trust, and drive genuine risk treatment

## **3- Tailor to each audience and focus on actionable outcomes**

Use the power of the each audience to drive action where needed

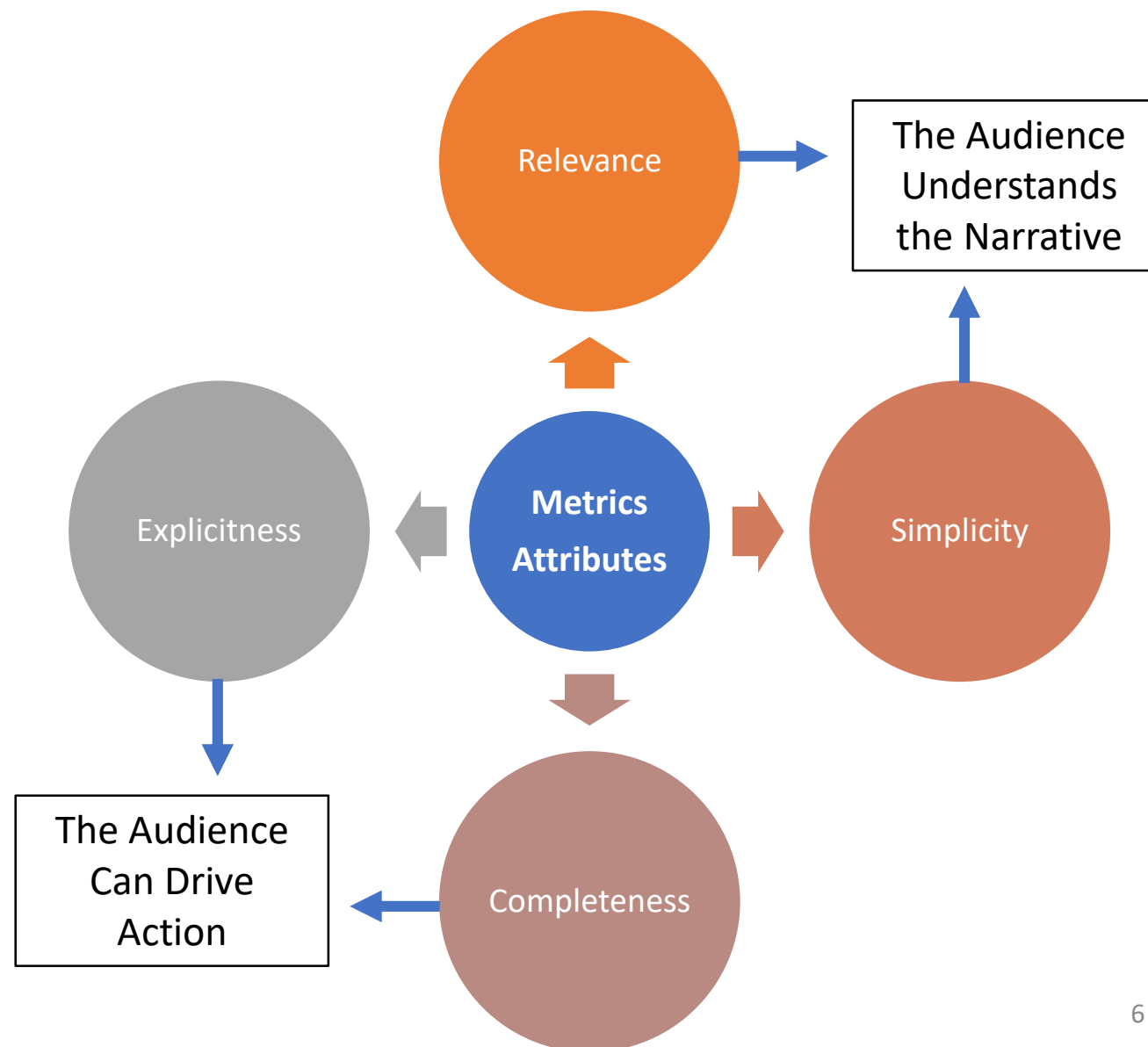


# Metrics

## Security Dashboards, Metrics and Data

### Metrics

- Metrics must underpin any dashboard. An **objective and quantitative** approach is essential to chart progress, but rarely sufficient in isolation: The **subjective and qualitative** elements – in particular around people, behaviours and awareness – cannot be missed
- Building meaningful metrics requires efficient and repeatable data collection and aggregation processes to be in place, on a scale sufficient to **accurately** address the expectation of each audience





Security Dashboards,  
Metrics and Data

Key  
Takeaways  
from our  
Focus Groups

# Metrics

## 1- Don't give too much away

Stay relevant and concise: Use the dashboards to build a dialogue with each audience

## 2- Security is not just about IT

Do not focus only on technology metrics: Engage with – and collect data from – all relevant stakeholders (HR, business units, etc...)

## 3- Prepare responses to the “so-whats”

Each audience may engage differently with the metrics: This will be underpinned by their own understanding of the context or cognitive biases

