
Gamify to Fortify
Implementing Gamification for Resilient Organizations
Dr. Lovelie Moore

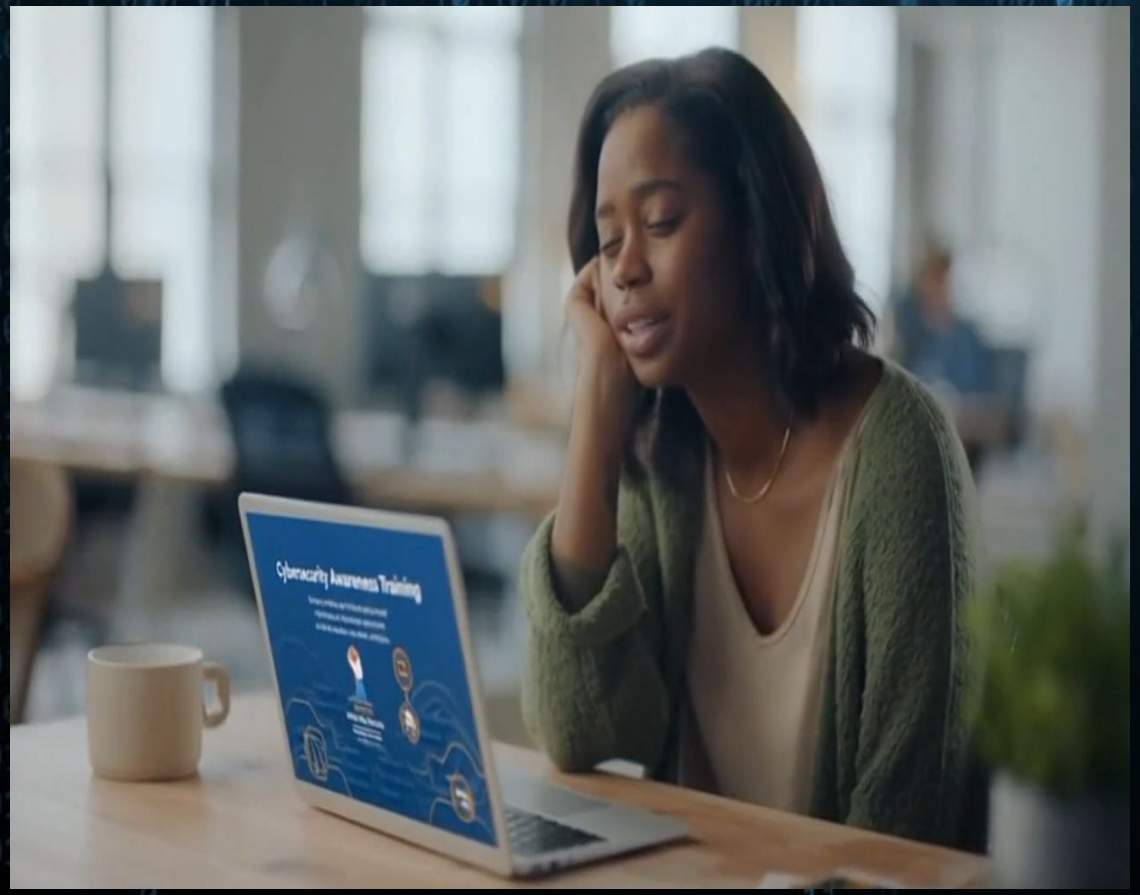
About Me

- Education
  - ***Doctor of Information Technology in Cybersecurity & Information Assurance***
- Career
  - ***Business Information Security Officer (BISO) – Toyota Financial Services***
  - ***Former U.S. Navy Information Professional Officer***
  - ***15+ years leading cybersecurity, risk***

Agenda

- Current State of Cybersecurity and Retention
- The Training Deficit
- Gamification
- The Traditional Approach
- Not Just Checking Boxes
- Current vs Future State
- Core Mechanics and Principles
- Psychological Drivers
- Metrics and ROI
- Resiliency
- Why AI

