Cyber Resilience for Democracy

Michael Coden

- Managing Partner, **Magjic Consulting** (magjic.com)
- Senior Advisor, **Boston Consulting Group (BCG)**
- Co-founder and Associate Director of MIT cybersecurity research consortium (**cams.mit.edu**)
- Member, **DBOS-Project**, novel cyber resilient operating system from MIT & Stanford (dbos-project.github.io)
- Advisory Boards: **Safe Inc.**, **The Decision Lab**
- Assisted **White House** in development of NIST Cybersecurity Framework
- Former Global Lead of Cybersecurity Consulting at **BCG**
- BSEE, MIT; MS in Mathematics, Courant Institute of Mathematical Sciences at NYU; Masters in Business Administration, Columbia University

Cyber security is a titanic problem

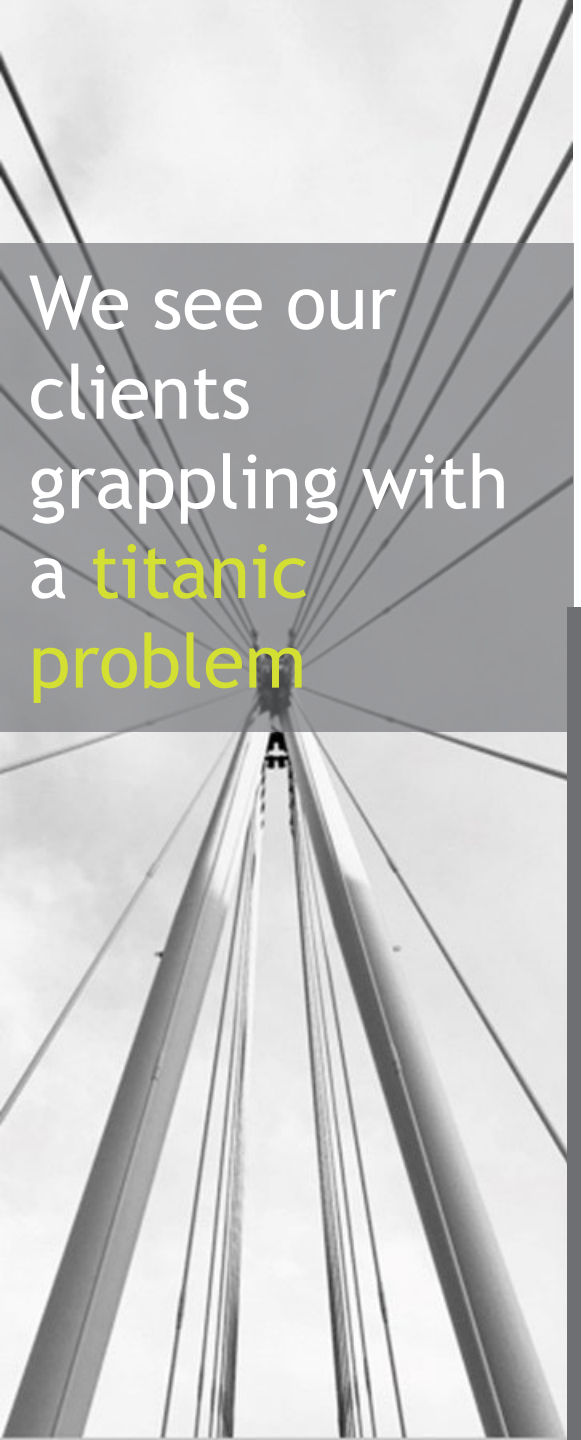
The focus is too often solely on technology and protection, while the hidden truth is that cyber is a business risk against a technology backdrop

Typical focus of attention
(and important)

Inadequate security technology causes 23% of breaches …

… organizational, process, and people failures cause 77%

Often neglected



We see our clients grappling with a titanic problem

We need to shift additional focus onto Resilience – how we can more rapidly detect attacks, and continue operations

Typical focus of attention
(and important)

