Cybersecurity: A Strategic Opportunity

Leveraging the CPD Framework for Competitive Advantage

GDS Summit – Dinner Keynote Address

May 28, 2025

Dave Chatterjee, Ph.D.
Duke University

Disclaimer

Fair Use Notice and Disclaimer

This presentation deck may contain copyrighted material the use of which has not been specifically authorized by the copyright owner. The fair use doctrine allows the presenter limited use of copyrighted material without requiring permission from the rights holders, such as commentary, criticism, news reporting, research, teaching or scholarship. It provides for the legal, non-licensed citation or incorporation of copyrighted material in another author's work under a limited balancing test. The material shall be used to enhance public understanding of cybersecurity preparedness, as such, the presenter believes this constitutes a fair use of any such copyrighted material as provided for in section 107 of the US Copyright Law. In accordance with Title 17 U.S.C. Section 107, this presentation is distributed without profit to those who have expressed a prior interest in receiving the included information for research and educational purposes. If you wish to use potentially copyrighted material from this presentation for purposes of your own that go beyond fair use, you must obtain permission from the copyright owner.

Errors and Omissions Disclaimer

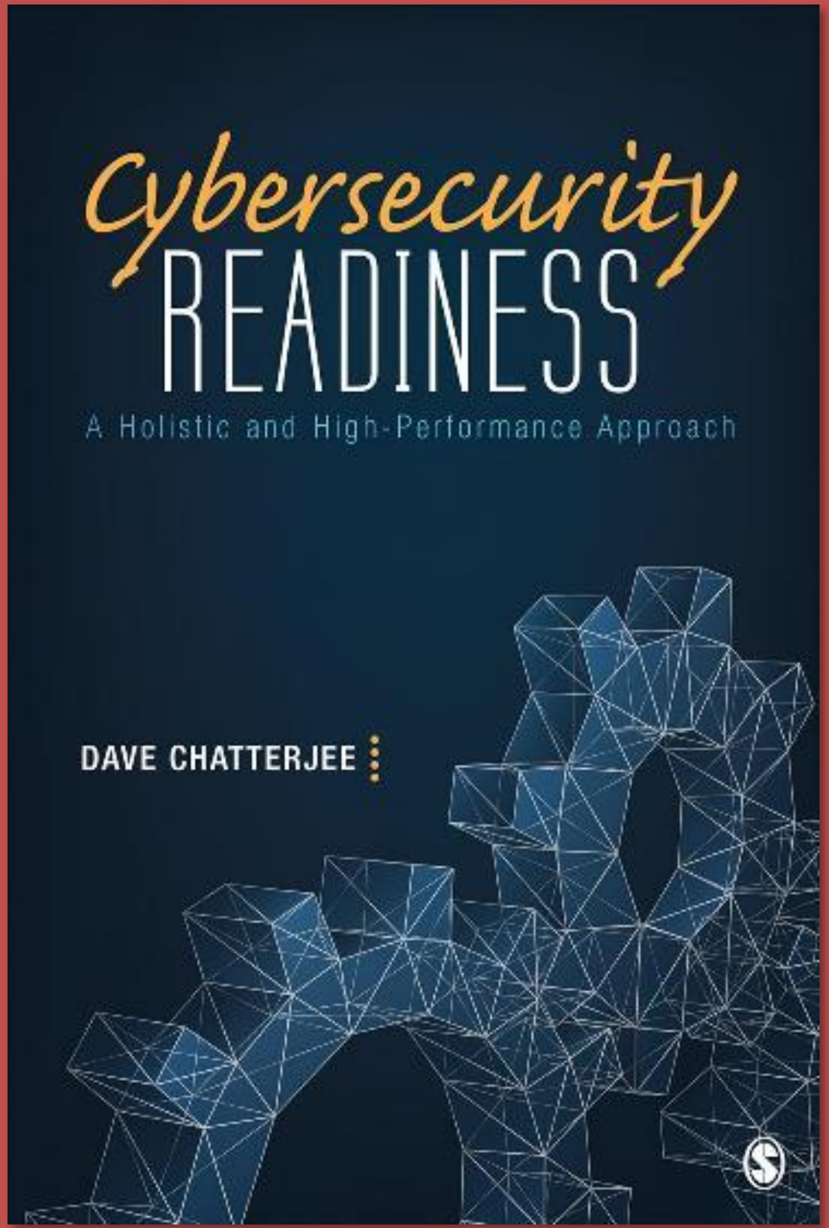
The information contained in this presentation is for general guidance only. The author/presenter assumes no responsibility or liability for any errors or omissions in the content of this presentation. The information contained in this presentation is provided on an "as is" basis with no guarantees of completeness, accuracy, usefulness, or timeliness.

Agenda

- Introduction
- Setting the Stage
- Value Creation Potential
- The CPD Framework
- Success Factors and Best Practices
- Practical Roadmap & Closing Thoughts
- Q&A