Current State of Cybersecurity Training

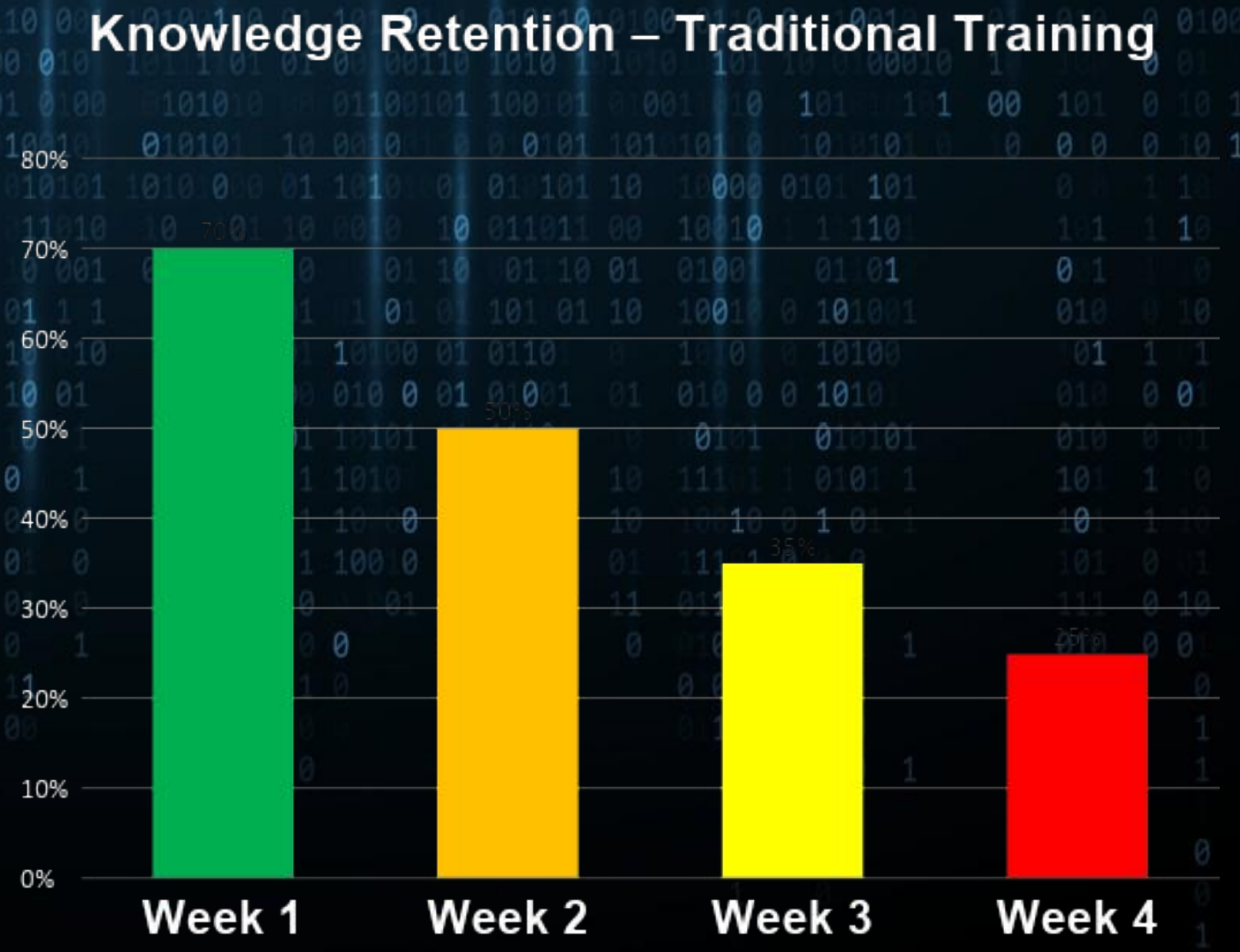


- It’s boring
- No one likes it
- Compliance dreads it
- Executives rely on it
- It burns money
- It strains the company
- IT’S ***BORING***….

