RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: CXO-R11

The Fine Art of Creating A Transformational Cyber Security Strategy

Jinan Budge

Principal Security & Risk Analyst
Forrester Research

FORRESTER®

Andrew Rose

Chief Security Officer
Vocalink, A Mastercard Company

VOCALINK
mastercard

Source: www.milanostyle.com

Source: www.unsplash.com

Source: www.unsplash.com

Without A Strategy, You Are Left Rudderless

An Intensifying Storm

Technology

Speed Of Business

Threat

Age Of The Customer

A Good Security Strategy Transforms..

FROM	TO
An IT issue	An issue of customer trust
No, you can't	Yes, and
Technically focused	Holistic
Lock & keys	Freedom

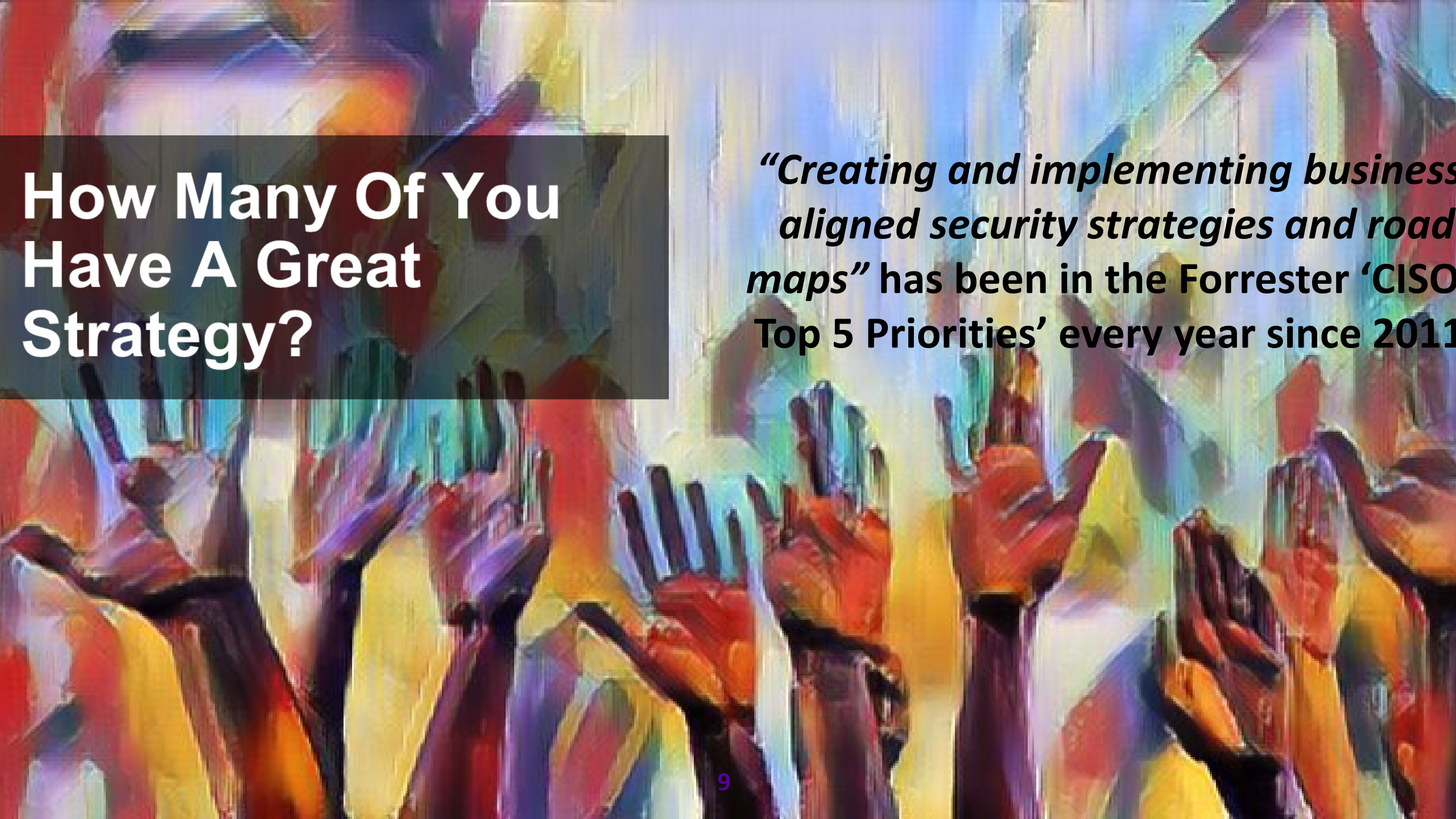
…And A Bad Strategy..