Introduction

Professional Highlights



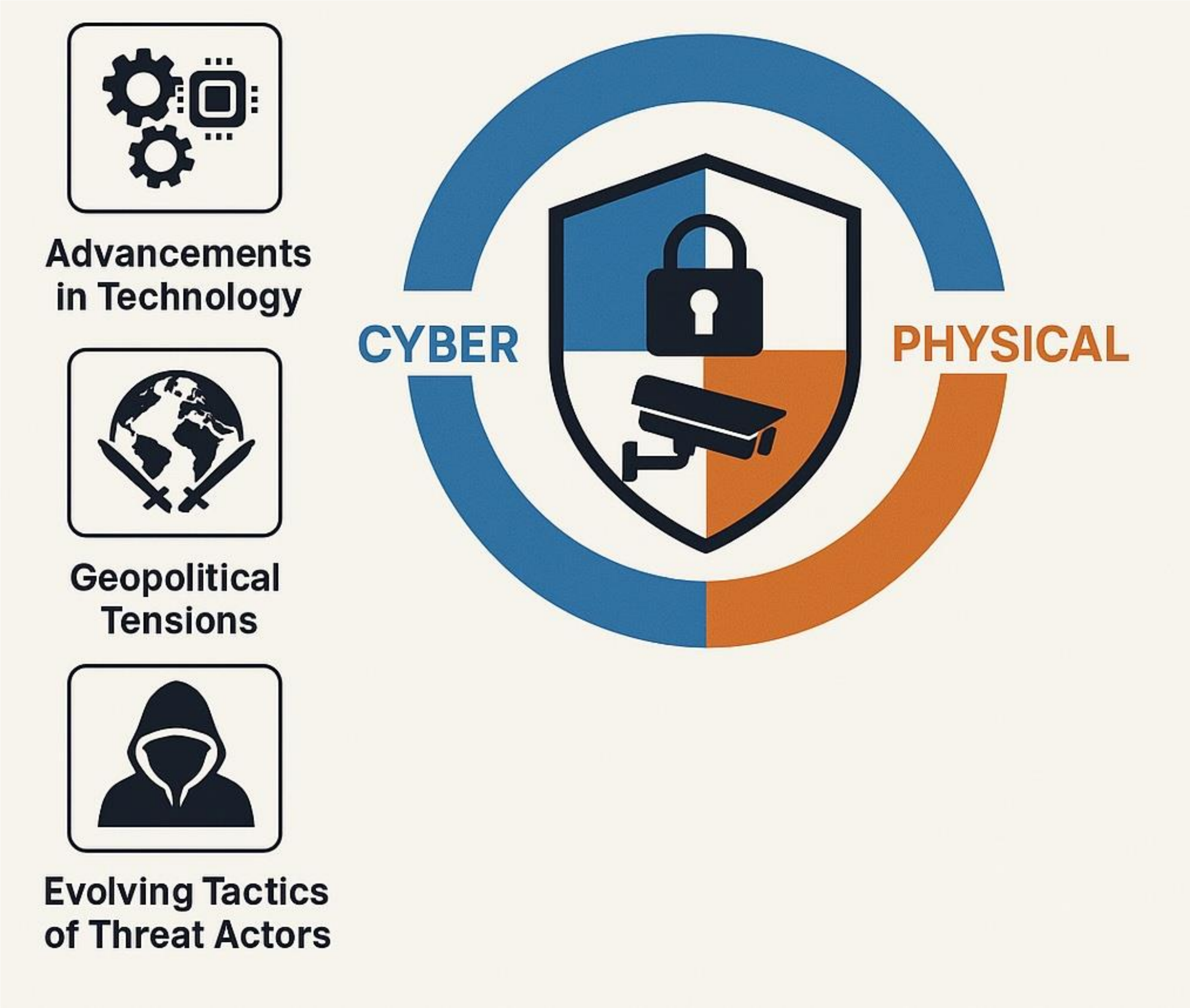
Amazon

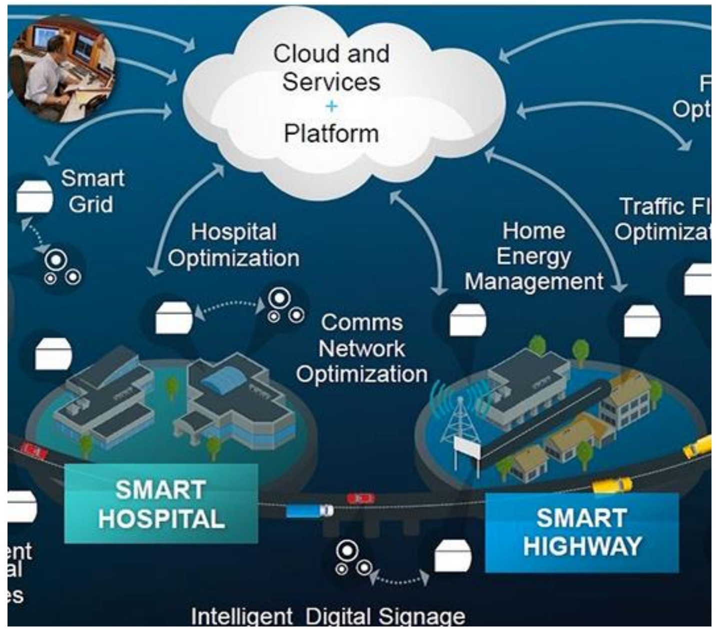
Sage

- Adjunct Associate Professor, Pratt School of Engineering, Duke University
  - Master of Engineering in Cybersecurity
  - Executive Cybersecurity Certificate Program
- Author, Cybersecurity Readiness: A Holistic and High-Performance Approach, SAGE Publishing
- Host and Producer, Cybersecurity Readiness Podcast Series
- Published in top academic and practitioner journals
  - Wall Street Journal; MIT Sloan Management Review; MIS Quarterly; Business Horizons; California Management Review
- Served on a cybersecurity SWAT team
- Featured on Forbes, Chicago Tribune, USA Today, Yahoo!Finance, Business Insider, Morning Star, GlobeNewswire, and others.
- Strategic Advisor
- Speaker and Moderator

Setting the Stage

Expanding and Converging Cyber Threat Landscape





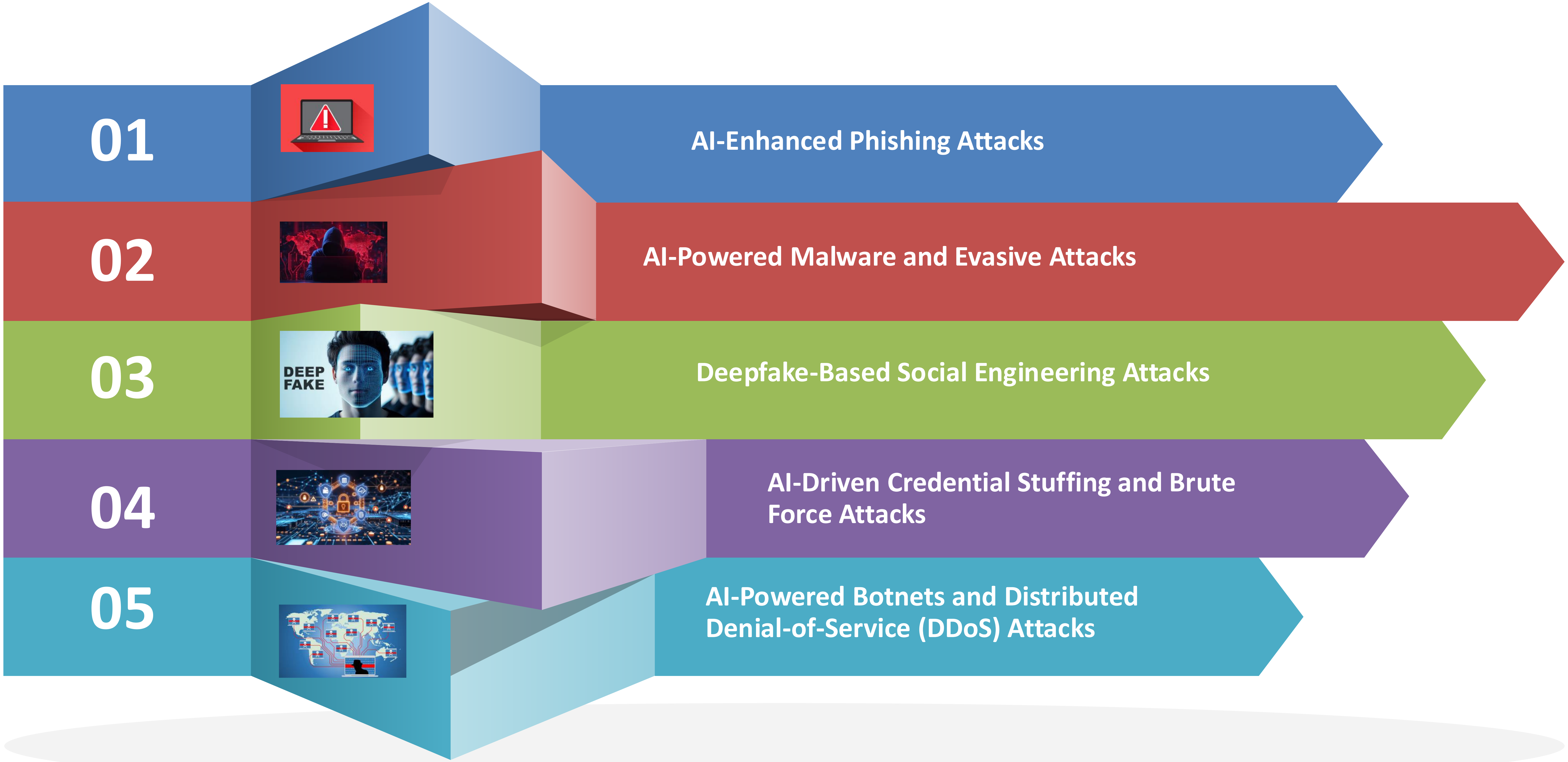
Digitization of Processes and Business Models

