ValueBridge Advisors

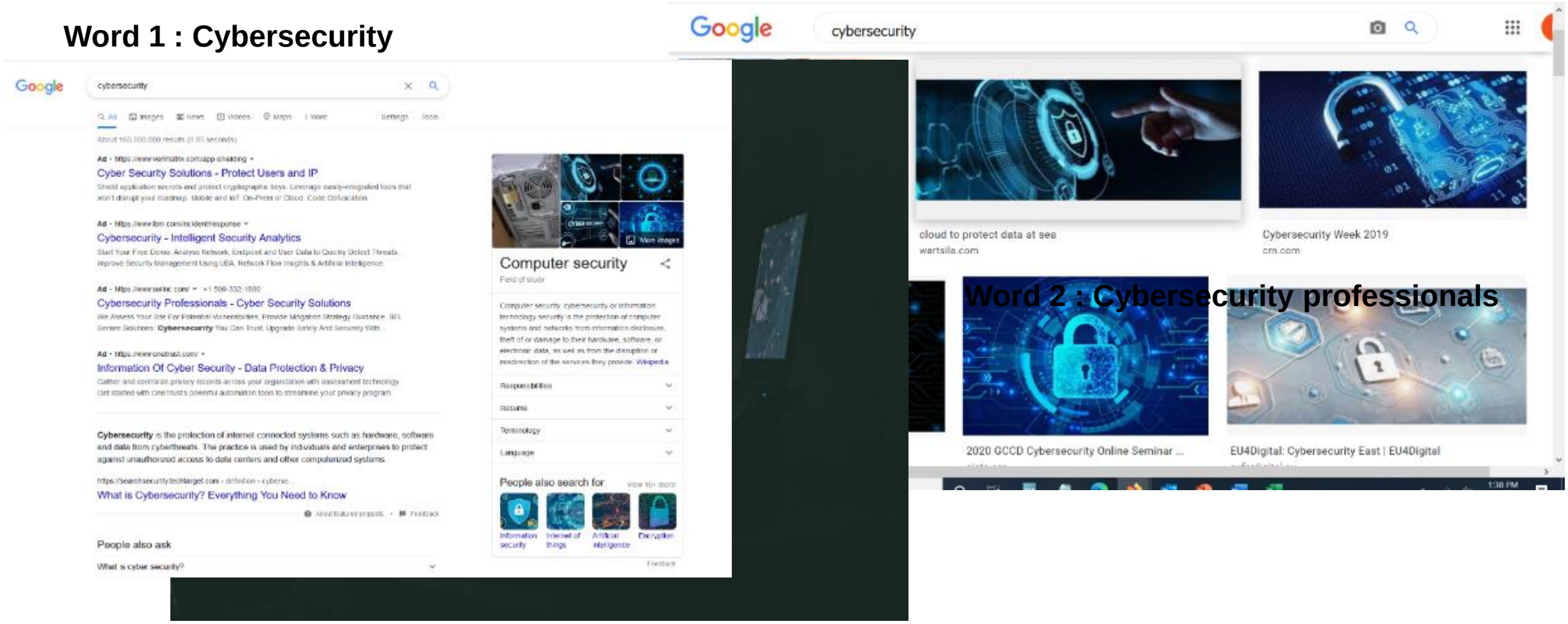
Design Thinking & Teaming to Cut Cyber Risk & Boost Resilience