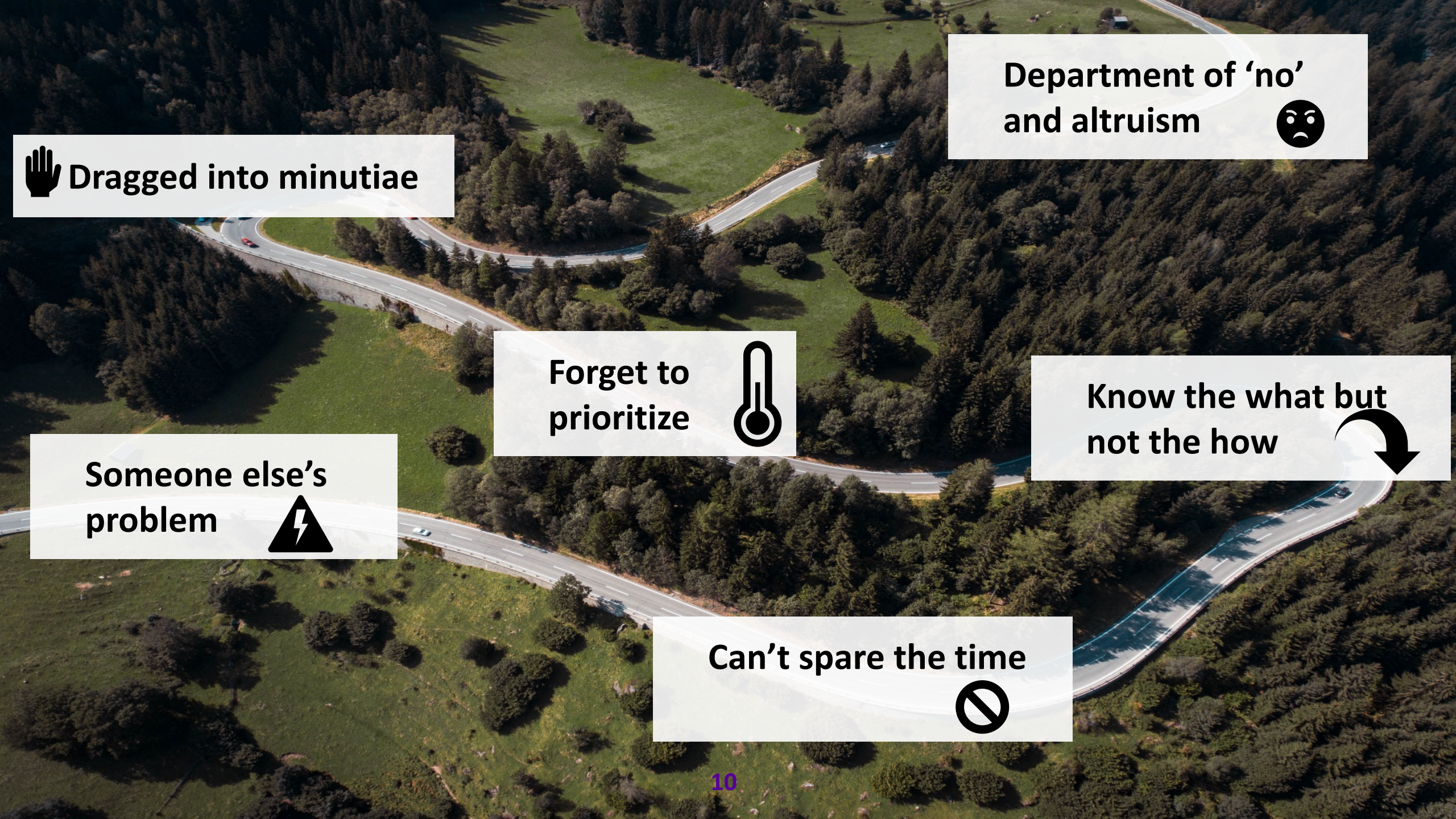
Suffer A Great Breach & Miss Smaller Ones

Continue To Invest In The Wrong Things

Spend Their Time Responding Tactically

Struggle To Attract And Retain


How Many Of You Have A Great Strategy?
"Creating and implementing business aligned security strategies and road maps" has been in the Forrester 'CISO Top 5 Priorities' every year since 2011


Department of ‘no’ and altruism
Dragged into minutiae
Forget to prioritize
Know the what but not the how
Someone else’s problem
Can’t spare the time

What Makes Or Breaks A Strategy

- Understandable
- Known
- Utilized and sustainable
- Business focused and risk-aligned
- People and culture at the heart

- Platitude
- Doesn’t consider people
- Shelfware
- One dimensional
- Inflexible


Three Paths To
Strategy

Decide On The Strategy Path You Want To Take

Each Path Has Pros And Cons

Risk-aligned Strategy

Benefits

- Drives a competitive spirit between business units
- Drives control maturity
- Good visuals & metrics to demonstrate risk reduction
- Transformative

Challenges

- IT focused maturity model drives the strategy, priorities are not driven by business goals
- Needs business unit engagement to collate data
- Aspects of 'marking your own homework'

Stakeholder Focused

Benefits

- Significant buy-in
- Embed security in all aspects of your business
- Customer and external stakeholder, regulator and peer support
- Transformative

Challenges

- High cost
- Significant change management skills
- Could be seen as overkill – short benefits are difficult to justify
- Outside of comfort zone of many CISOs

A Quick Tech Roadmap

Benefits

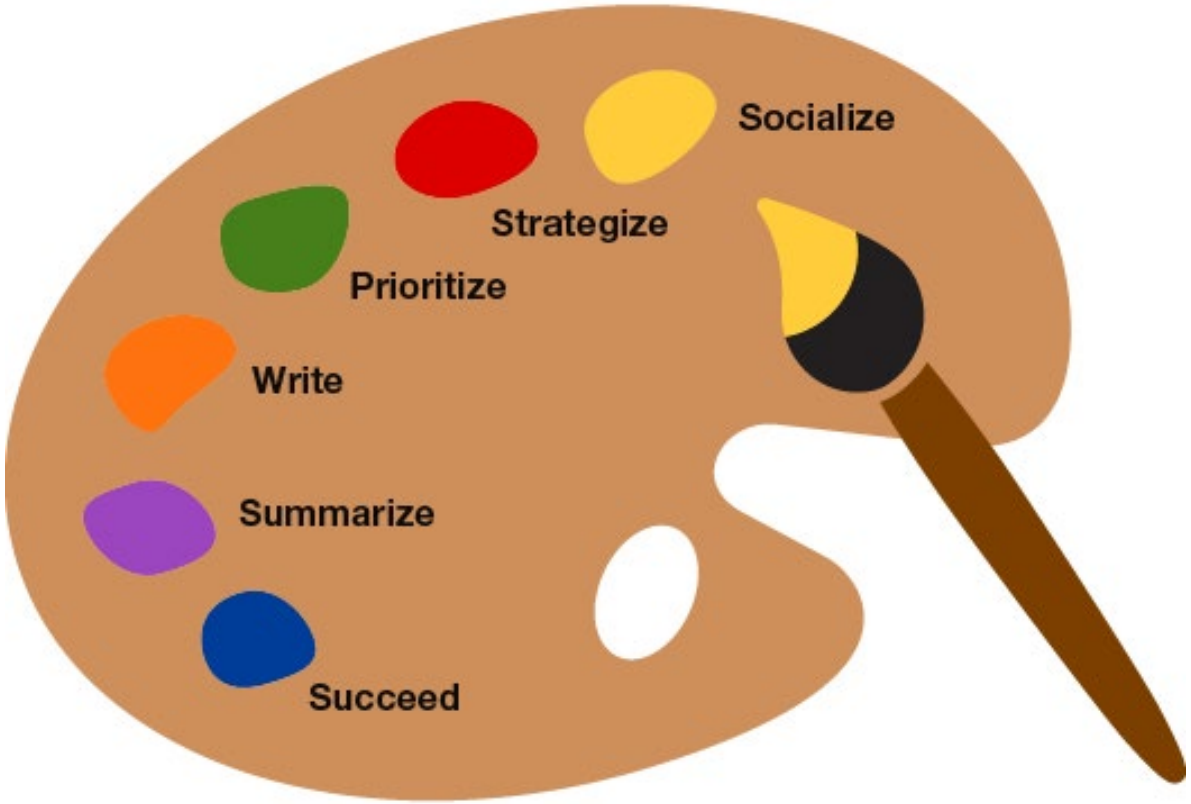
- Quick to do
- A 1-year plan
- Comfortable for CISO and security team