Highly Mobile Work Environment

Increasing use of IoT and Smart Devices

Artificial Intelligence

AI-Powered Attacks



01 AI-Enhanced Phishing Attacks

02 AI-Powered Malware and Evasive Attacks

03 Deepfake-Based Social Engineering Attacks

04 AI-Driven Credential Stuffing and Brute Force Attacks

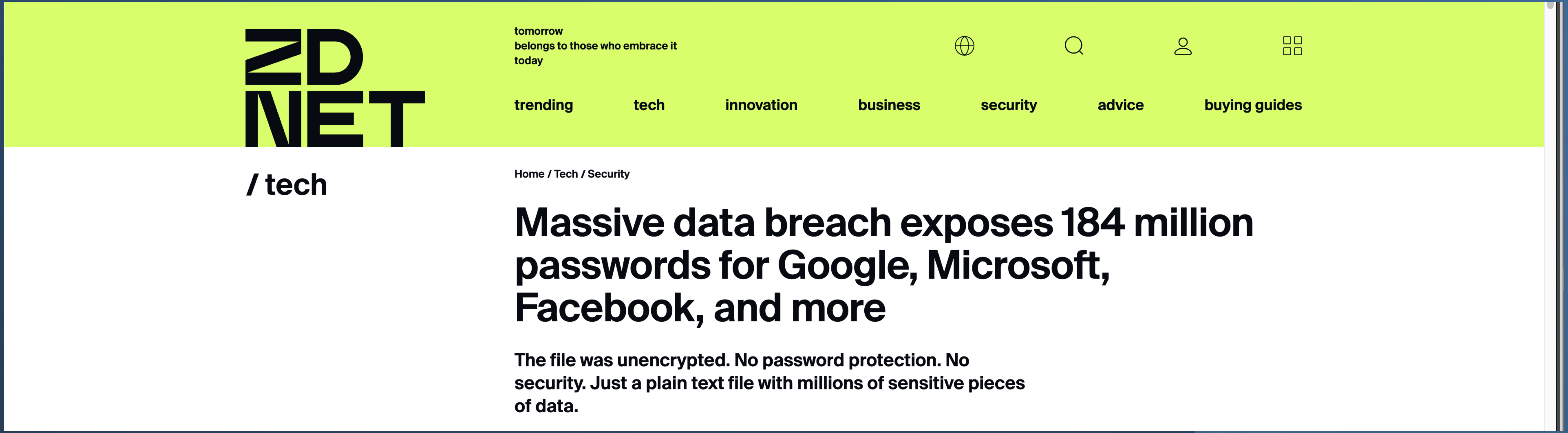
05 AI-Powered Botnets and Distributed Denial-of-Service (DDoS) Attacks

The human factor continues to be the most significant vulnerability

Organization Shortcomings and Vulnerabilities

Review of Data Breach Records from 2013-2023

- Usernames and Passwords not encrypted
- Weak encryption system
- Unencrypted customer data stored in multiple locations
- Networks not adequately segmented
- Multi-factor Authentication (MFA) not in place
- Delay in notifying victims
- The breach went undetected for several weeks
- The company did not pay heed to the alerts sent by the monitoring company
- Misconfigured web application firewall
- Lack of well rehearsed disaster recovery and incident response plan

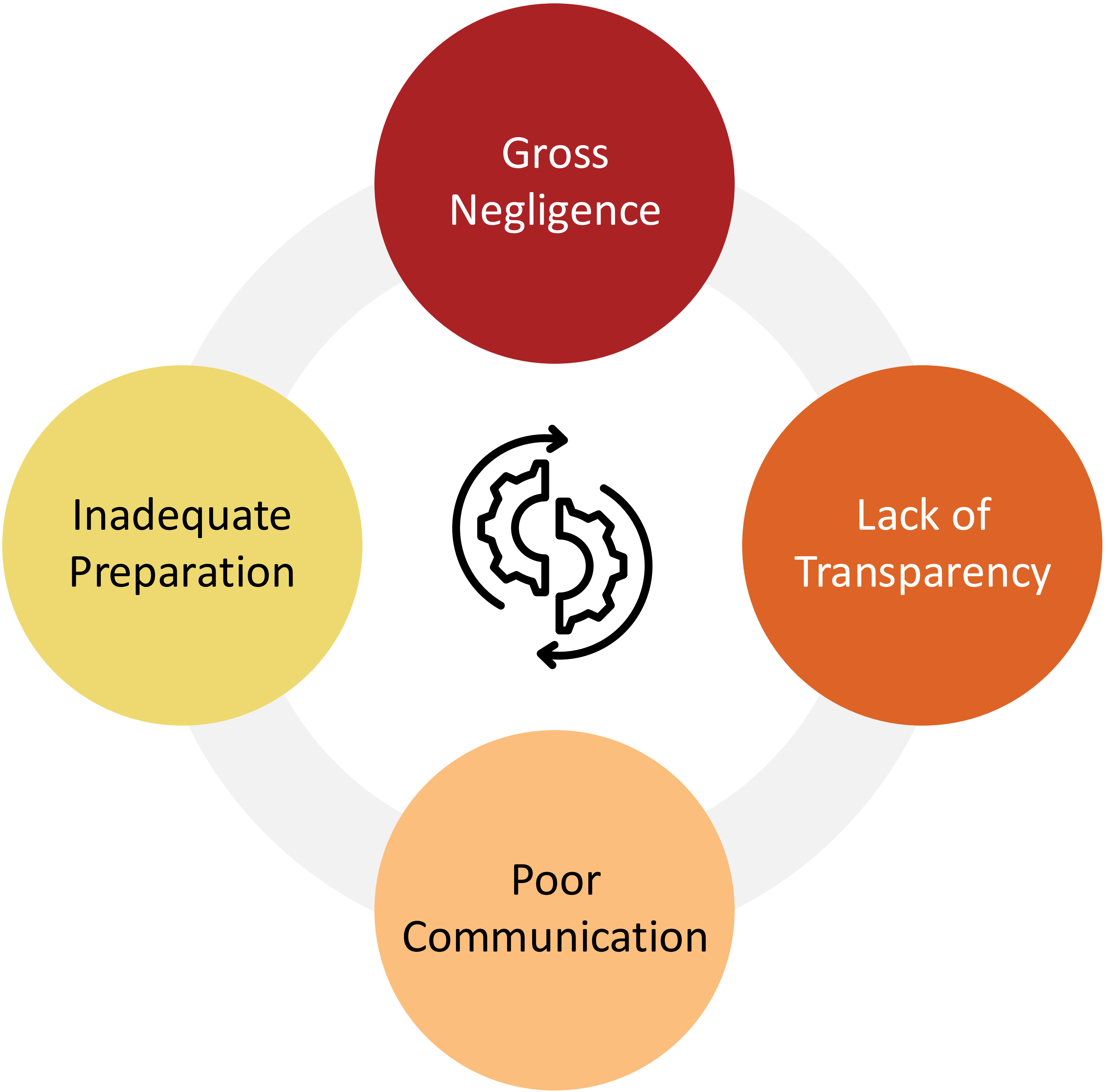


Home / Tech / Security

Massive data breach exposes 184 million passwords for Google, Microsoft, Facebook, and more

The file was unencrypted. No password protection. No security. Just a plain text file with millions of sensitive pieces of data.

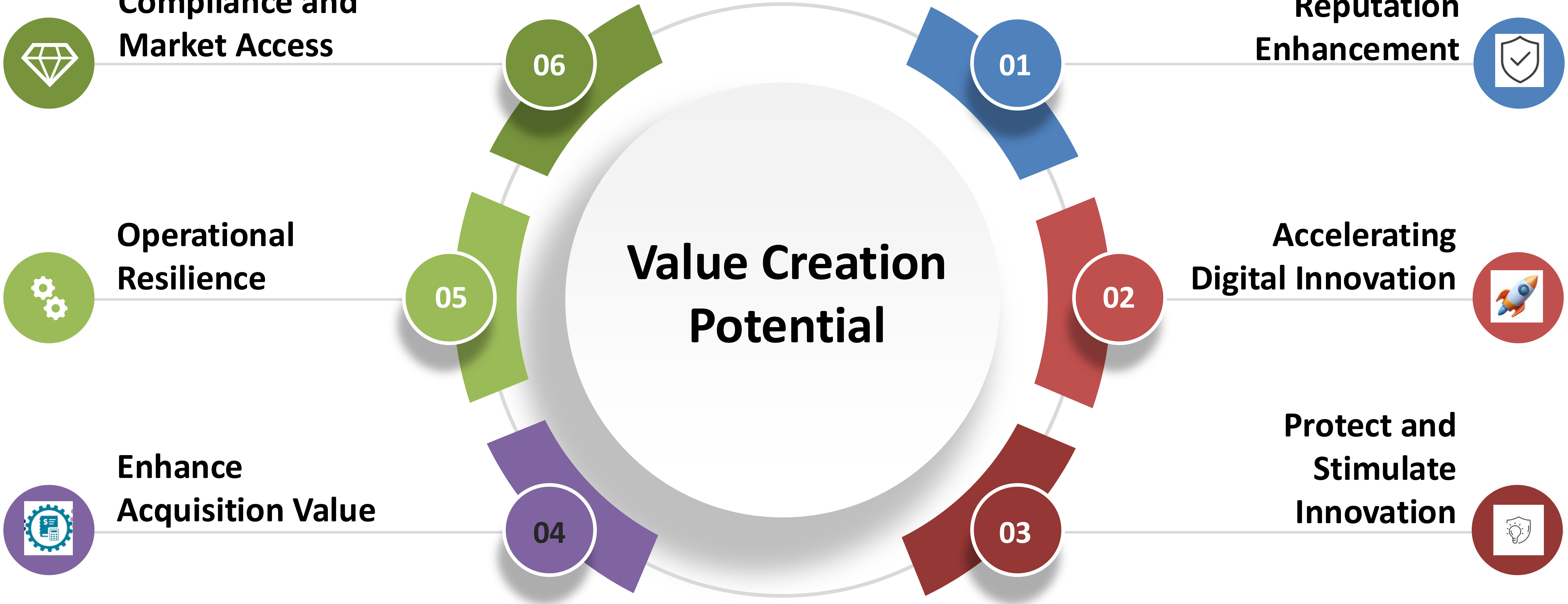
Organization Shortcomings and Vulnerabilities