… Resilience

Technology

Inadequate security technology causes 23% of breaches …

People

Process

Organization

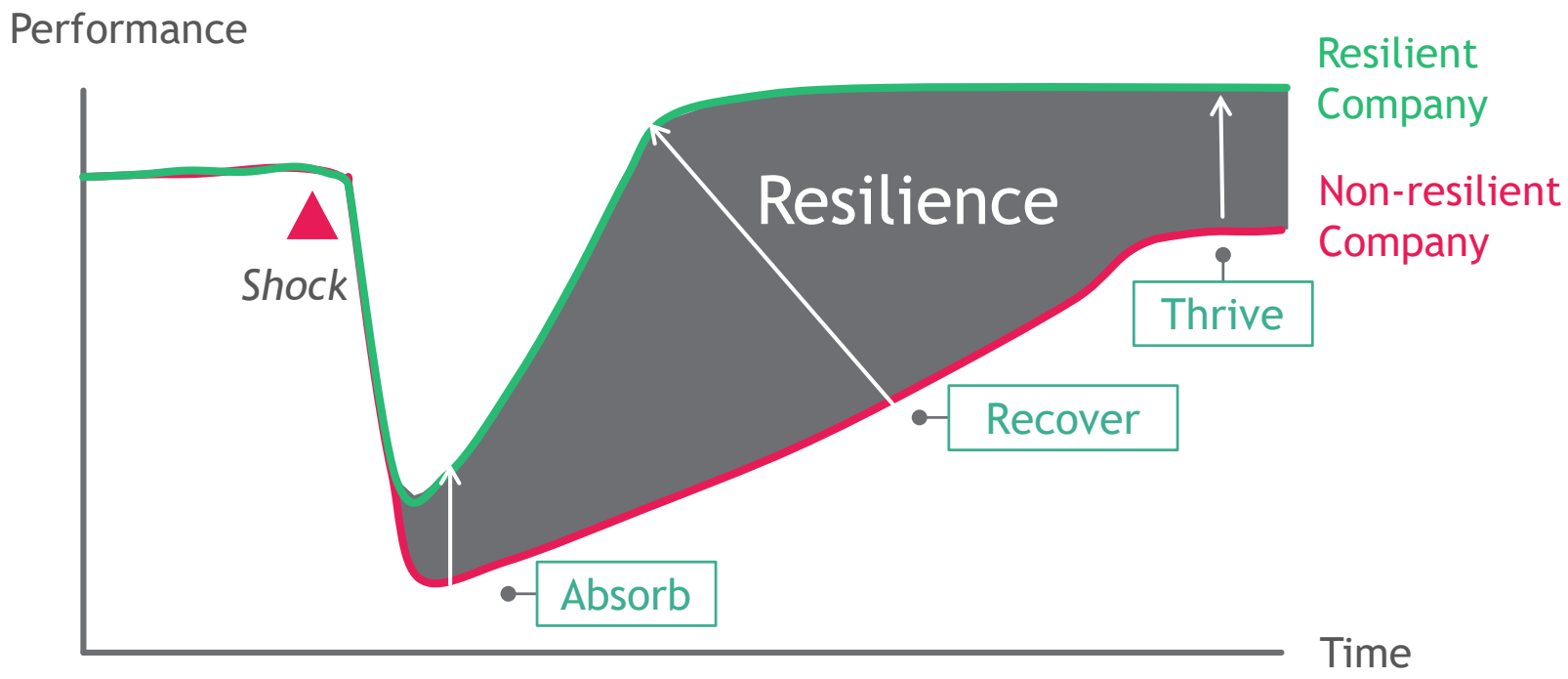
… organizational, process, and people failures cause 77%

Often neglected

"Cyber Resilience" plans can both reduce the magnitude and duration of the cyber supply chain impact