Brian Barnier
Prachee Kale
April 19, 2021

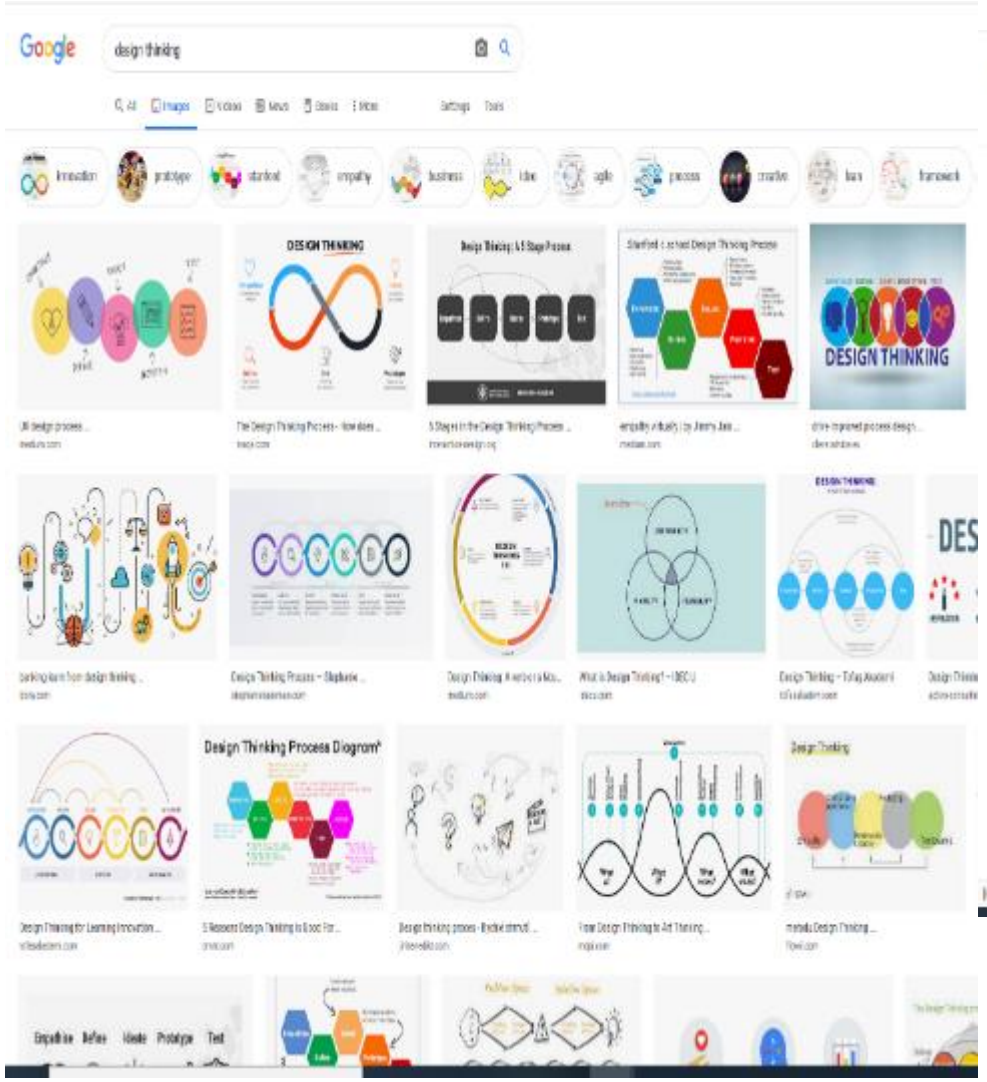
PERFORMATICA
STRATEGY · OPERATIONS · TECHNOLOGY · ALLIANCES

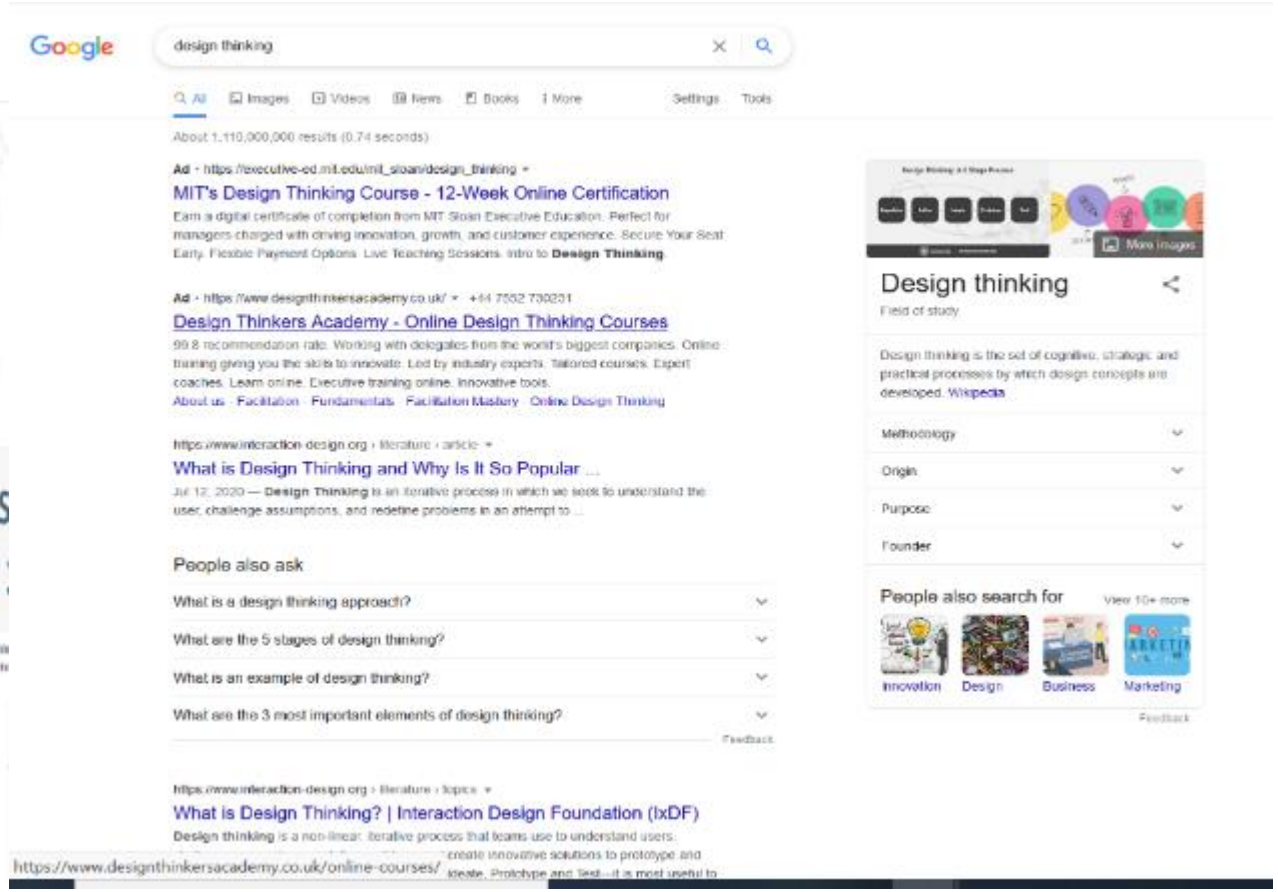
Let’s play: ‘What comes to mind!’ (Type your answers in chat!)

Word 1 : Cybersecurity



Word 3: Design Thinking – what comes to mind?! Type in chat!

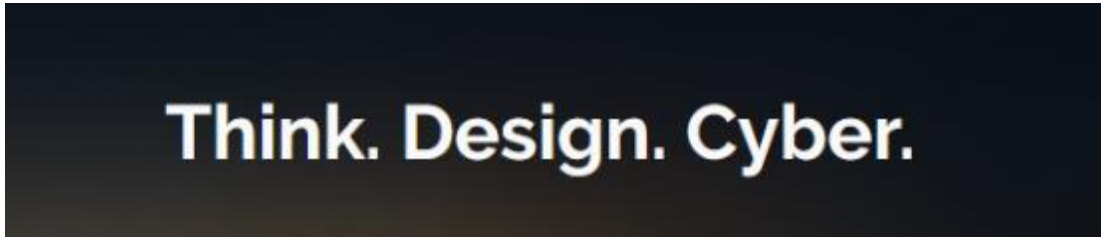




Cybersecurity and Design Thinking!

Our offer for you

- **Discover design thinking**
- **Apply design thinking to Cybersecurity**
- **Differentiate yourself**

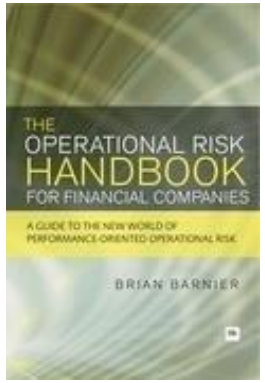


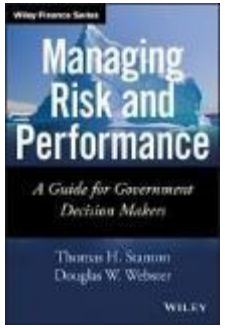
Prachee Kale

- Expert Generalist with a love of learning
- Dot Connector. Speaker. Writer. CyberCoach. Breaking the mold.
- Author of award winning EDPACS article!
- Currently applying business acumen to D&I and CSR
- Previously served in corporate America in Cybersecurity and Management Consulting
- Heard about PCR??? She's done them .. experimented with HIV infected cells
- She's deathly afraid of swimming in open waters but loves sailing!