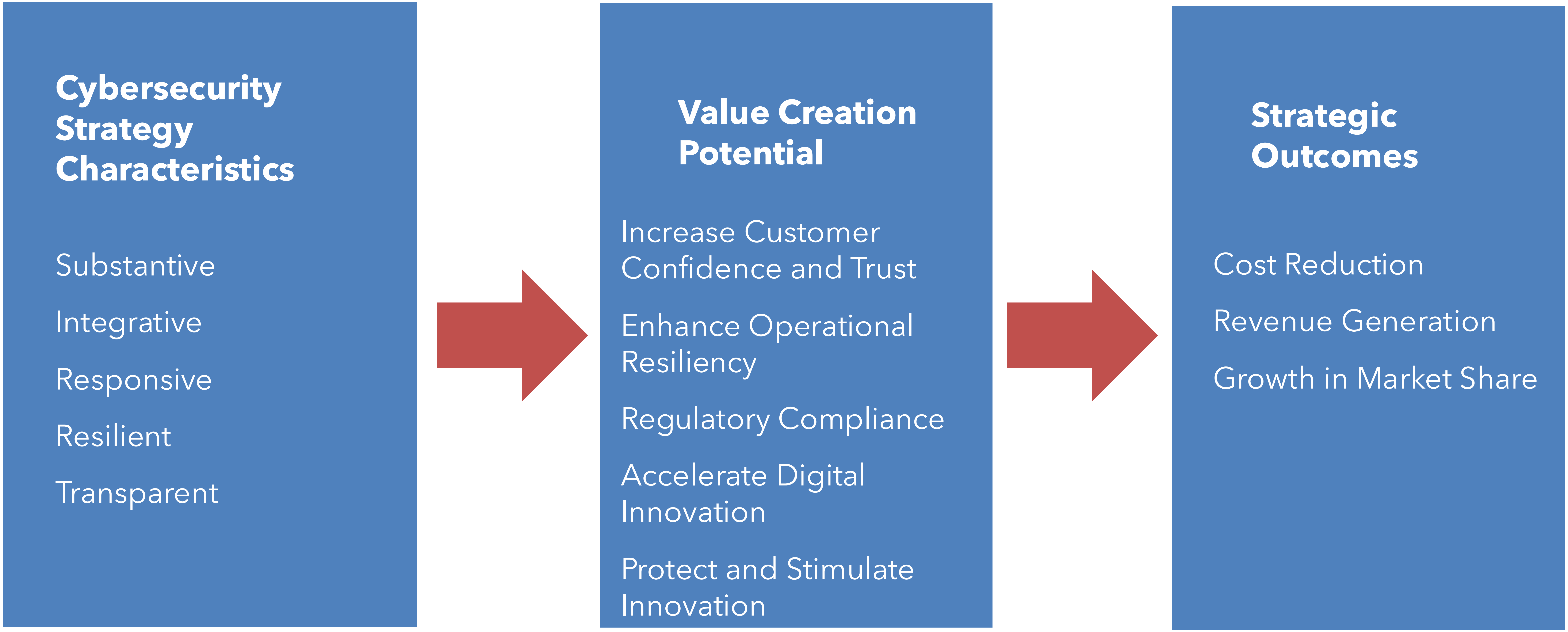
- Lack of coordination
- Lack of strategic alignment
- Operating in silos
- Business continuity, safety, and cybersecurity are not integrated

Value Creation Potential

Value Creation Potential


Value Creation Potential
01
Brand Trust and Reputation Enhancement
02
Accelerating Digital Innovation
03
Protect and Stimulate Innovation
04
Enhance Acquisition Value
05
Operational Resilience
06
Regulatory Compliance and Market Access

