



Securing the Future of Microfinance

Driving Digital Innovation through
Robust Information Security

Alden Arban, AVP for Information Security,
CARD MRI Information Technology, Inc. (CMIT)

The Dual Mandate of CMIT

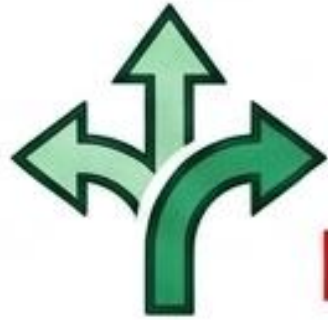


Driving and sustaining digital transformation. Managing vital IT infrastructure to deliver seamless, accessible financial services across the CARD MRI network nationwide.



Ensuring innovation is matched by robust information security. Safeguarding operations, protecting sensitive client data, and maintaining decades of institutional trust.

Rethinking Digital Transformation



NETFLIX

Agility Over Obsolescence (The Netflix Lesson)

Traditional View

Use IT to simply digitize paper forms and make existing processes slightly faster.

CMIT View

Fundamentally transform delivery models. Change the business culture to reach unbanked communities with unprecedented agility.



Embracing Productive Risk (The Musk/Tesla Lesson)

Traditional View

Avoid risk at all costs; rely entirely on safe, off-the-shelf vendor products.

CMIT View

Build an appetite for calculated risk. Learn from failures to build resilient, in-house solutions tailored for the Filipino people.



Decentralized Empowerment (The Ford Lesson)

Traditional View

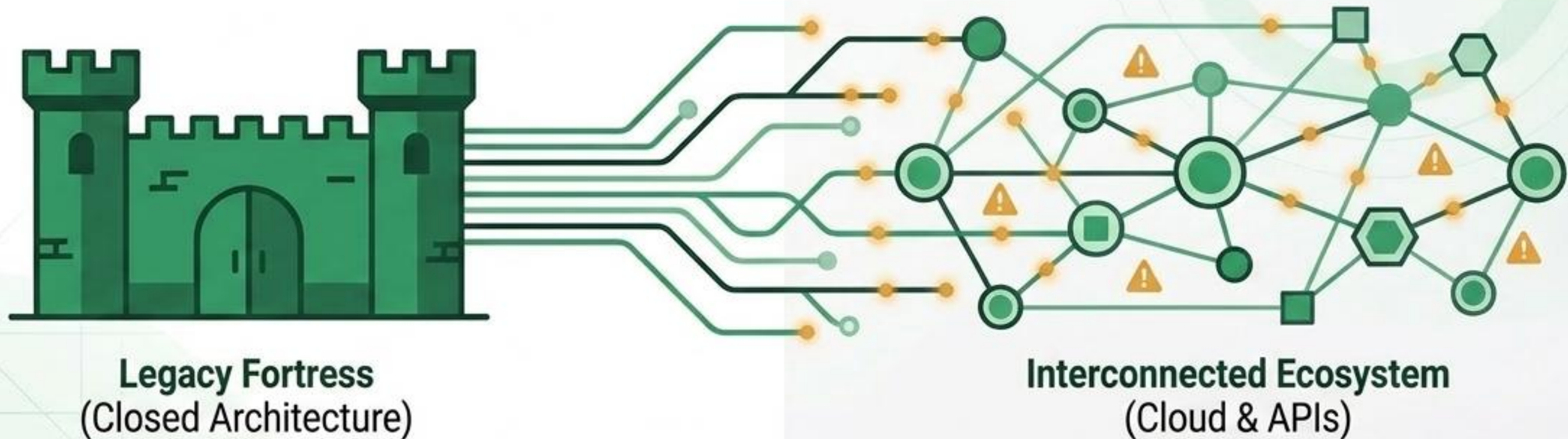
Centralize all approvals, creating a single executive bottleneck that stifles culture.

CMIT View

Deploy technology to empower branches and staff. Push decision-making outward to drive localized innovation.

The Innovation Paradox

Opening our architecture to drive service delivery exponentially increases our vulnerabilities.



New Mobile Apps + Integrated APIs + Cloud Migration = New doors and windows for highly motivated threat actors. The technologies that empower our mission simultaneously expand our borders.

Defending the Expanded Border

Sophisticated Social Engineering



Targeting the human element.
Highly targeted phishing and smishing campaigns aimed at staff and microfinance clients navigating digital banking for the first time.