Current State of Retention

Key Issues:

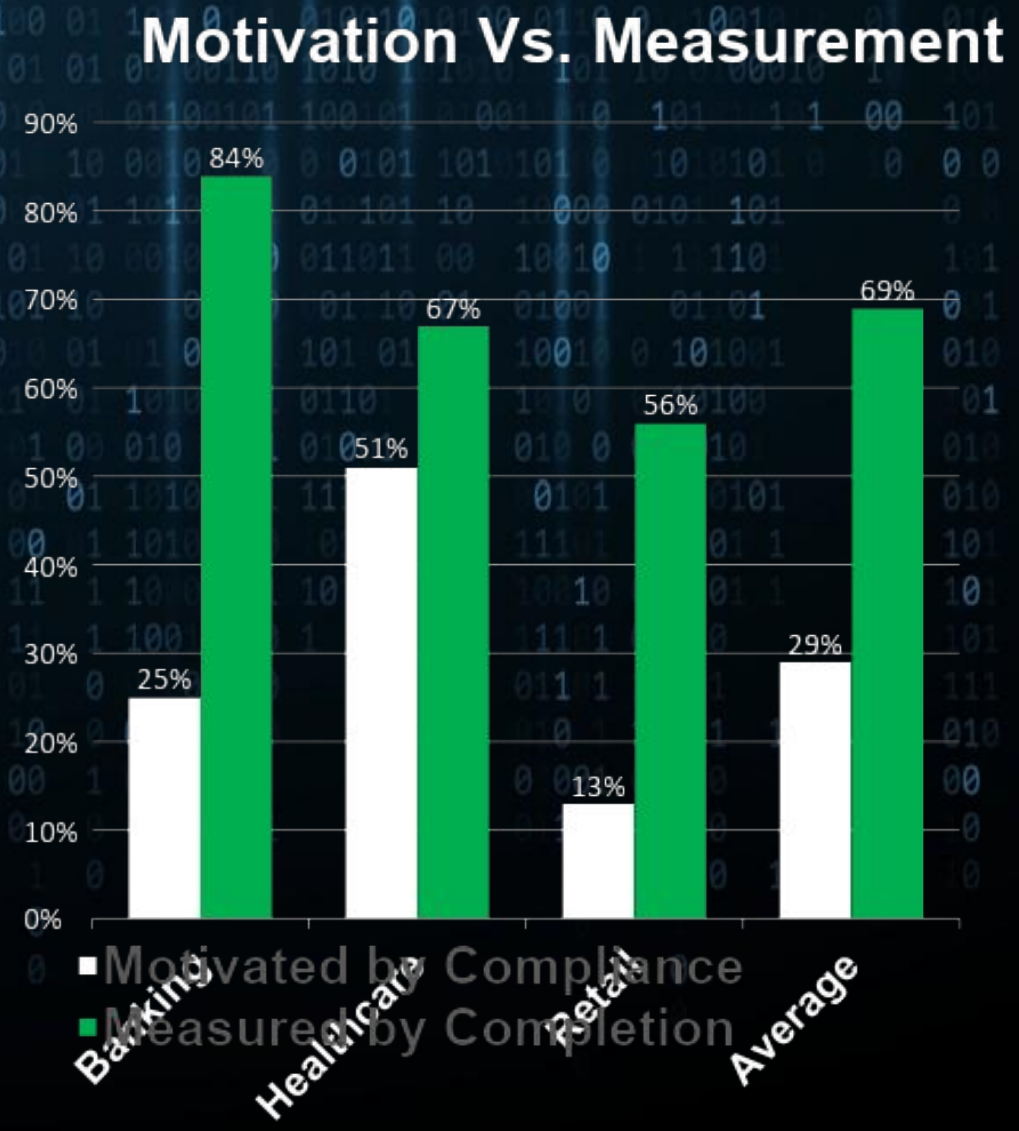
- Checkbox' training
- Low retention: <30% after 4 weeks
- 74% of breaches linked to human error
- Reactive culture: response occurs only after incidents



The Training Deficit

Why Traditional Security Training Falls Short

- **Compliance-Driven**
  - Traditional training often focuses on "checking boxes" rather than fostering genuine understanding or lasting behavioral change.
- **Rushed Engagement**
  - Employees rush through modules, resulting in low knowledge retention and high vulnerability to threats.
- **Persistent Vulnerability**
  - Focus on regulations rather than active engagement renders training ineffective against evolving threats.