Strategic Cybersecurity Model



Cybersecurity Strategy Characteristics

Substantive

Integrative

Responsive

Resilient

Transparent

Value Creation Potential

Increase Customer Confidence and Trust

Enhance Operational Resiliency

Regulatory Compliance

Accelerate Digital Innovation

Protect and Stimulate Innovation

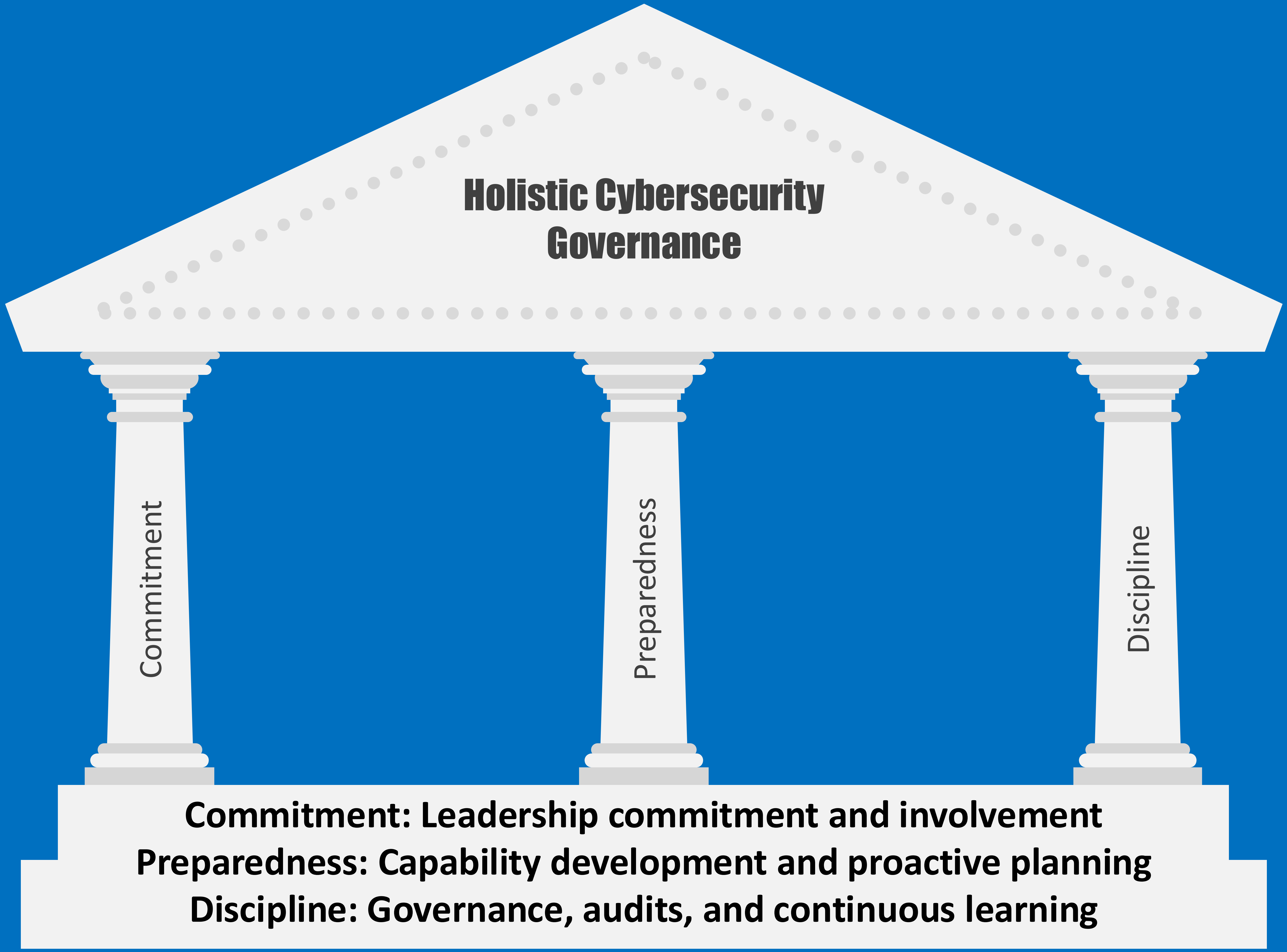
Strategic Outcomes

Cost Reduction

Revenue Generation

Growth in Market Share

The CPD Framework



Holistic Cybersecurity Governance

Commitment

Preparedness

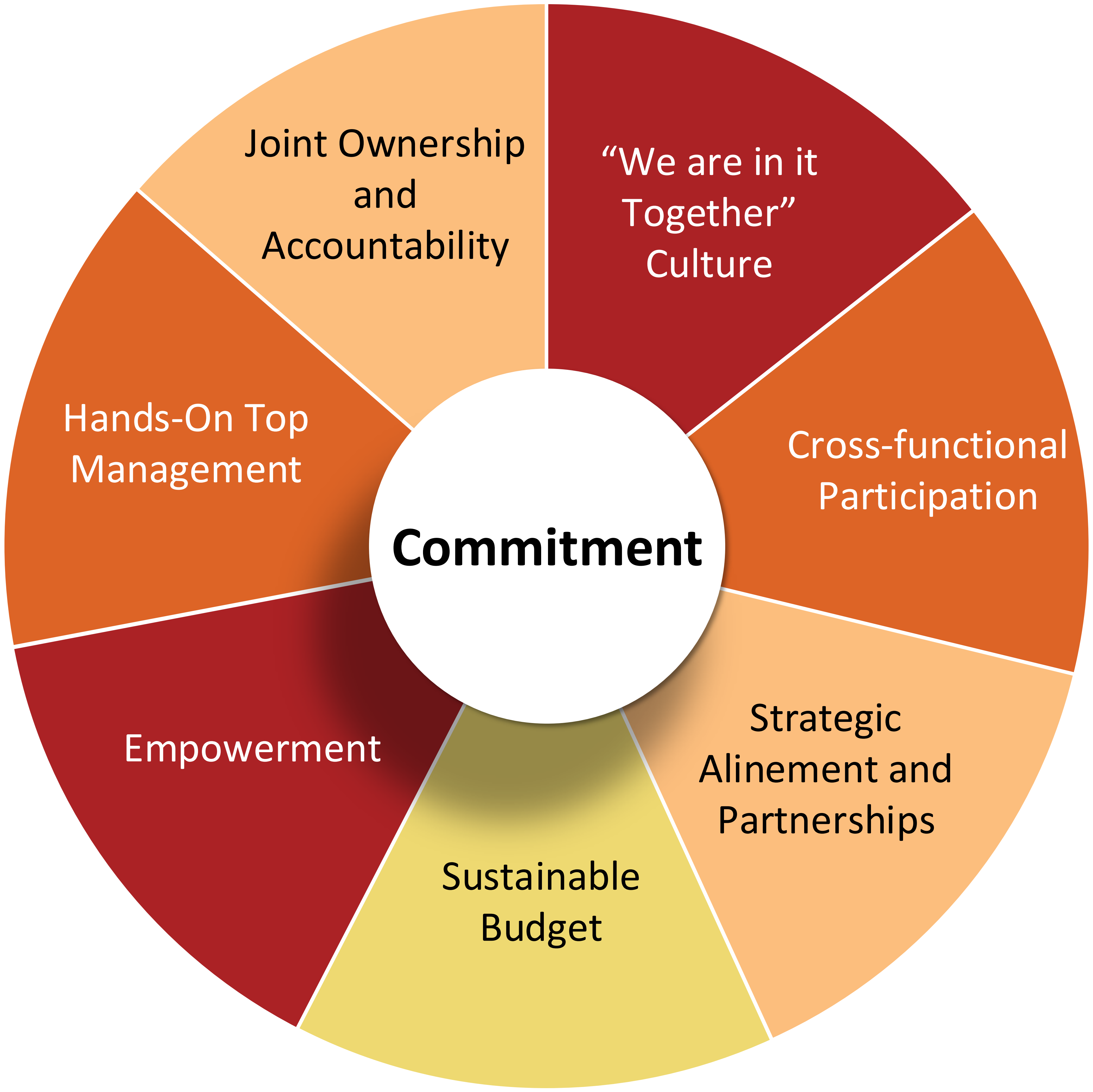
Discipline

Commitment: Leadership commitment and involvement

Preparedness: Capability development and proactive planning

Discipline: Governance, audits, and continuous learning

1 2 3



Commitment

“We are in it Together” Culture

Cross-functional Participation

Strategic Alinement and Partnerships

Sustainable Budget

Empowerment

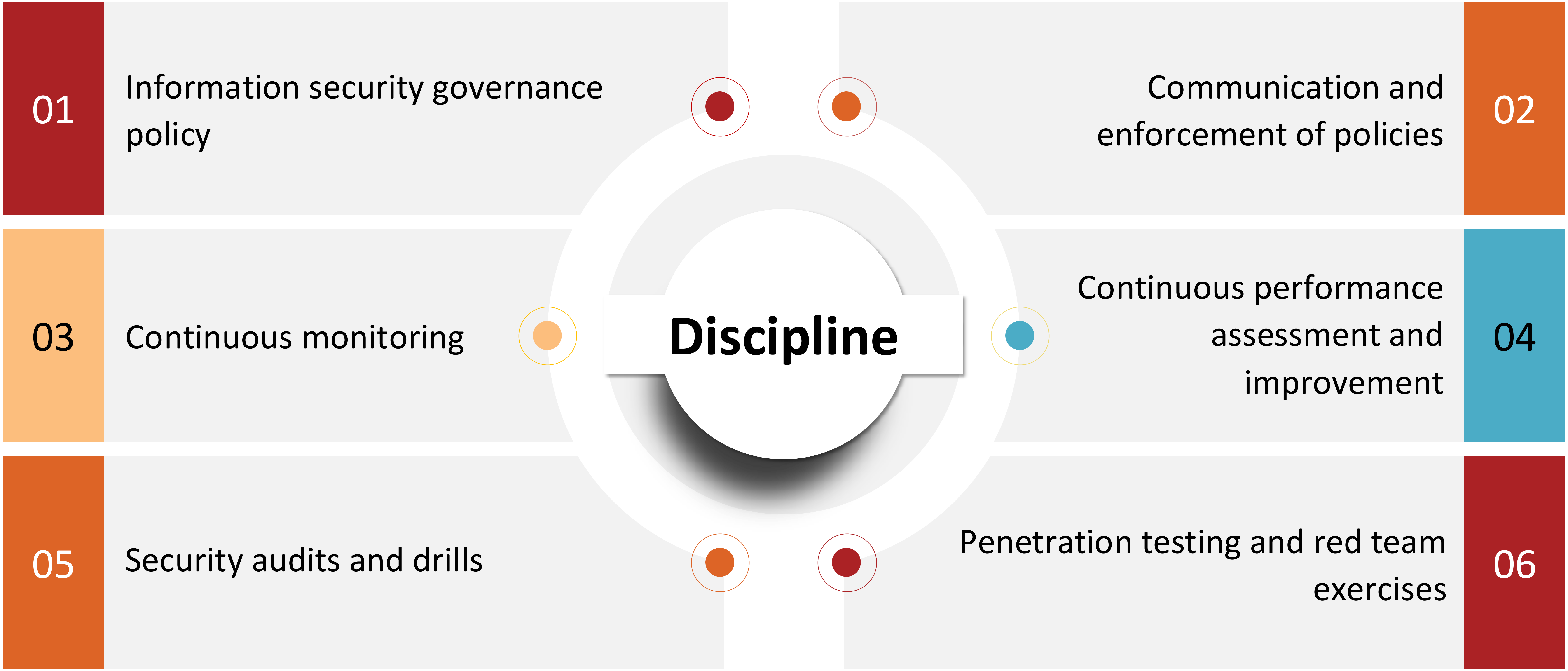
Hands-On Top Management

Joint Ownership and Accountability

1 2 3

Preparedness	Identify	Protect	Detect	Respond & Recover
	Organization role recognition Cyber risk assessment Asset identification and prioritization	Access control Configuration management Securing clients and browsers Securing networks Managing removable media Data security Data back up and retention Asset maintenance Awareness and training Business continuity planning	Detect anomalies and events	Incident response capability Disaster recovery planning