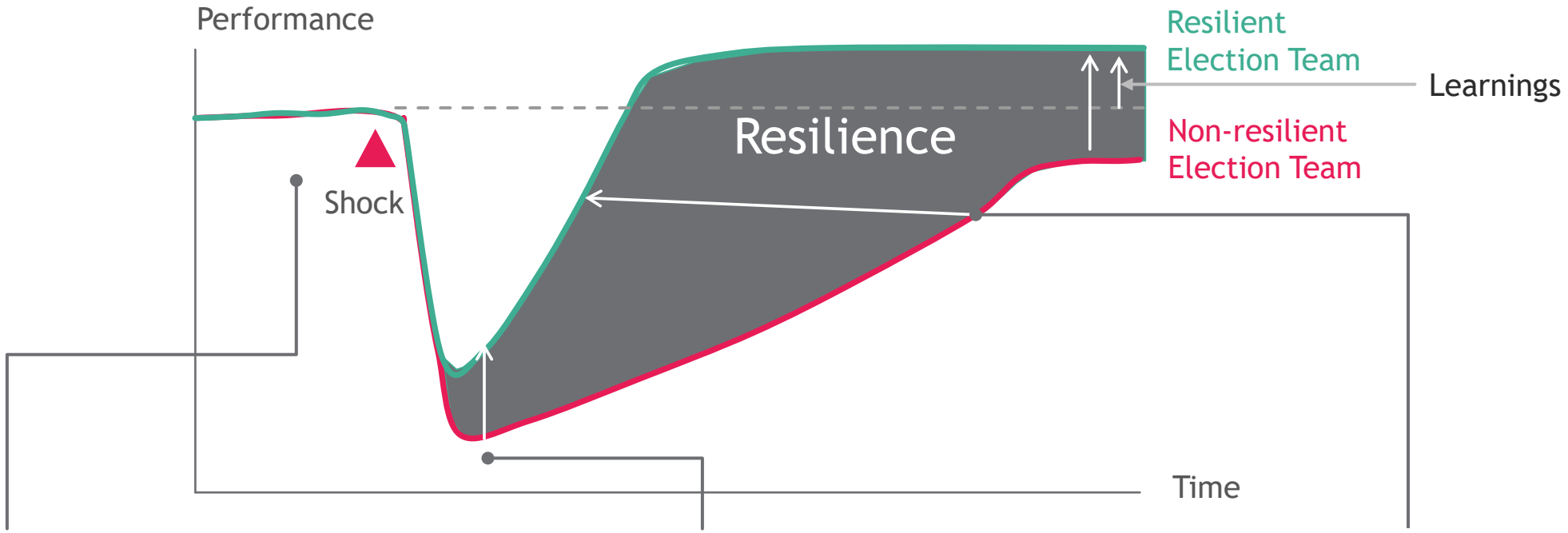
Typical response protocols

- Detection & Incident Response
- Business Continuity
- Disaster Recovery



Source: BCG Henderson Institute Analysis

Cyber resilience creates advantage through effective planning and response



Anticipation advantage

Imagine the worst possible scenarios. Prepares for an attack with all employees trained, practiced, and all external needs at the ready