What if we Gamified Cybersecurity Awareness Training?

- Everyone plays games
- Tiny missions, not long videos
- Instant feedback
- Real storyboards
- Fun
- Better Outcomes
- Compliance

How do we Gamify? We use AI!

Personalized Learning Paths

AI analyzes user interactions to identify knowledge gaps and deliver targeted content when and where needed.

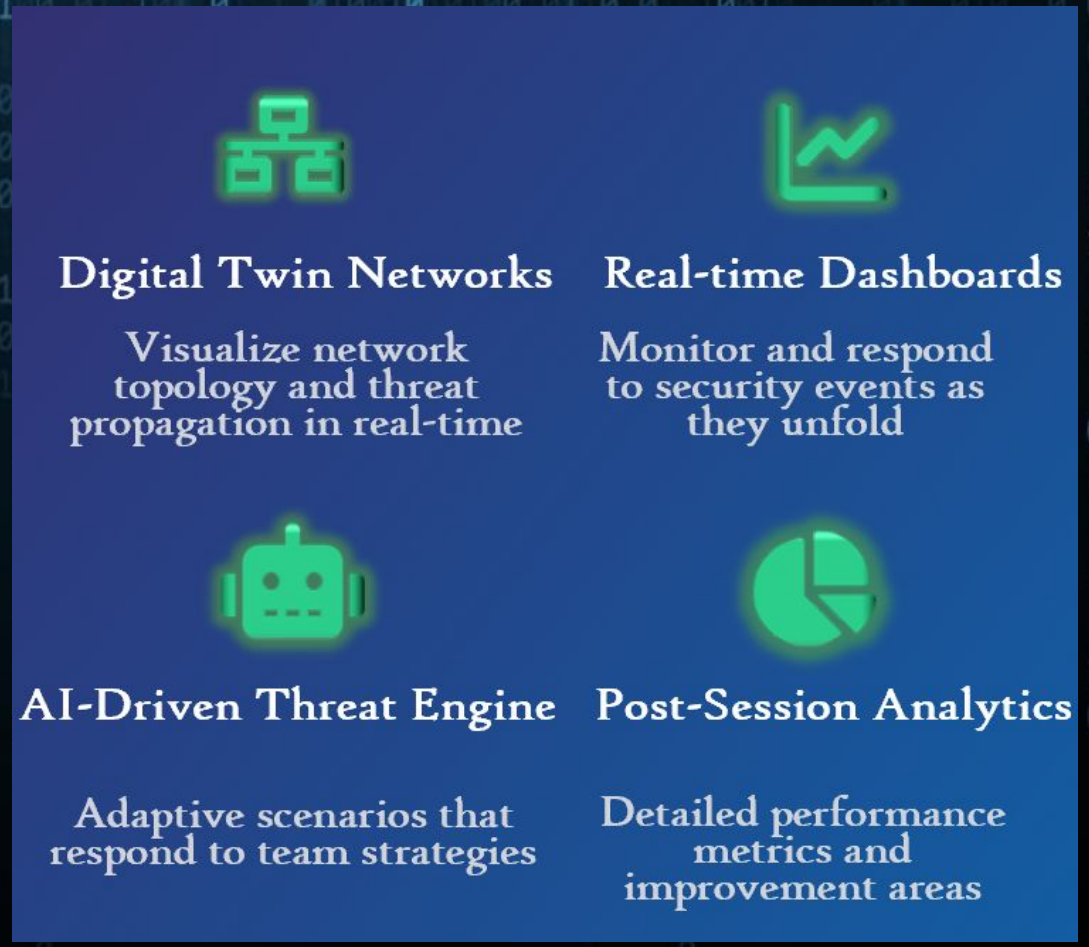
Targeted Intervention

Content difficulty automatically adapts based on performance, keeping users in an optimal learning zone.