Third-Party & Supply Chain Risks



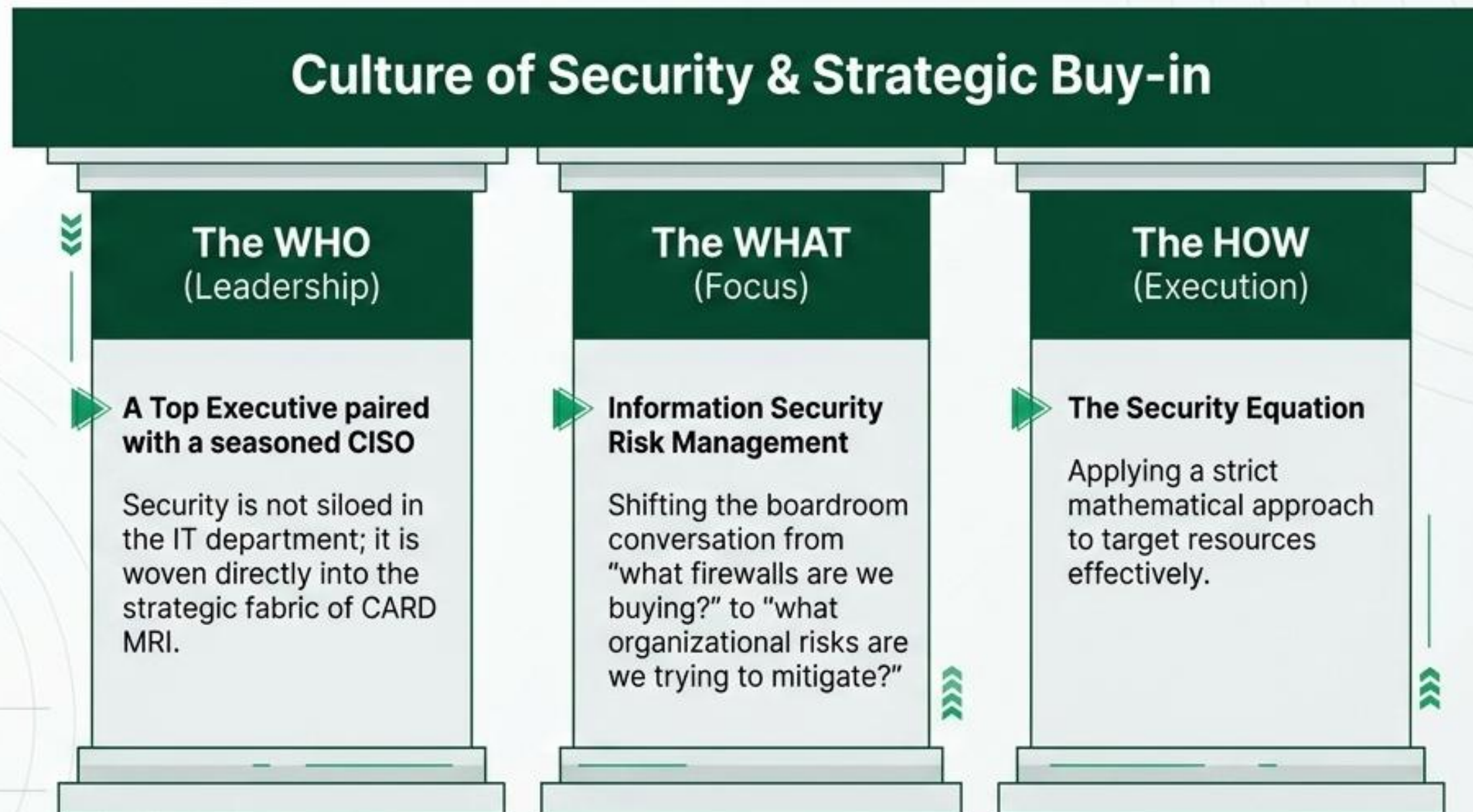
We do not innovate in a vacuum.
Reliance on vendor ecosystems means a single vulnerability in a partner's system can become a backdoor into ours.

Ransomware & Data Extortion



The threat has evolved beyond system downtime.
Extortion directly threatens the exposure of sensitive client data, risking permanent damage to institutional trust.