Cushioning advantage

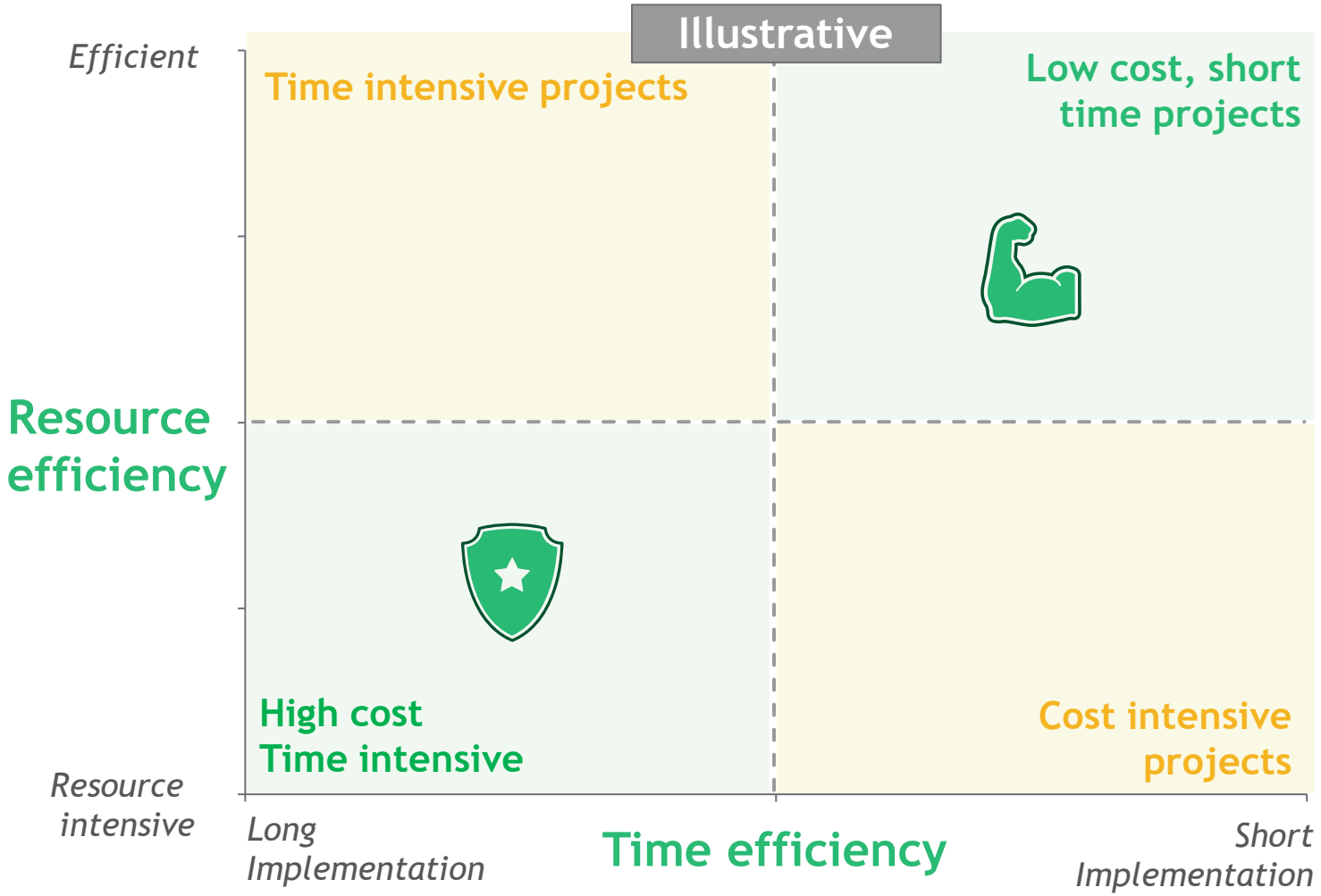
Good planning, preparation, and practice can reduce the impact of the event through redundancy, modularity and diversity

Adaptation & shaping advantage

Embeds and adapts to make the company less prone and more resilient to future attacks – think outside the box

Source: BCG

Resilience costs less and provides benefits faster



Protection

Most protection levers are **expensive and time consuming, functioning as pre-emptive measures**

Resilience

Most of the resilience levers are quick win projects that are **cheap and easy to implement** (e.g., pre-written comms, regular periodic updates)

Some key concepts to consider in developing your election day resilience

Checklist

Ensure you can detect, respond, **continue** & recover quickly

Detection and Incident Response	Business Continuity	Disaster Recovery

01 Imagine the worst things that could happen. Then imagine even worse things – think outside the box

02 How well are Cyber and Physical plans integrated?

03 What are the emergency communication systems in place for each plan? (Technologies and call lists – think paper!)

04 How are all election staff trained to quickly execute their roles in each plan?

05 Who are the external contacts in the community that must be contacted: legal counsel, law enforcement, regulators, government agencies, technology partners, supply chain

06 What are the most critical systems for election continuity and how are they prioritized for restoration?