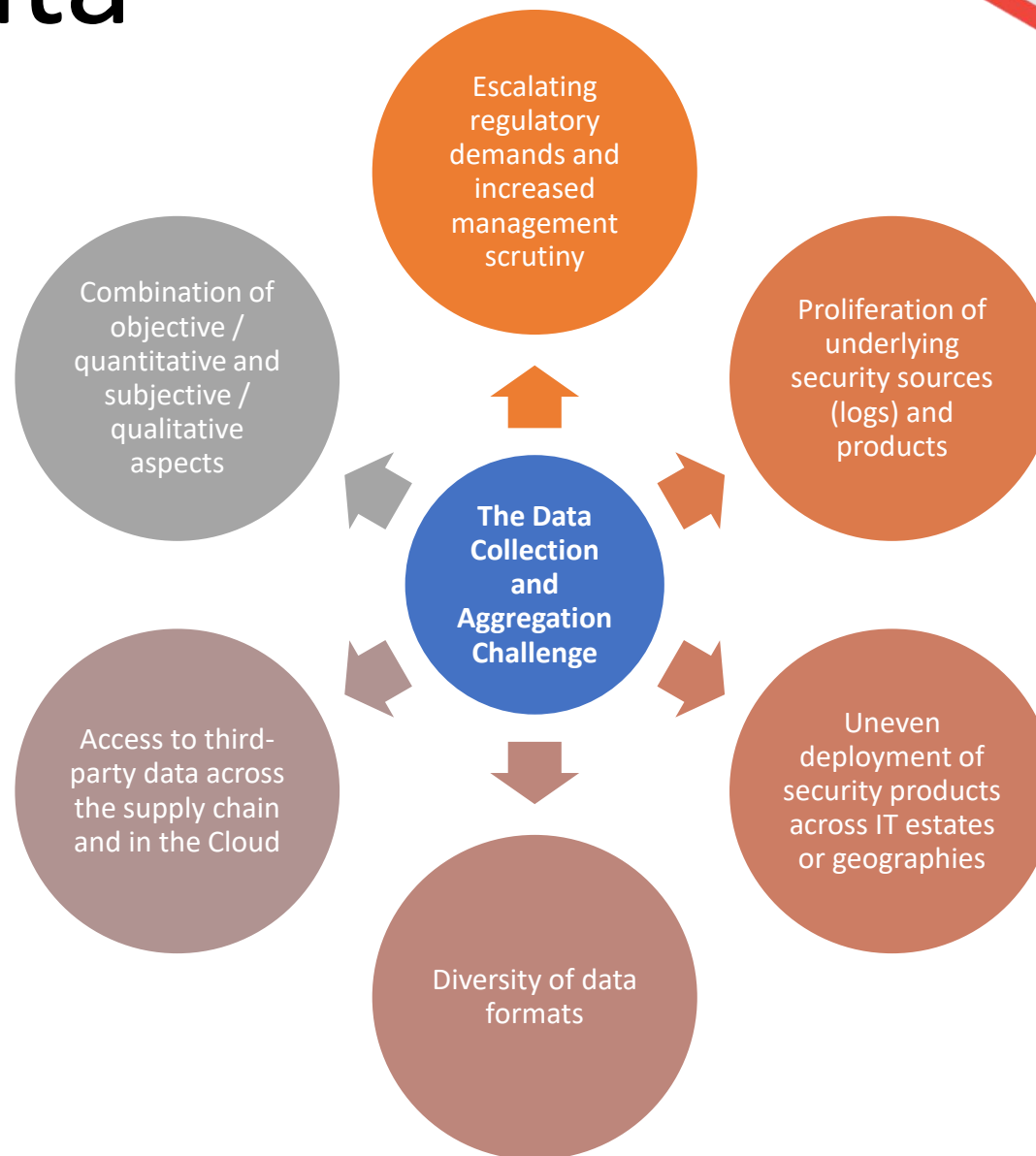


# Data

## Security Dashboards, Metrics and Data

### Data

- **Data Quality** underpins Metrics and their Accuracy
- The **Accuracy** of Metrics underpins the **Trust** in the dashboards and their **Value** for stakeholders
- But the complexity of real enterprises in today's digital world undermines data **Completeness** (cloud, supply chain ecosystems, legacy systems etc...) and creates a considerable challenge for the reporting teams







# Reporting

## Security Dashboards, Metrics and Data

### Reporting

- Most Reporting Processes are still manual – at least in part – for many security teams
- This is error-prone, labour-intensive, repetitive and rarely motivating for security operators and analysts
- Beyond the costs involved and the immobilization of scarce security resources and skills which could be used on higher value-added tasks, it can develop into an attrition factor compounding the problem many CISOs have in staffing their teams



Security Dashboards,  
Metrics and Data

Key  
Takeaways  
from our  
Focus Groups

# Data & Reporting



**1- Focus on the efficiency of the collection and aggregation process, and automate as much as you can**

Manual reporting processes may sometimes be unavoidable but are expensive, demotivating for the staff and error-prone

**2- Collect and process what you need, not what you can**

Build on solid asset inventories and focus on metrics and dashboard objectives and the expectations of their audiences

**3- “Best-of-breed” is still a valid strategy around cyber security tooling but product proliferation must be managed**

Declutter the Security estate and consolidate data on intermediary portals to make reporting analysts and security operators more efficient

Security Dashboards,  
Metrics and Data

Many thanks to  
all contributors  
and to the CIO  
Water Cooler  
team



# Thank You

**Zsuzsanna Berenyi**

**Jean-Christophe Gaillard**  
(Corix Partners)

**Richard Preece**  
(DA Resilience)

**Rupert Brown**  
(Evidology Systems)

**Ben Holt**  
(Strata Security)

**Brian Roche**  
(Belfast City Airport)

**Chris Burtenshaw**  
(Strata Security)

**Steve Lamb**

**Justyna Schultz**  
(Mimecast)

**Steve Collins**  
(First Quantum  
Minerals)

**Jean-Marie Lapeyre**  
(PSA Group)

**Harvey Seale**  
(Mimecast)

**James Willans**  
(Lhasa)



# The Security Transformation Research Foundation

The Security Transformation Research Foundation is a dedicated think-tank and research body aimed at approaching Security problems differently and producing innovative and challenging research ideas in the Security, Business Protection, Risk and Controls space

[www.securitytransformation.com](http://www.securitytransformation.com)



@Transform\_Sec



The Security Transformation  
Research Foundation