1 2 3



Discipline

01 Information security governance policy

02 Communication and enforcement of policies

03 Continuous monitoring

04 Continuous performance assessment and improvement

05 Security audits and drills

06 Penetration testing and red team exercises

Success Factors & Best Practices

Hands-on Top Management

Mindset Shift

- Treat cybersecurity challenges as a strategic opportunity
- Treat cybersecurity capabilities as core competencies

Active Engagement

- In all aspects of cyber governance – from strategizing to monitoring and measurement
- Take ownership and responsibility
- Serve on governance teams
- Participate in training and awareness programs

First of all Dr. Chatterjee, let me thank you for giving
What is the Role of Top Level Management in Security Governance? w/ Rohit Verma CEO of Crawford and Company
THE CYBERSECURITY READINESS PODCAST
WITH DR. DAVE CHATTERJEE

Rohit Verma
Chairman and CEO, Crawford and Company

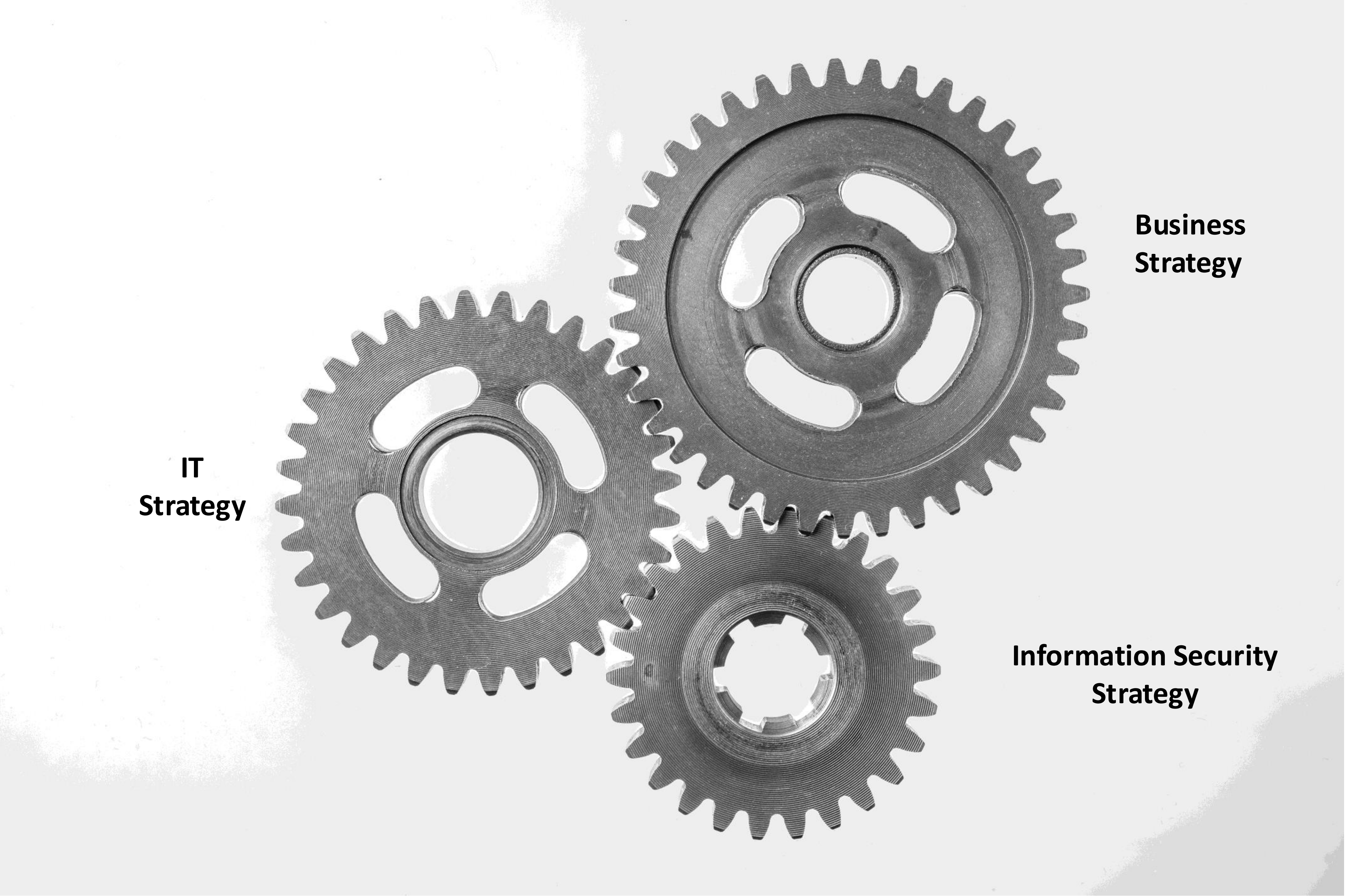
> Several of us in senior leadership are digital immigrants and not digital natives. Many of the security issues are new to us. We will be naïve if we don’t take interest and are not willing to learn and stay updated.

Gaining Top Management Attention & Commitment

Destroy Your Business (DYB) Scenario

- Come up with various security breach-related scenarios
- For each scenario, discuss
  - How the attack or breach is likely to happen?
  - What are the implications and consequences of the breach?
  - How can the potential attack/breach be prevented?

Strategic Alignment



"Implications of data security and protection must feature in every strategic and operational decision making"

CISO Empowerment

- CISO must be appropriately empowered to be effective
- Ideally, the CISO should be part of the C-level team or at least have direct access to the top management