Structured Governance at CMIT



Focusing on the Controllable Variable



$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Impact}$$

Threat (Uncontrollable):

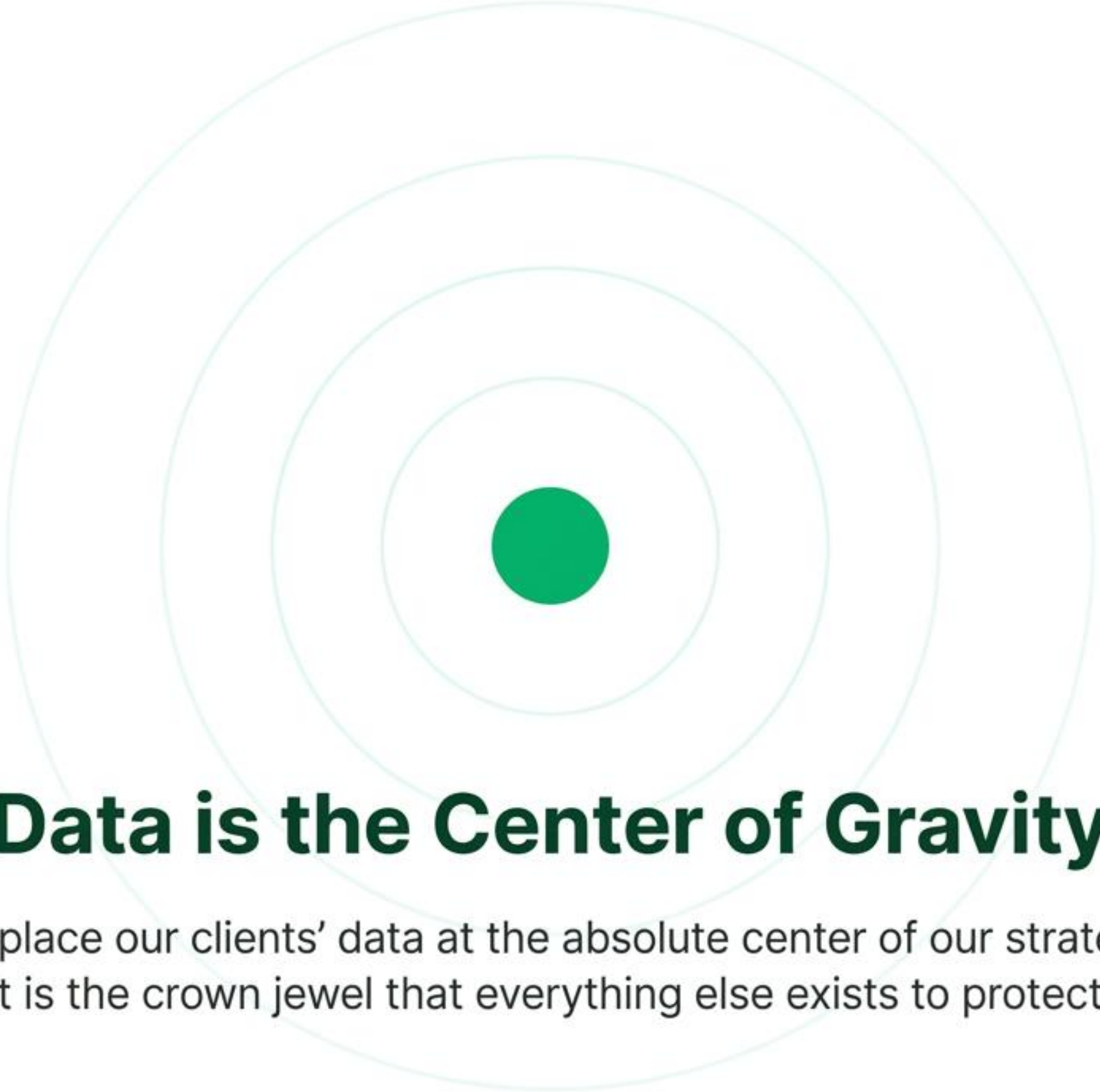
Highly motivated bad actors will always target financial institutions. We cannot change this.

Vulnerability (Controllable):

The only adjustable variable.
By aggressively identifying, patching, and mitigating system and human gaps, we drive down overall organizational risk.

Impact (Uncontrollable):

Client data is critical. The business impact of a breach will always be devastating. We cannot lessen this.