Brian Barnier

- Thought leader of “systems thinking” for better security
- Creator of robust, film-style scenario design for security
- Contributor to multiple security frameworks and guides
- Recipient of ISACA V. Lee Conyers Award
- Created IBM’s “security as a process team”
- Launched first secure distributed messaging product
- Former bank regulator
- Author of accepted comments by Basel Committee

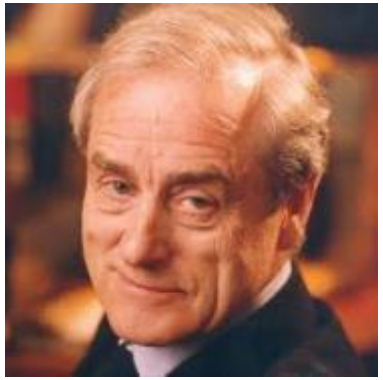


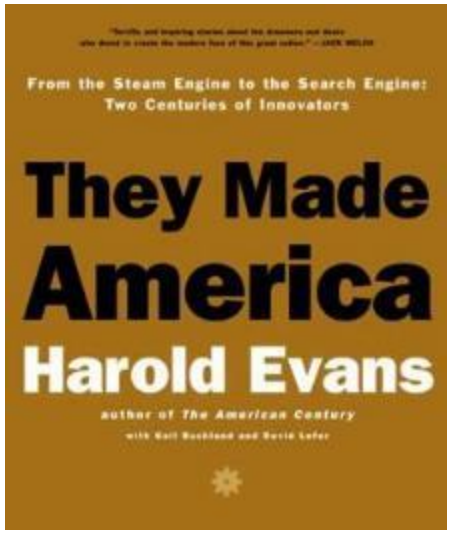


Discover design thinking

Design is everywhere, formalizing first in art and architecture

Design spirit to challenge prevailing views and innovate products



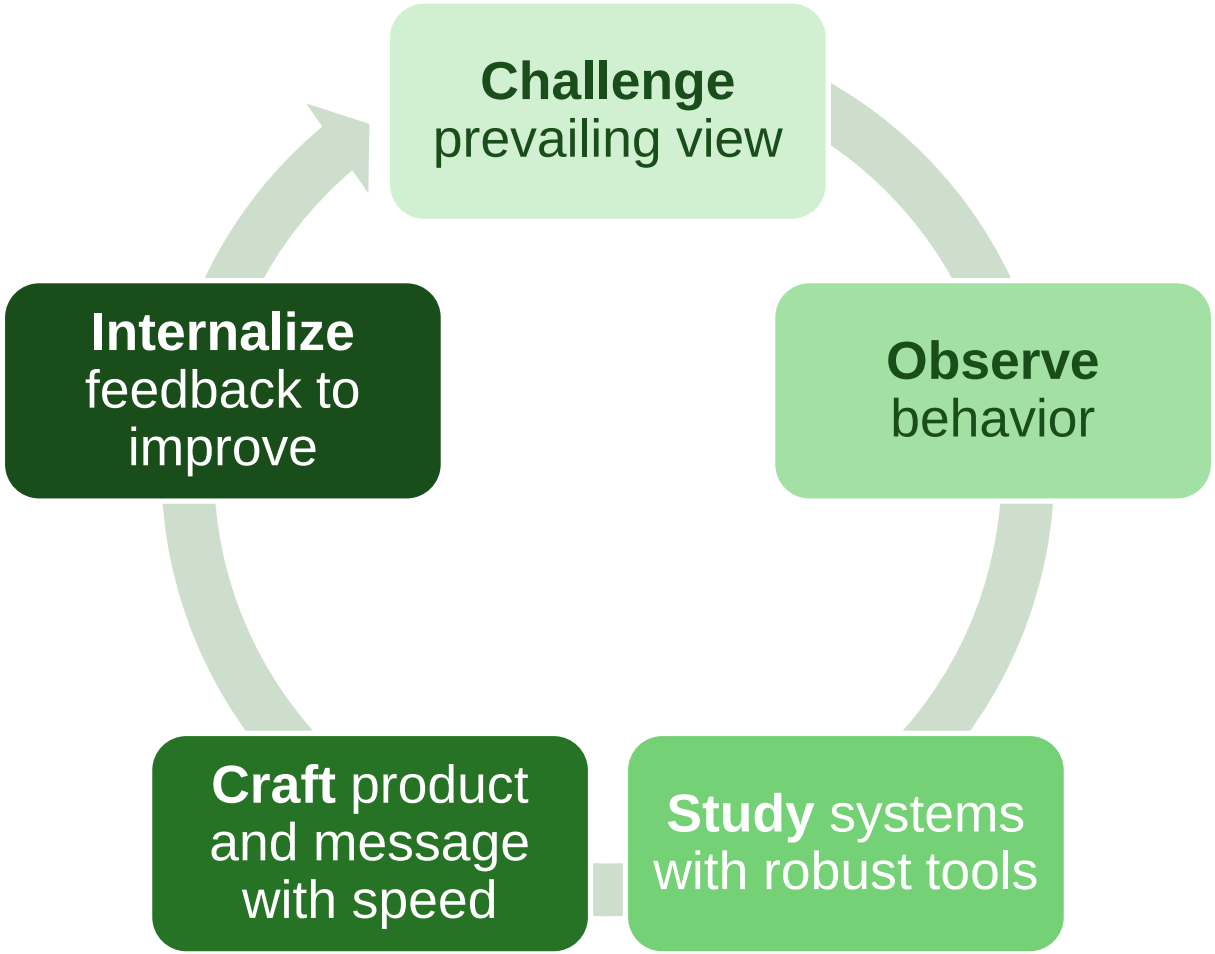


Think back…

What is “Design Thinking?”

- **Design Thinking is thinking like a designer**
- **Observing behavior to discover what people might need**
- **Design became formalized into schools of thought**
- **The study of how designers think became formalized into "Design Thinking”**

Design thinking DO cycle -- to *accelerate* outcomes



“Design Thinking” applications

- **Style**
- **Ease of:**
  - Use
  - Service
  - Manufacture

Design thinking – powerful, practical and popular

- **Examples of U.S. schools of thought…**
  - Rhode Island School of Design (1877)
  - Louis Sullivan and Chicago Architecture (1890s)
  - Cranbrook Academy of Art (1904)
  - College for Creative Studies (1906)