Challenges

- Insular and doesn't consider culture, business and customer
- Security remains a technology low level issue
- May miss elements of oversight, process and people
- Does not get the buy-in required for sustainable lasting change

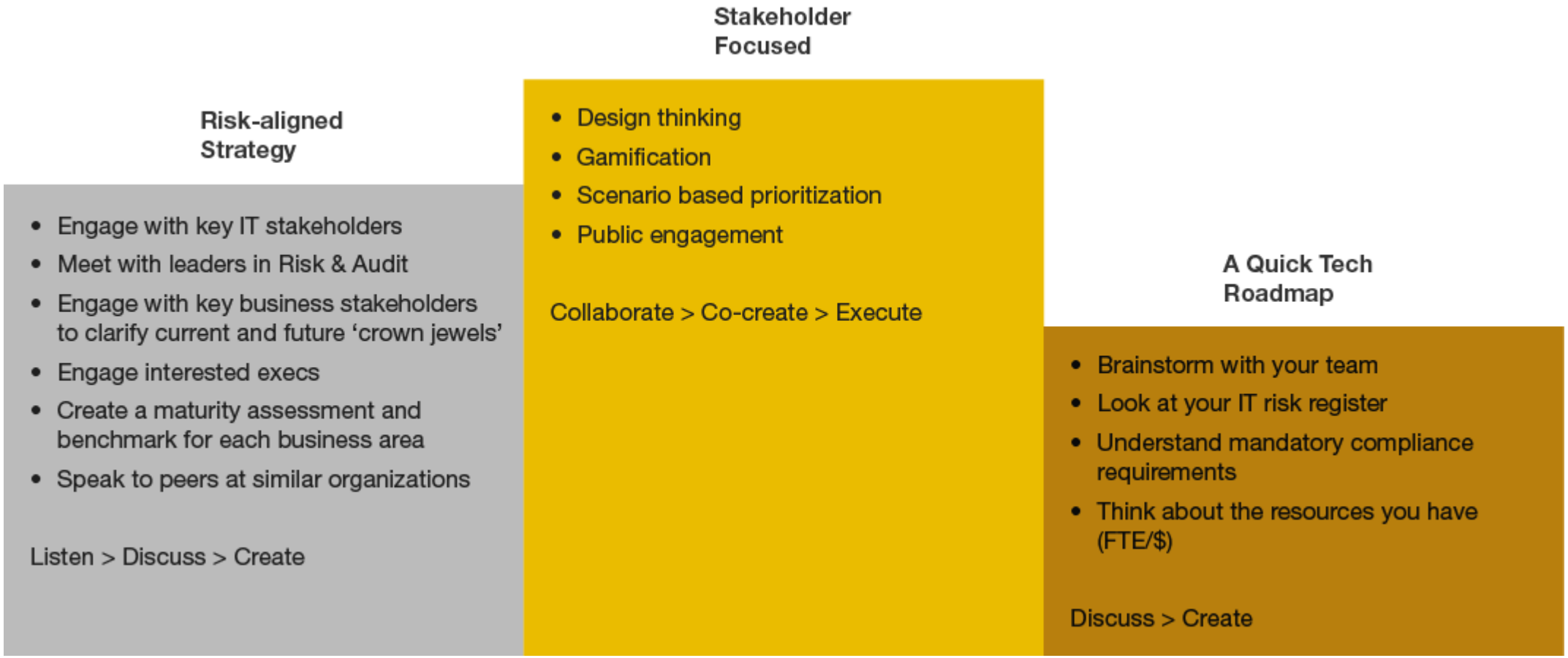
Choose Your Strategy Path Wisely Depending On…

Strategy Fundamentals: Part 1 - Socialize



- Socialize your strategy to gain visibility, budget and influence

Gather Data From Key Stakeholders



Perspectives From The Boardroom

- Cyber risk is a top business priority.
- Awareness and understanding of security: not perfect but improving. Translators required.
- Boards want to hear from and have a trusted dialogue with the CISO.
- Boards need transparency and risk.
- Normalizing the security conversation.

Security 101 – Do You Have Support?

Do you really have senior management support? Ask yourself:
✓ Have they committed to funding the program, or are they on the journey to offer funding?
✓ Do they understand that cybersecurity is a business risk?
✓ Is cybersecurity risk on the corporate risk register?
✓ Am I empowered by executive sponsors, and do I have direct access to them?
✓ Does my governance board represent my whole business, and at a level senior enough to make decisions?

Strategy Fundamentals: Part 2 – Strategize

- In taking the time to strategize, you consider
  - What is important?
  - Why does your role matter?
  - What's the point of it all?
- Strategize alone, with your team or in consultation with stakeholders
- Brainstorm on a whiteboard or piece of paper
- Ask yourself some hard questions

Mission Statement

Mission Example 1

CLEAR STATEMENTS OF AMBITION AND PURPOSE

1. Direct and assure

- Have a cyber security capability which protects the continued provision of 24/7 financial transaction services

2. Drive scalable security architecture

- Enable the rapid and safe realization of future business objectives

2. Leverage recent company acquisition

- Drive improvements in control and oversight

Mission Example 2

AN APPROACH TO LEADERSHIP FOR THE SECURITY FUNCTION

1. Commercially focused on how to help the business execute its vision

- Focus on how to make the business execute its strategy securely
- Good team player in the organizational ecosystem

2. Trusted partner for the business in strategic growth opportunities

- Collaborate with the business by providing security expertise that aids but does not hinder them

3. No net new security technology investment without clear business benefit

- Depart from old habit of technology acquisition without adequate business case. With clear value for the business and its strategy

Mission Example 3

MINISTER'S FOREWORD (NSW GOVERNMENT CYBER SECURITY STRATEGY)

Developing strong cyber capabilities that scale with our ambitious digital agenda, will be key to our success. By investing in cyber security today, we are enabling the NSW Government to accelerate digital transformation while providing confidence to citizens who trust us with their data and services.