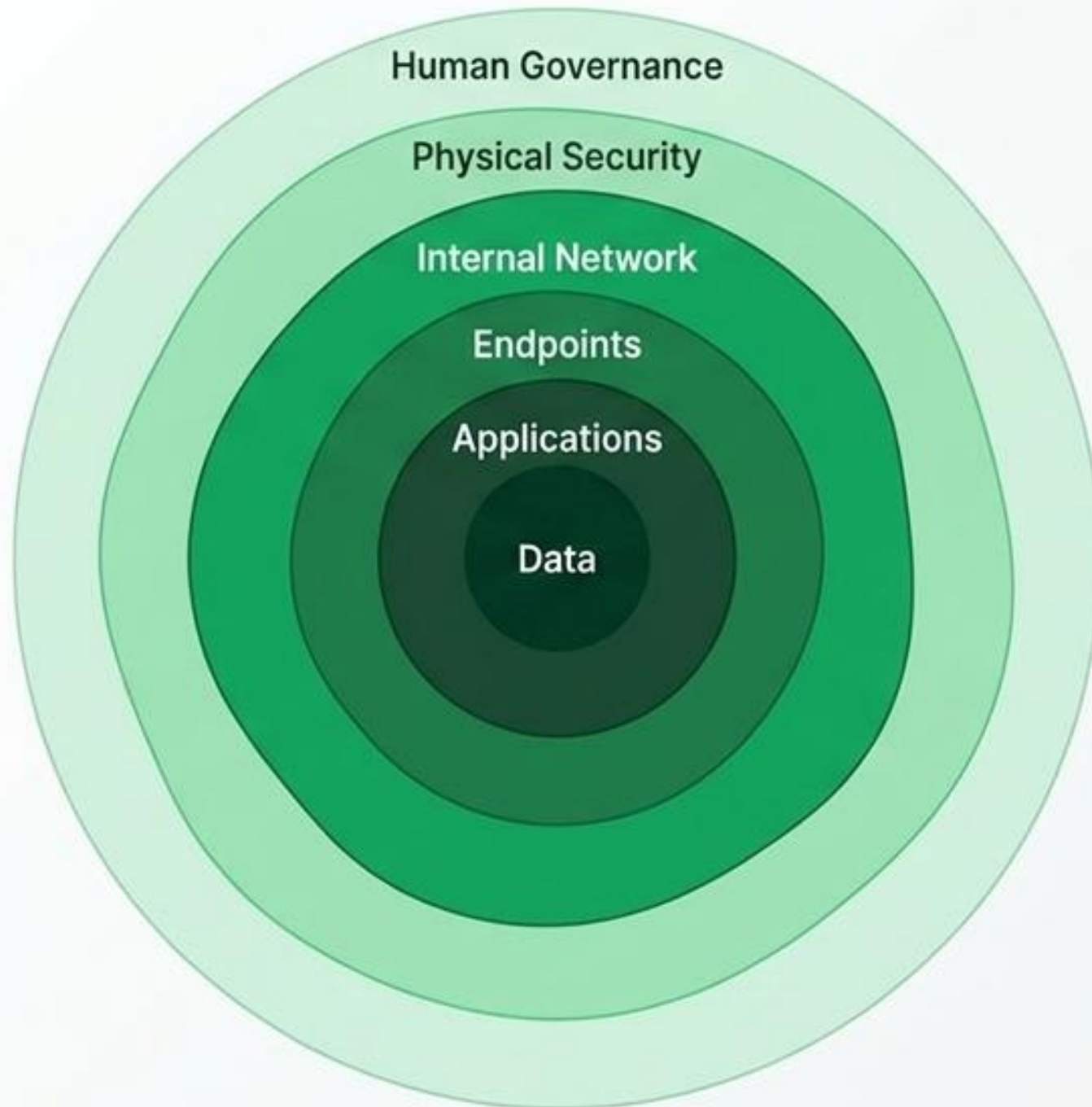


Data is the Center of Gravity

We place our clients' data at the absolute center of our strategy.
It is the crown jewel that everything else exists to protect.

Targeted Control Allocation

Utilizing Northrop Grumman's Cyber Security Reference FAN™ Framework



With finite resources, microfinance institutions cannot afford a “shotgun approach.” The FAN framework allows us to map the layers surrounding our data and deploy budget and manpower methodically to address specific vulnerabilities.

“The moment you build a higher wall, threat actors invent a taller ladder.”

A static, unbreachable fortress does not exist. We must shift our institutional goal away from the myth of 100% security and toward relentless, continuous improvement.



The Engine of Resilience

Act

Adjust strategies based on lessons learned—even when we are 'productively wrong.' Repeat the cycle relentlessly.

Check

Monitor the environment, run penetration tests, and rigorously measure effectiveness.



Plan

Assess the expanding attack surface. Map resources and gaps using the FAN framework.

Do

Implement targeted controls specifically designed to address the most critical vulnerabilities.



Actively Shaping the Future

Our goal is not to be perfect tomorrow. It is to ensure that our security posture is decisively stronger, smarter, and more resilient in every single cycle.