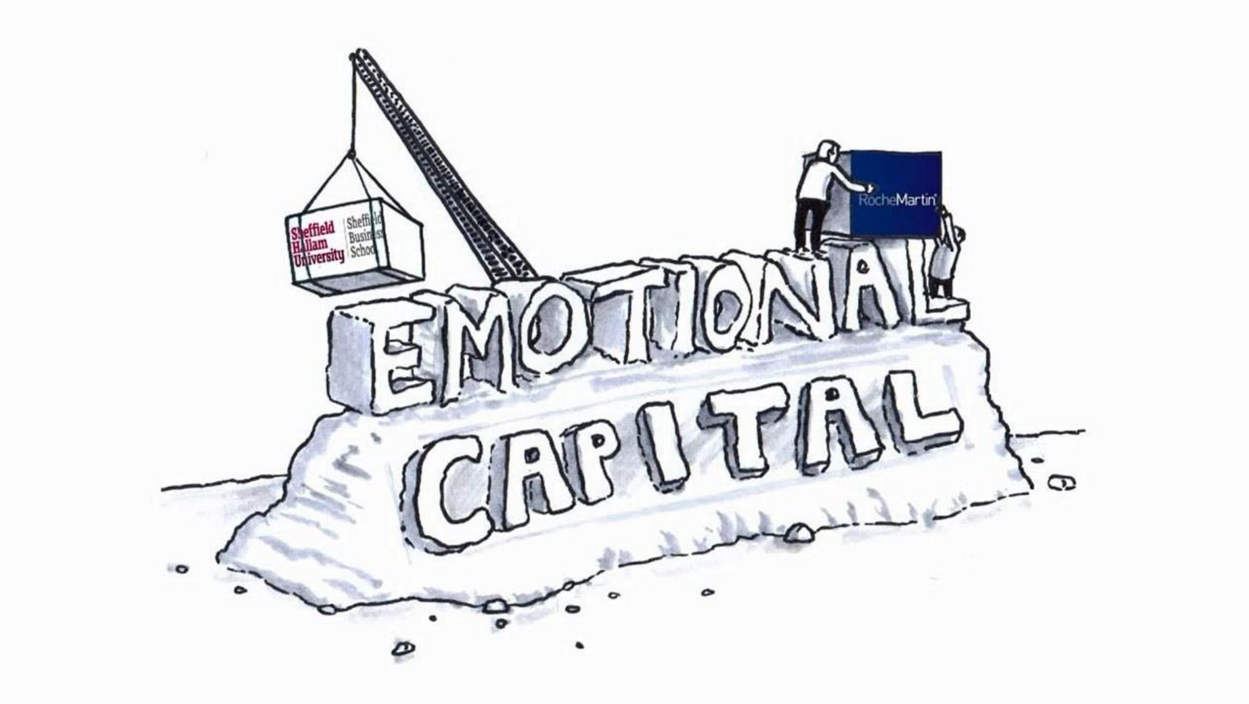
It is always preferred that
Perspectives of a Global CISO w/ Vishal Salvi, CISO & Head of Cyber Practice at Infosys
THE CYBERSECURITY READINESS PODCAST
WITH DR. DAVE CHATTERJEE

Vishal Salvi
Former Global CISO & Head of Cyber Practice
Infosys

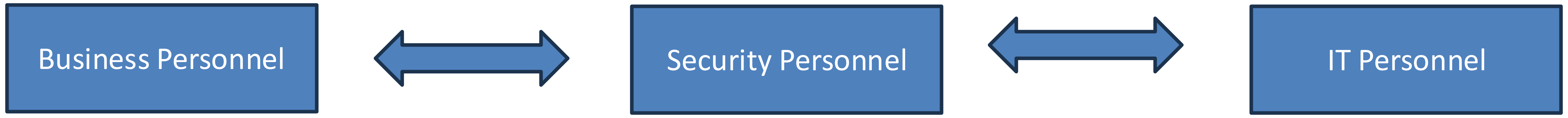
> There is growing recognition that the CISO is much more than a risk or technology officer. They are business enablers and must be involved in strategic and value creation activities

Creating a Culture of Empathy and Enablement

- Building Emotional Capital
  - Feeling valued
  - Developing a sense of belonging
  - Taking pride in their work
  - Having fun
  - Perceiving leadership to be genuine and authentic



Role Reversal



Business Personnel

Security Personnel

IT Personnel

Joint Ownership and Accountability

Business partners, third party service providers, and vendors must share responsibility in protecting sensitive data

Preparedness Fundamentals

Comprehensive Asset Discovery

Automated and Continuous

Asset Prioritization

Criticality; Strategic Value

Enhance Data Protection

Adopting the most rigorous encryption methods

Robust Identity and Access Management

Phishing-resistant MFA solutions; least privileged access; regular account reviews

Reliable Data Backup and Retention

Frequent Testing

Regulatory Compliance

Going beyond checking the box.

Preparedness Fundamentals

Proactive Threat Hunting

Proactively anticipate and thwart attacks

Defend the Cloud Infrastructure

Invest in cloud-native application protection platforms

Prioritize Vulnerability Management

Prioritize regular patching and upgrading of critical infrastructure

Robust Vendor Management Program

Thorough vetting and regular reviews

Educate Users

Customized; Incremental; Continuous

Conduct Regular Security Assessments

Audit SaaS providers to ensure compliance with security frameworks

Developing and Leveraging AI Capabilities

- Leverage AI tools for proactive defense
  - Threat Detection and Prediction
  - Automated Incident Response
  - Threat Intelligence and Analysis
  - Identity and Access Management
  - Phishing and Social Engineering Defense
  - Vulnerability Management
- Robust Data Handling and Validation
- Continuous Testing
- Limited Application Permissions
- Rigorous vetting of vendors
- AI Policy Committee

Highly Rehearsed Response and Recovery Capability

- Cross-functional Involvement
- Inter-Organizational Participation

Customized Awareness and Training

01 Role-based

02 Incremental and continuous

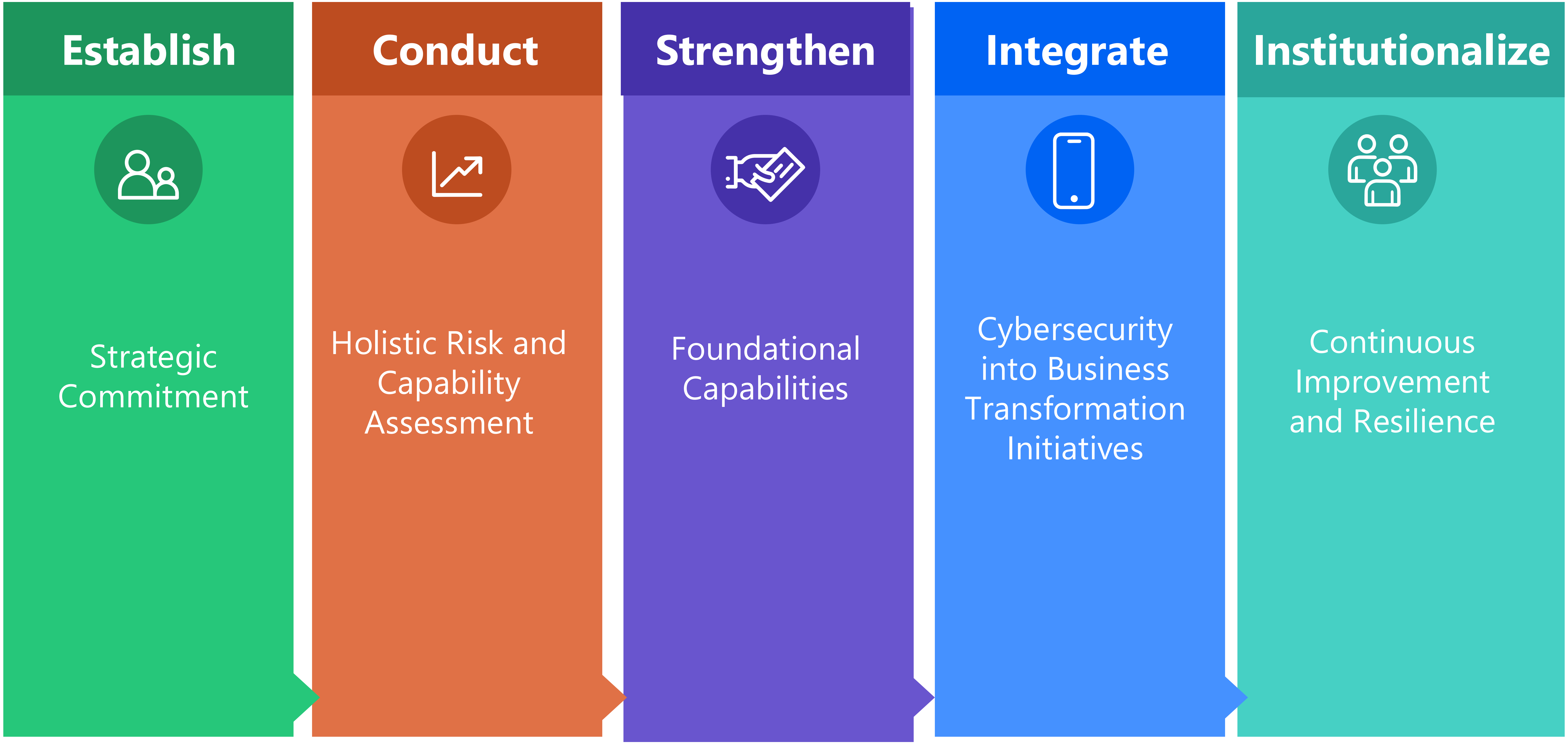
03 Engaging and interactive

04 Important component of performance review

Like Wordle and Nerdle, the daily word and mathematics games and challenges, organizations can adopt an incremental and continuous approach to spreading security awareness and knowledge.