Dynamic Difficulty Adjustment

A platform that delivers personalized phishing simulations and microlearning modules based on individual risk profiles.

Continuous Adaptation Reduced Vulnerabilities Accelerated Learning



"These immersive simulations go beyond traditional desktop exercises, placing users directly into scenarios that mimic real-world cyber threats."

Core Mechanics and Principles

Building Blocks of Gamified Security

Points & Badges

Provide immediate feedback and visual recognition for completing tasks and achieving milestones

Leaderboards

Display rankings of individuals or teams, introducing competitive elements that motivate.

Role-based Scenarios

Immerse users in realistic, simulated situations relevant to their specific job functions.

Simulations

Provide hands-on experience in identifying and responding to cyberattacks,

These mechanics collectively transform passive recipients into active participants in organizational defense

Before Gamification

The Reactive Security Posture

High Risk Behaviors

High failure to detect and report potential l threats proactively

Poor Threat Detection

Traditional training fails to equip organizations with the skills needed to identify emerging threats, leaving them vulnerable to sophisticated attacks.

Human Firewall Deficit

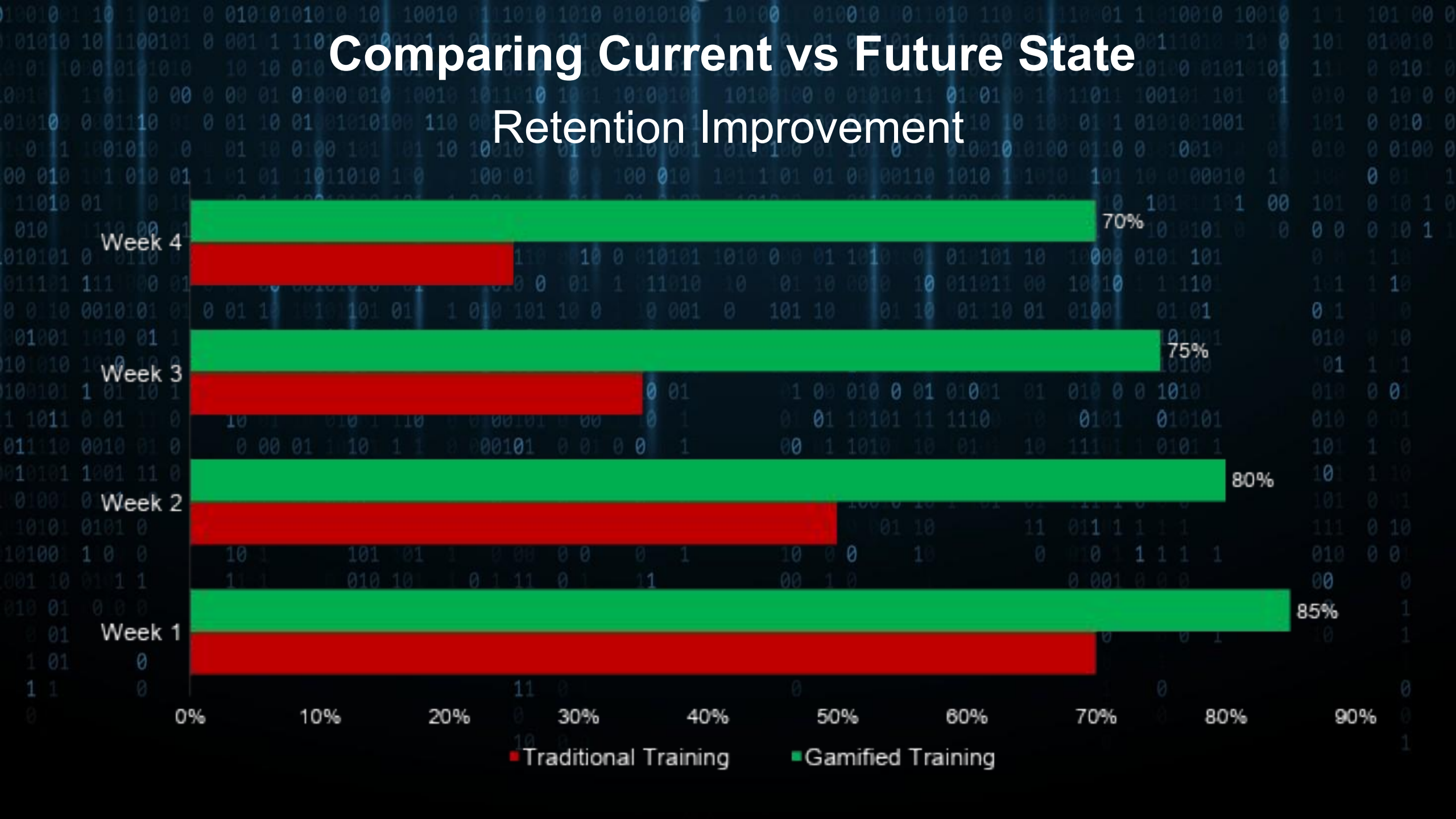
The workforce is ill-equipped to act as an effective human firewall against evolving cyber threats, relying instead on technical controls.