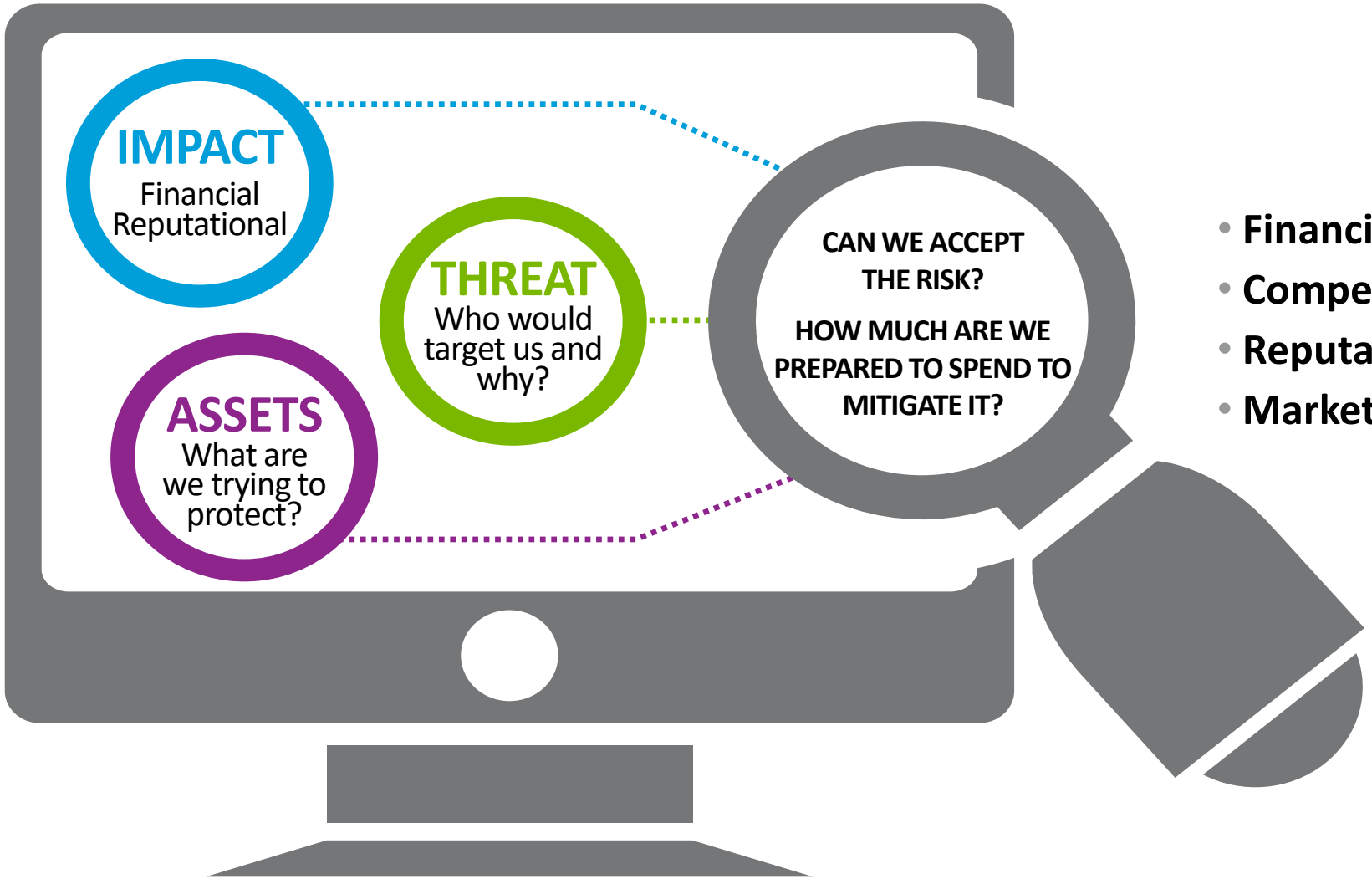
The Hon. Victor Dominello, Minister for Finance, Services and Property