  - German Bauhaus (1919), Hasso Plattner Institute of Design (d.school) at Stanford, HPI School of Design in Germany – commercialized by firms such as IDEO
  - Military (with lessons for cyber), mid-1990s
  - Plus, influences of disciplines such as manufacturing, psychology, sociology and anthropology

- **Concepts variously emphasized by schools**
  - Expansive and empathetic
  - Human centric – what users need or desire from a product or process
  - Re-framing the problems
  - Challenging prevailing norms
  - Solution focused thinking
  - Experimental and progressive changes to product and process
  - Multi-disciplinary and cross-functional
  - Highly collaborative

Design thinking is all around you…

Double design – business and product

Reframing problems!

Focus on Physician

vs.

Focus on Patient

https://www.nist.gov/blogs/taking-measure/making-sure-virtual-doctor-visits-are-private-and-secure

Design thinking in cybersecurity

A pioneer's origin story -- design in Detroit

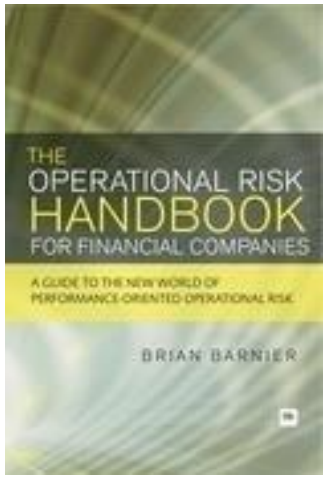
UNIVERSITY OF MICHIGAN

Merle Crawford

Michigan Banking & Business News

Judith Olson

ISACA Journal



IBM Financetech

Tivoli software Security ISACA

9 Patents
Lucent Technologies
Bell Labs Innovations

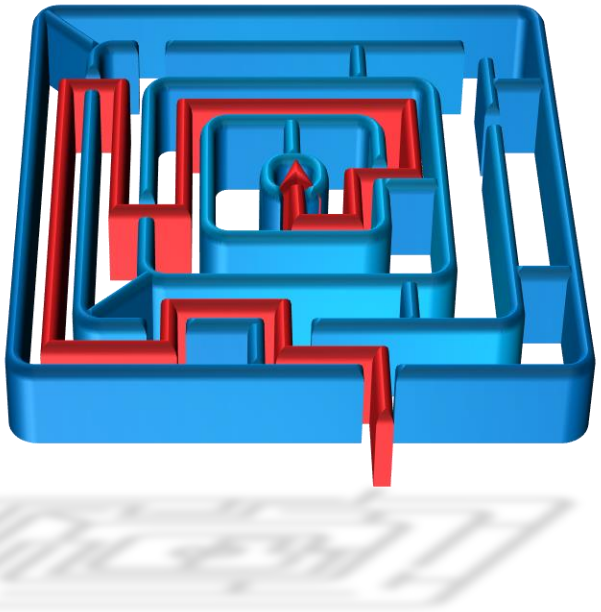
UNIVERSITY OF DETROIT MERCY

Design from Detroit energizes design in cybersecurity with…

- **Challenge to prevailing views**
- **Systems insight**
- **Robust tools**
- **Organizational change – both desired and forced**