Practical Roadmap & Closing Thoughts

Roadmap for Advancing Cybersecurity Maturity



Establish

Strategic Commitment

Conduct

Holistic Risk and Capability Assessment

Strengthen

Foundational Capabilities

Integrate

Cybersecurity into Business Transformation Initiatives

Institutionalize

Continuous Improvement and Resilience

Ideal Mindset and Approach

Mindset

Consider the cyber attack epidemic to be a strategic opportunity

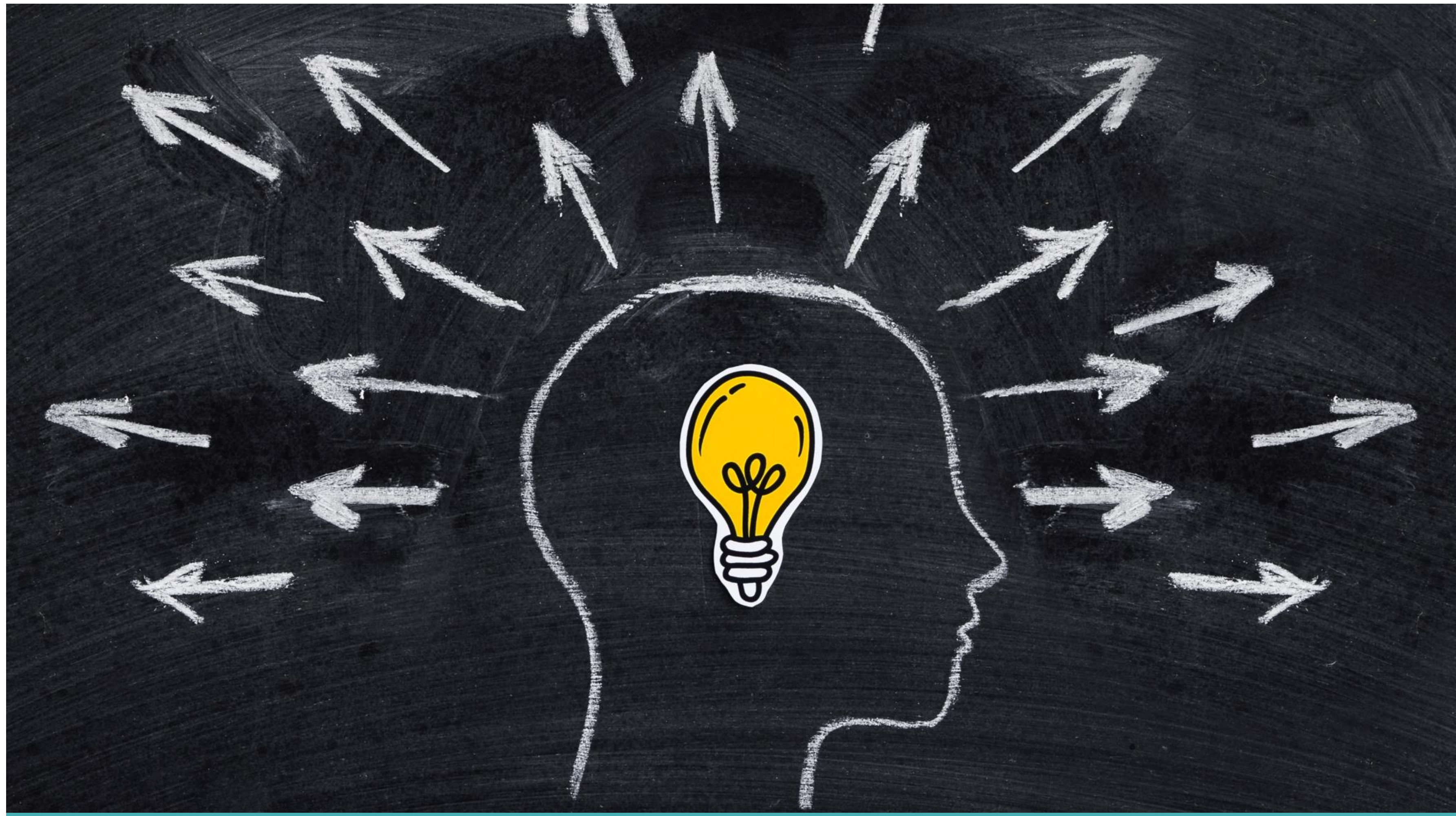
Treat cybersecurity as a strategic competency/capability

Everyone has a role to play in securing the organization

Ideal Mindset and Approach

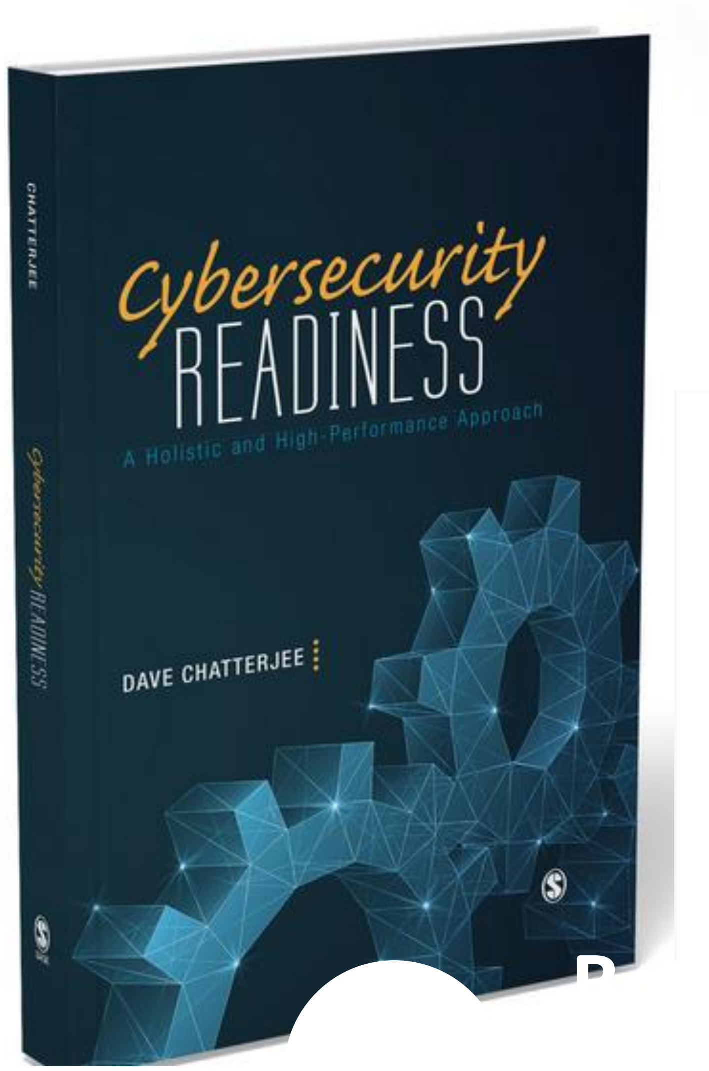
Approach

- Be proactive
- Be prepared
- Continuously monitor and make adjustments
- Promptly act on the intelligence received
- Continuous training
- Don’t outsource cybersecurity governance; actively engage and manage



- Be truly committed to protecting confidential and strategic assets
- Go above and beyond the Check-the-Box approach

Q&A



Amazon

https://www.dchatte.com/podcast/

https:www.cybersecurityreadinesspodcast.com

THANK YOU!!

Book

Cybersecurity Readiness: A Holistic and High-Performance Approach

Podcast

The Cybersecurity Readiness Podcast

https://www.dchatte.com/podcast

https:www.cybersecurityreadinesspodcast.com

Website

https://www.dchatte.com/

Email

dchatte@gmail.com