Strategy Fundamentals: Part 3 – Prioritize

- Decide what's important
- Focus your program
- Justify decisions

Prioritization Takes Effort And It Depends On Your Path

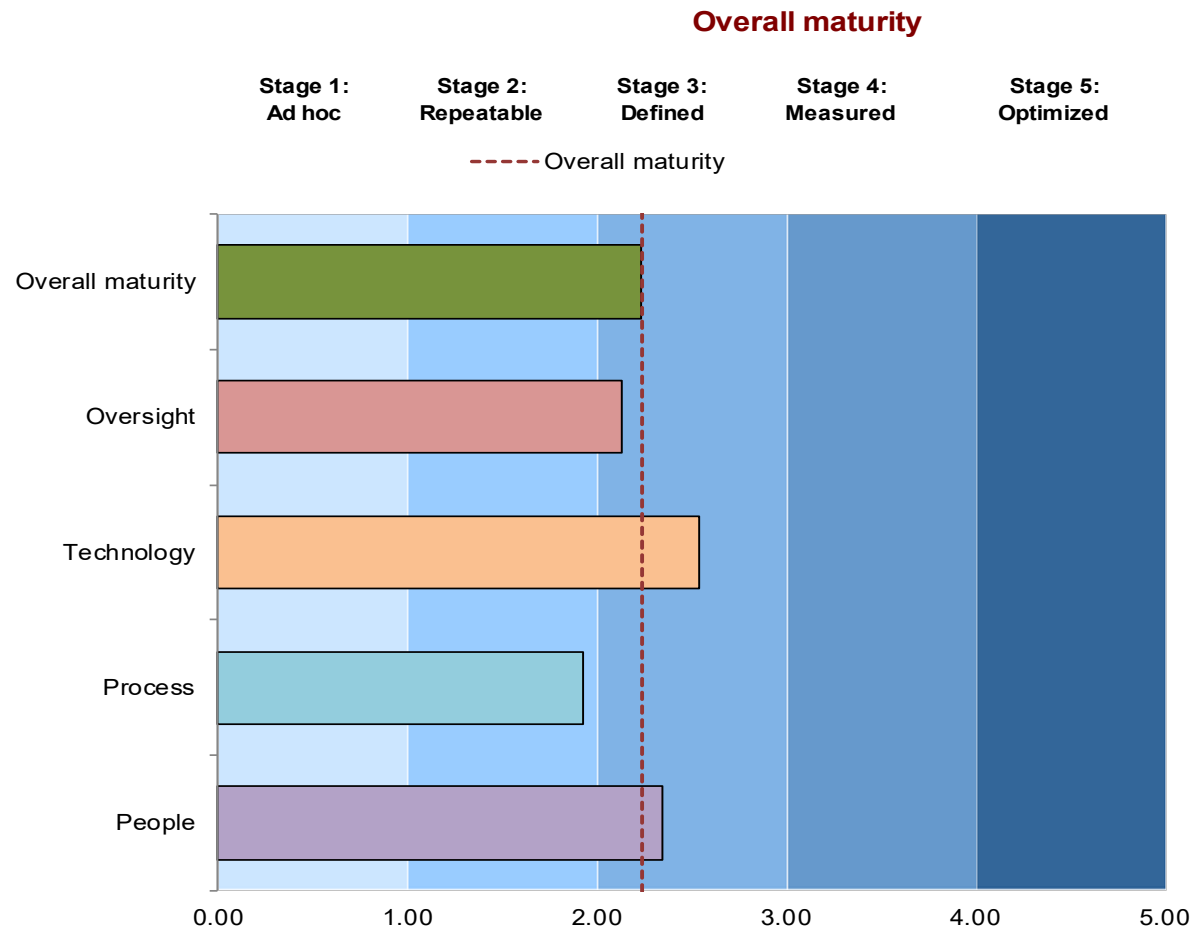
How Much Does It All Matter?



- **Financial performance**
- **Competitive advantage**
- **Reputation**
- **Market presence**

Security Performance Snapshot

USE RECOGNISED STANDARDS TO SELF ASSESS YOUR SECURITY AND HELP DEFINE GOALS



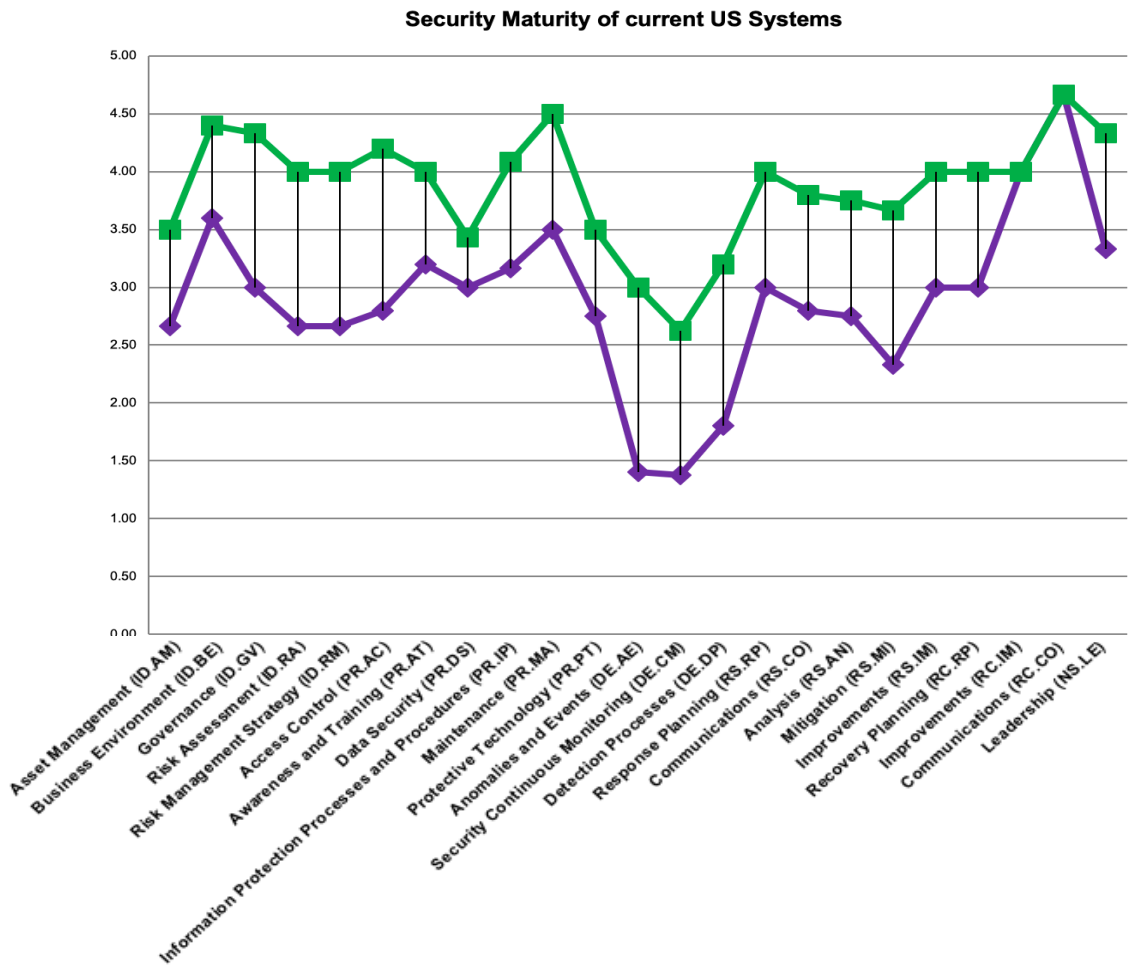
Overall maturity	2.24
Oversight	2.13
Technology	2.54
Process	1.93
People	2.35

*Stages are defined as follows: Stage 1 = 0.01-1.00, stage 2 = 1.01-2.00, stage 3 = 2.01-3.00, stage 4 = 3.01-4.00, stage 5 = 4.01-5.00.