Reactive vs. Proactive Security

Reactive Security	Proactive Security
Broken then repaired	Upgraded continuously
Responding to incidents	Anticipating threats
Low engagement	Active engagement

Comparing Current vs Future State

Retention Improvement



Psychological Drivers

Why Gamification Works

Gamification taps into fundamental psychological motivators to foster a robust security culture:

Competition

Leaderboards introduce a competitive element, motivating participants to improve performance and strive for recognition.

"Leverages social comparison and the drive for status"

Achievement

Points and badges provide immediate feedback and visual recognition, tapping into the desire for achievement and mastery.

"Offers tangible rewards for effort and progress"

Mastery

Role-based scenarios allow users to practice decision-making in safe environments, building confidence and competence.

"Promotes a sense of competence and skill development"

The Impact on Security Culture

- Collaboration
- Accountability
- Continuous Learning

Transforming passive recipients of information into **active participants** in organizational defense.

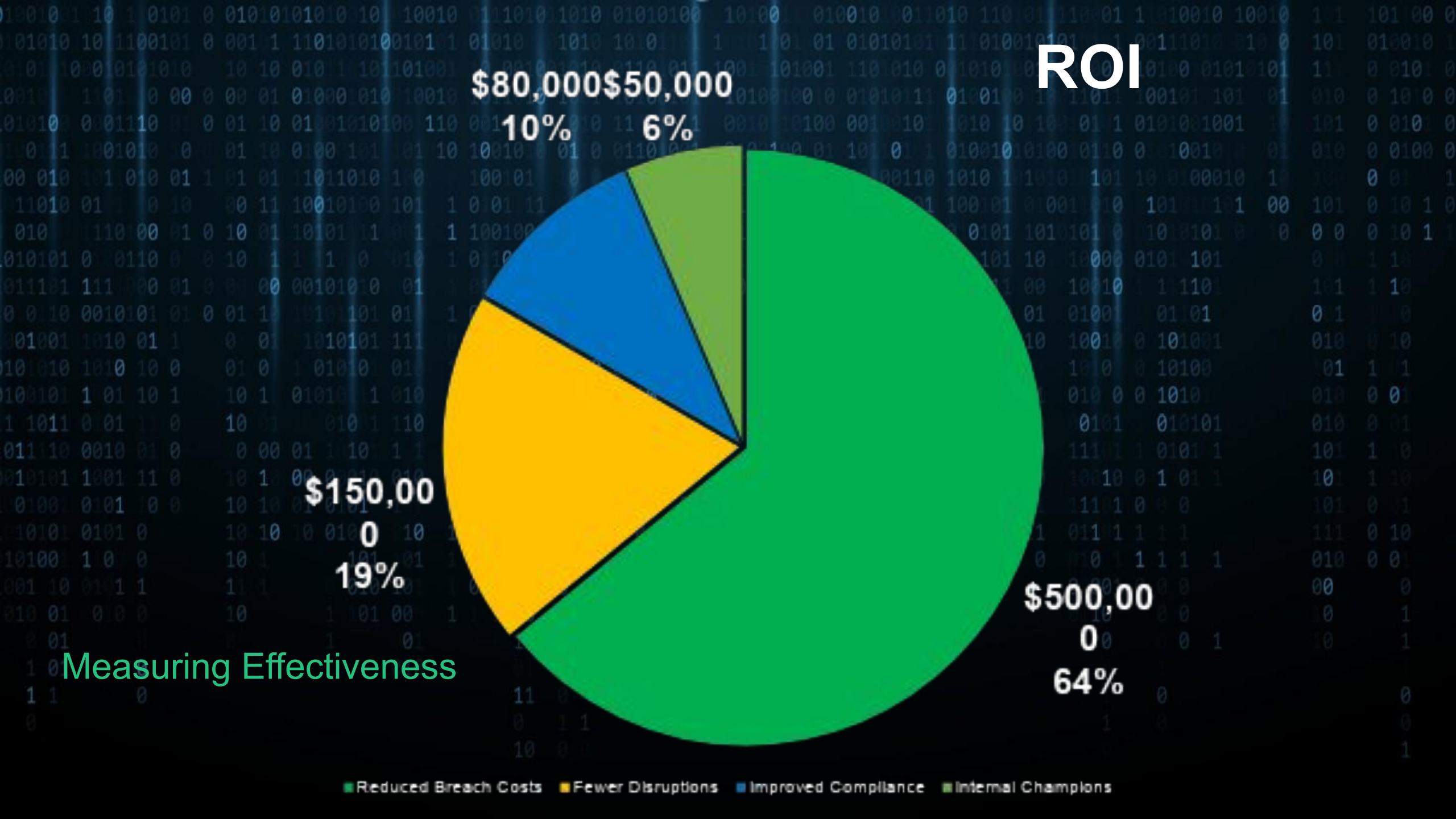
Success Metrics

Measuring Effectiveness

Key Performance Metrics

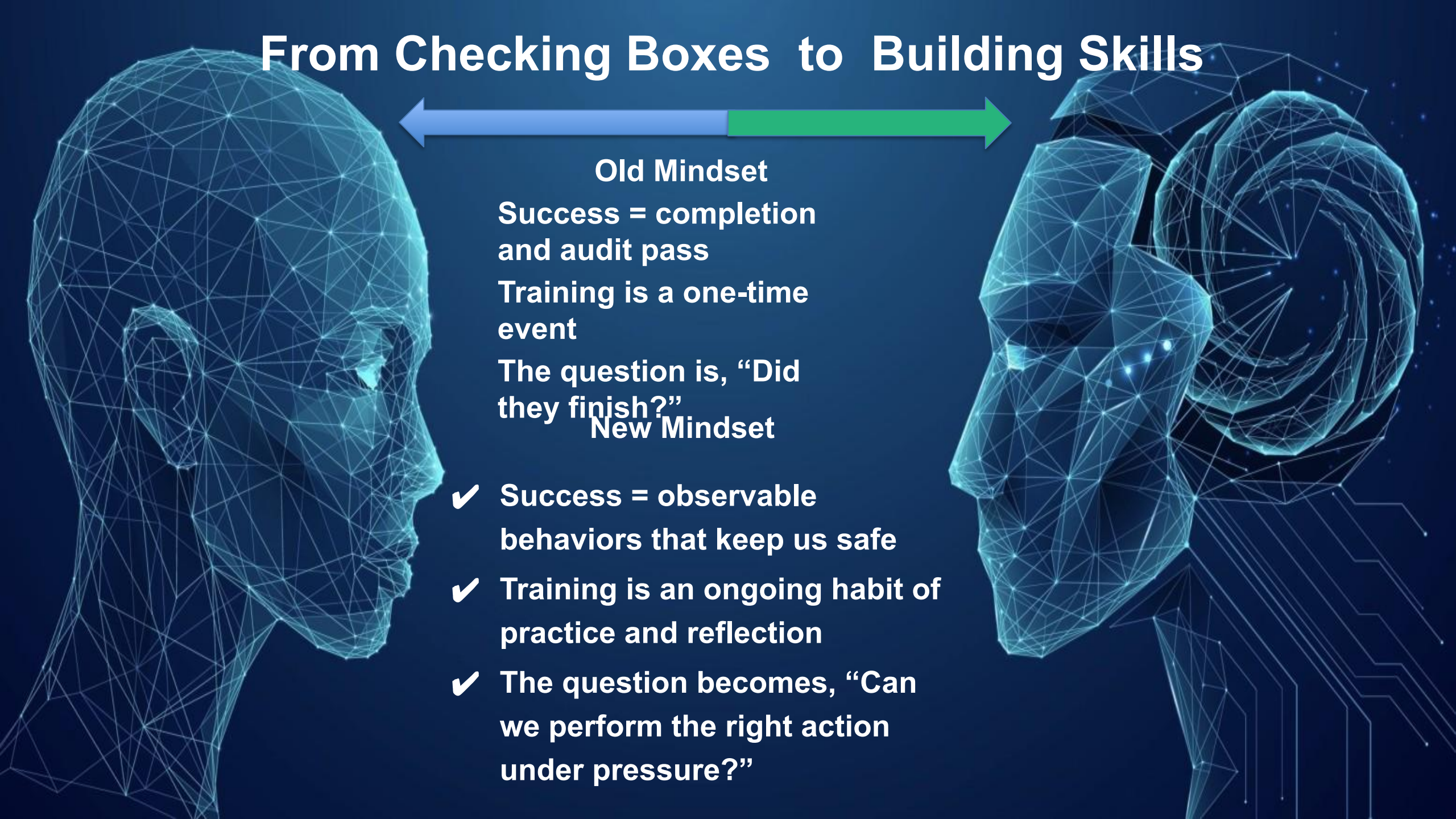
"Gamified training isn't just more engaging it delivers measurable security improvements a financial benefits."

ROI



Measuring Effectiveness

From Checking Boxes to Building Skills



Old Mindset

Success = completion and audit pass

Training is a one-time event

The question is, “Did they finish?”

New Mindset

- ✔ Success = observable behaviors that keep us safe
- ✔ Training is an ongoing habit of practice and reflection
- ✔ The question becomes, “Can we perform the right action under pressure?”

Resilient Implementation

Leadership Acceptance

- Strategic Alignment
- Foster change
- Influence
- Commitment
- Impact
- Support

Call to Action: Beyond Compliance

Building a Resilient Security Posture Through Gamification

CYBERSECURITY IS NO LONGER OPTIONAL

To fortify your organization's human firewall and cultivate a truly resilient security posture:

Move Beyond Compliance

Transform security training from a regulatory requirement to an engaging, interactive experience.

Engage Your Workforce

Foster a culture of continuous learning and collaboration around security awareness.

Embrace Gamification

Leverage game-design elements to create memorable learning experiences that build lasting skills.

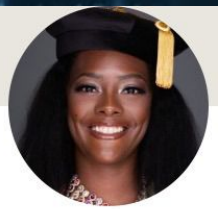
Traditional Training
Compliance-Driven

Gamified Training
Engagement-Driven

Resilient Security
Human Firewall

THANK YOU

Let's Connect



Dr. Lovelie Moore

DIT, MSIT, C|CISO, CISM, SEC+, CASP+,
Navy Veteran / Keynote / Public Speaker /...