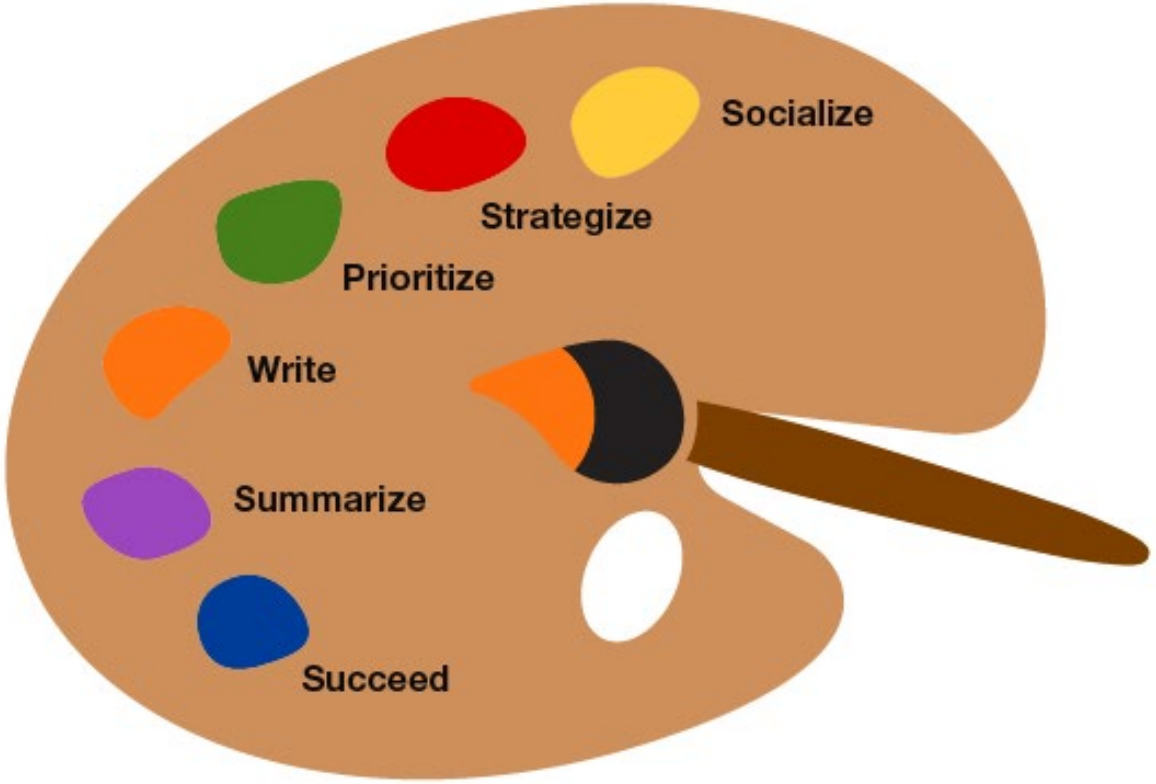
Source: Forrester Report, 'Assess Your Security Program With Forrester's Information Security Maturity Model'.

Security Performance Snapshot

USE RECOGNISED STANDARDS TO SELF ASSESS YOUR SECURITY AND HELP DEFINE GOALS

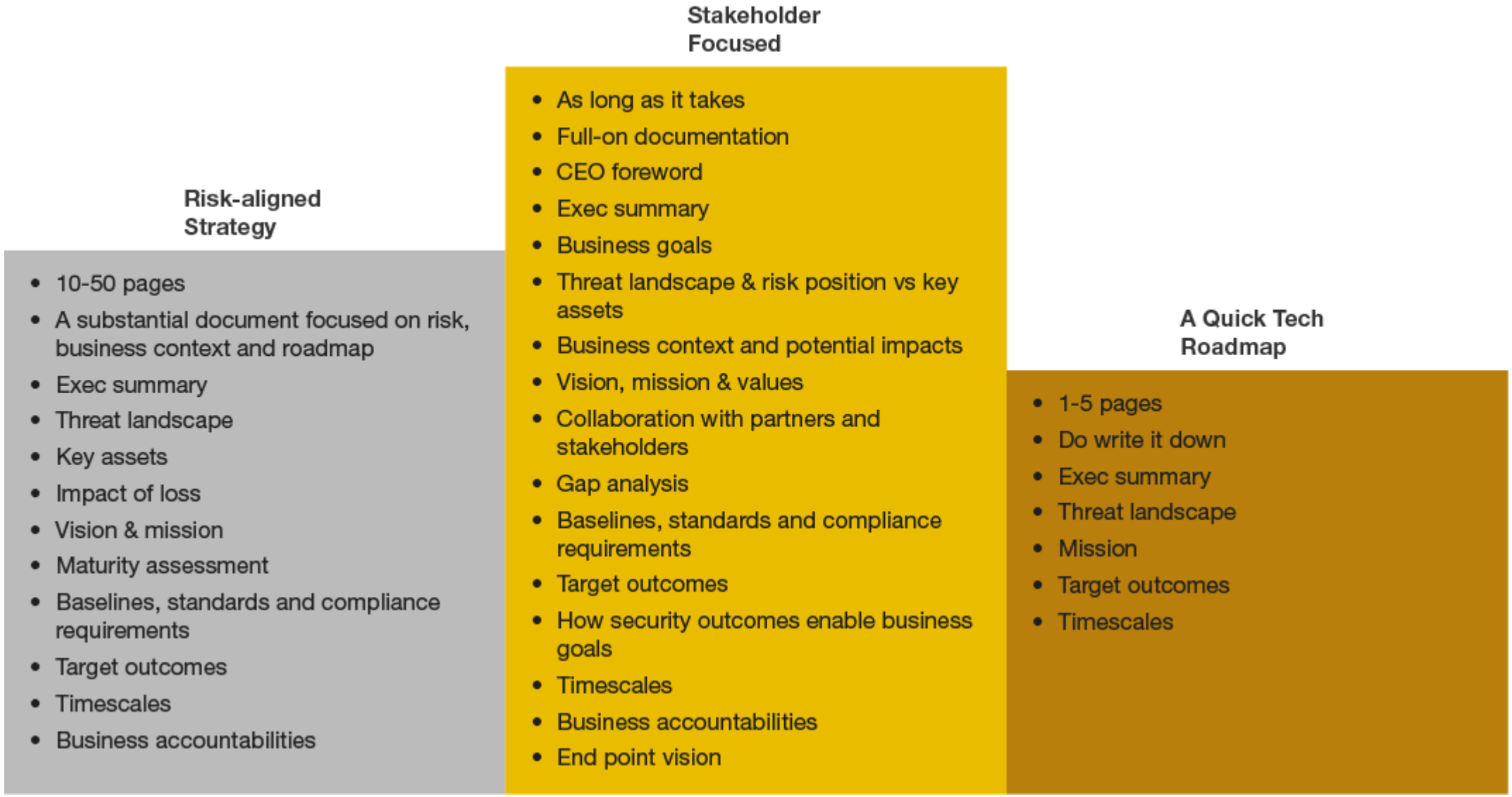


Strategy Fundamentals: Part 4 – Write

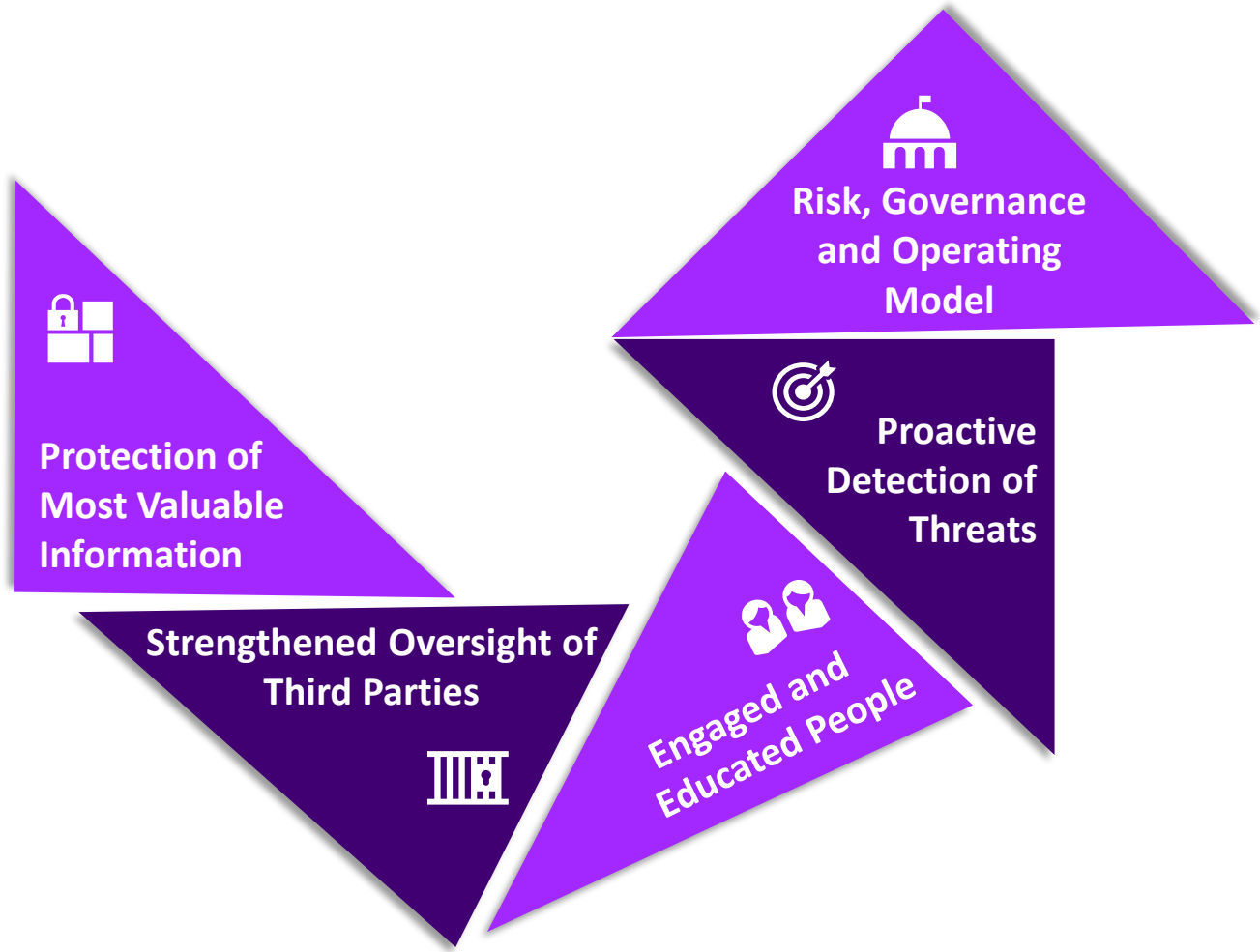


- Typically where people start, or stop
- No silver bullet
- It drives all actions, accountabilities and decisions
- The document is a means not the end

Document Your Strategy



A Holistic Approach Stops Your Strategy From Becoming Shelfware



Strategy Fundamentals: Part 5 – Summarize

- Remember your audience and your focus

Your Audience Will Vary

Risk-aligned Strategy

Your security governance board, and an interested VP, or SVP. Sometimes it includes your board and execs.

Stakeholder Focused

Top level Executive Management, The Board, Partners and Customers

A Quick Tech Roadmap

Your audience is you, your team and your boss

Create A Focus Sheet for Executives - Example

SHOW HOW SECURITY SUPPORTS BUSINESS OBJECTIVES

Security mission — "security will neither hinder nor halt our business."

Our current issues:	We will address this by:	Enabling the following business benefits:
• Low maturity security function as assessed during recent internal audit • Reactive to incidents rather than proactive • Inhibits business growth and not seen as a trusted business partner • Embryonic capabilities in most areas	• Transforming security function to become a trusted business partner • Addressing risks highlighted by audit • Delivering a forward-thinking security function that drives new technology adoption • Refreshing perimeter controls and enhancing monitoring capability	• 30% decrease in customer complaints related to security • 20% reduction in security waivers • Partnership scores of 8/10 on business projects that we support • Decrease in incidents based on 2015 to 2018 average

Overview of the security culture program

Overview of the security program

Create Your Own Focus Sheet

Your Vision of Cybersecurity

[Statement]

State of Cybersecurity [Year]
Top security business risks describing the initial state

Risk [Current State/Metric]

Risk [Current State/Metric]

Risk [Current State/Metric]

Risk [Current State/Metric]

Risk [Current State/Metric]

Key cybersecurity initiatives/projects

1. Security initiative/project 1
2. Security initiative/project 2
3. Security initiative/project 3
4. Security initiative/project 4
5. Security initiative/project 5

Key cybersecurity assumptions and requirements

1. [Assumption/requirement]
2. [Assumption/requirement]
3. [Assumption/requirement]
4. [Assumption/requirement]
5. [Assumption/requirement]

State of Cybersecurity In [Year]
Top risks describing the end state

Risk [Target State/Metric]

Risk [Target State/Metric]

Risk [Target State/Metric]

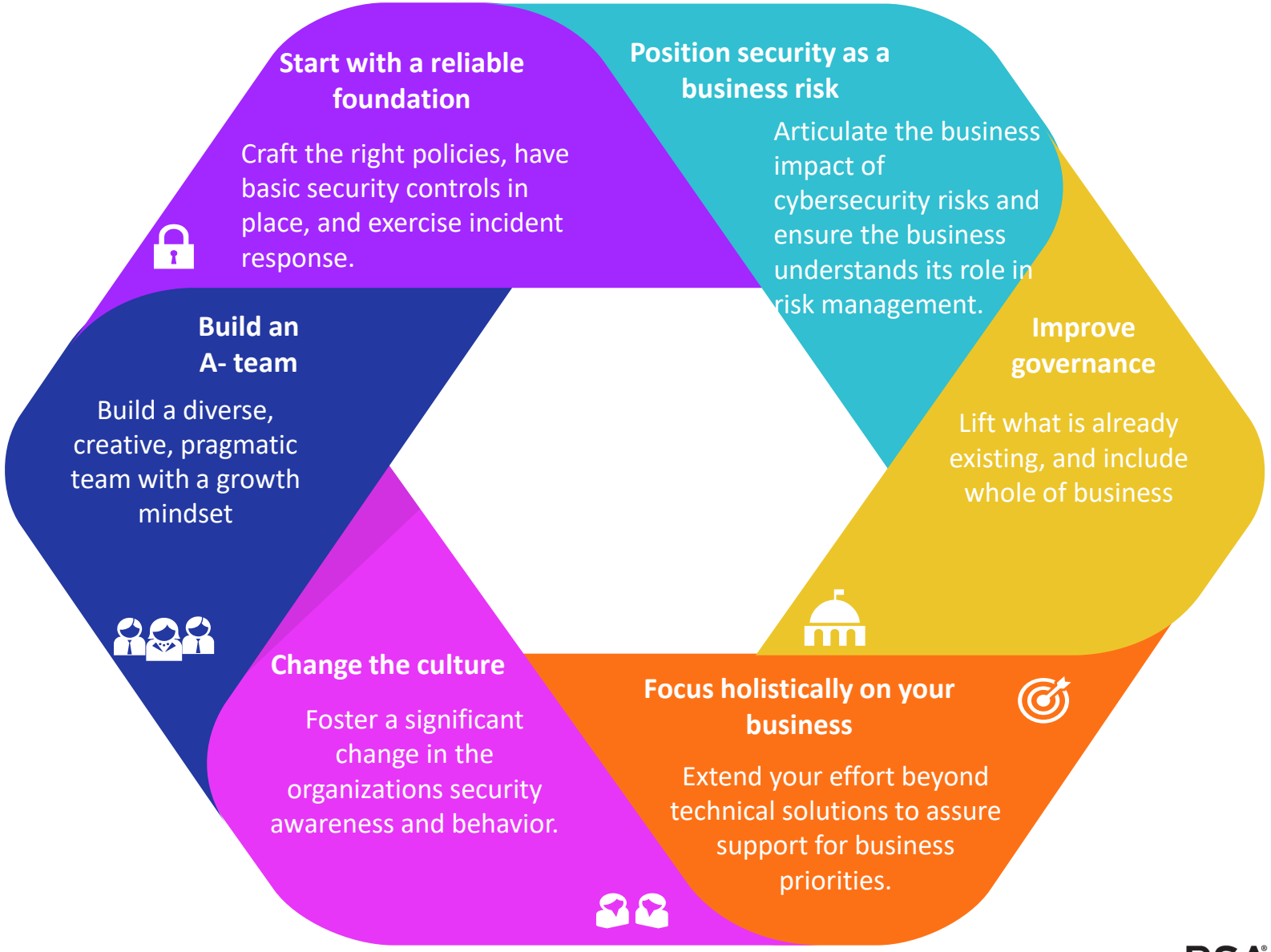
Risk [Target State/Metric]

Risk [Target State/Metric]

Strategy Fundamentals: Part 6 – Succeed

- Follow key principles for a successful transformation

Principles of A Successful Transformation



How Will You Create Your Strategy?

Apply What You Have Learned Today

- **Next week you should:**
  - Decide what your strategy path is
  - Identify influential key stakeholders, and how they can be part of your strategy and transformation
- **In the first three months following this presentation you should:**
  - Define your mission statement, co-creating if appropriate
  - Be clear on your security program priorities
- **Within six months you should:**
  - Build a right-sized, risk-based, business aligned cybersecurity strategy document
  - Socialize your strategy with your key stakeholders

RSAConference2019

Q&A

Jinan Budge, Principal Security and Risk Analyst, Forrester

Andrew Rose, Chief Security Officer, Vocalink, A Mastercard Company

References

Source: North American Consumer Technographics Consumer Technology Survey Q2, 2014 and Consumer Technographics® North American Online Benchmark Survey (Part 2), 2017

See Forrester Report, "Use Forrester's CISO strategic Canvas To Align Security With Business", November 2018

See Forrester Report, "How To Talk To Your Board About Cybersecurity", December 2018

See Forrester Report, "Instill A Security Culture By Elevating Communication", October 2018

See Forrester Report, "Transform Your Cybersecurity Capability", August 2018