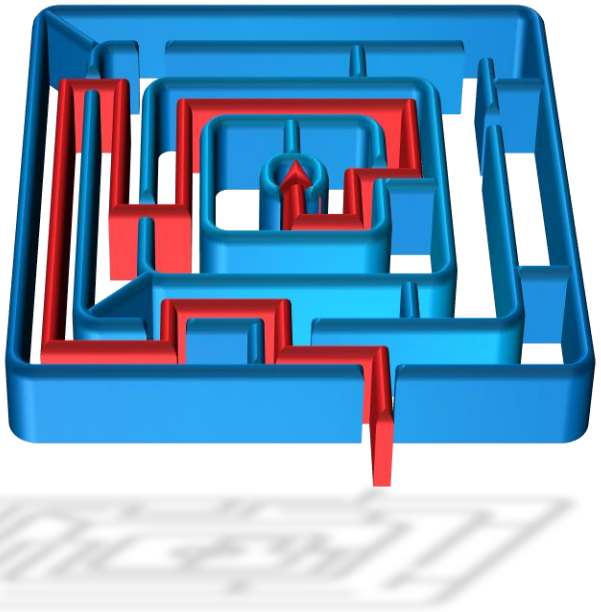
Design thinking for cybersecurity is NOT primarily about:

- User Experience (UX) design to make security easier for users
- Earlier design of security into Dev or DevOps
- Using individual cybersecurity tools/appliances
- Linear process, design is iterative



Design thinking is primarily about outthinking and outmaneuvering adversaries by…

- **Challenging** prevailing view and “trusted sources”
- Designing **teams** that can see broadly, think clearly and take action to solve problems
- **Reevaluating** math, method and tools



Design thinking succeeds through diverse, high performing teams

TRADITIONAL TEAMS	DESIGN THINKING TEAMS
• Focus on problems	• Reframe problems
• Process driven	• Solution focused
• “Group Think”	• Divergent Thinking
• Conforming	• Breaking the mold!
• Cross-functional	• Multi-disciplinary and Cross-functional
• Segmented data	• Users, empathy and broader data
• Siloed & Hierarchical	• Collaborate and Cocreate

Apply design thinking to Cybersecurity

Big scary reasons to think differently

Breaches

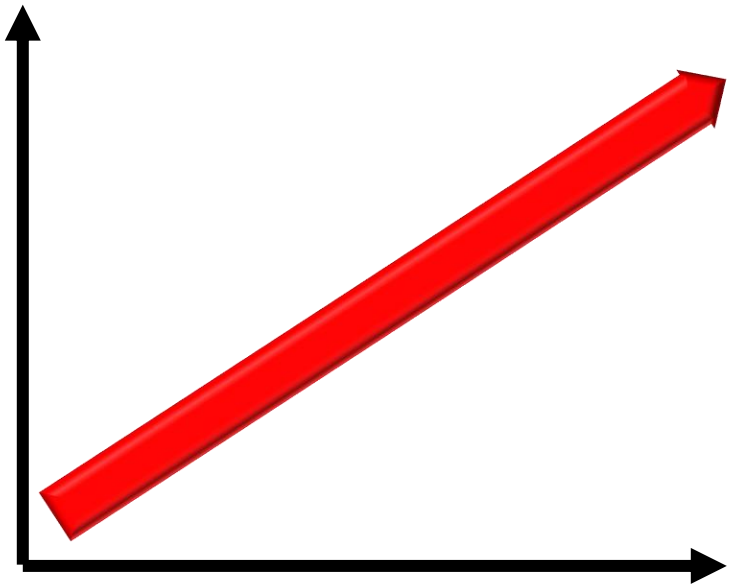
Budgets

Regulation

Ransom

Hostility

Change



Complexity

Confusion

Fatigue

Management Focus

Is cybersecurity performance acceptable elsewhere?

Why do adversaries win?

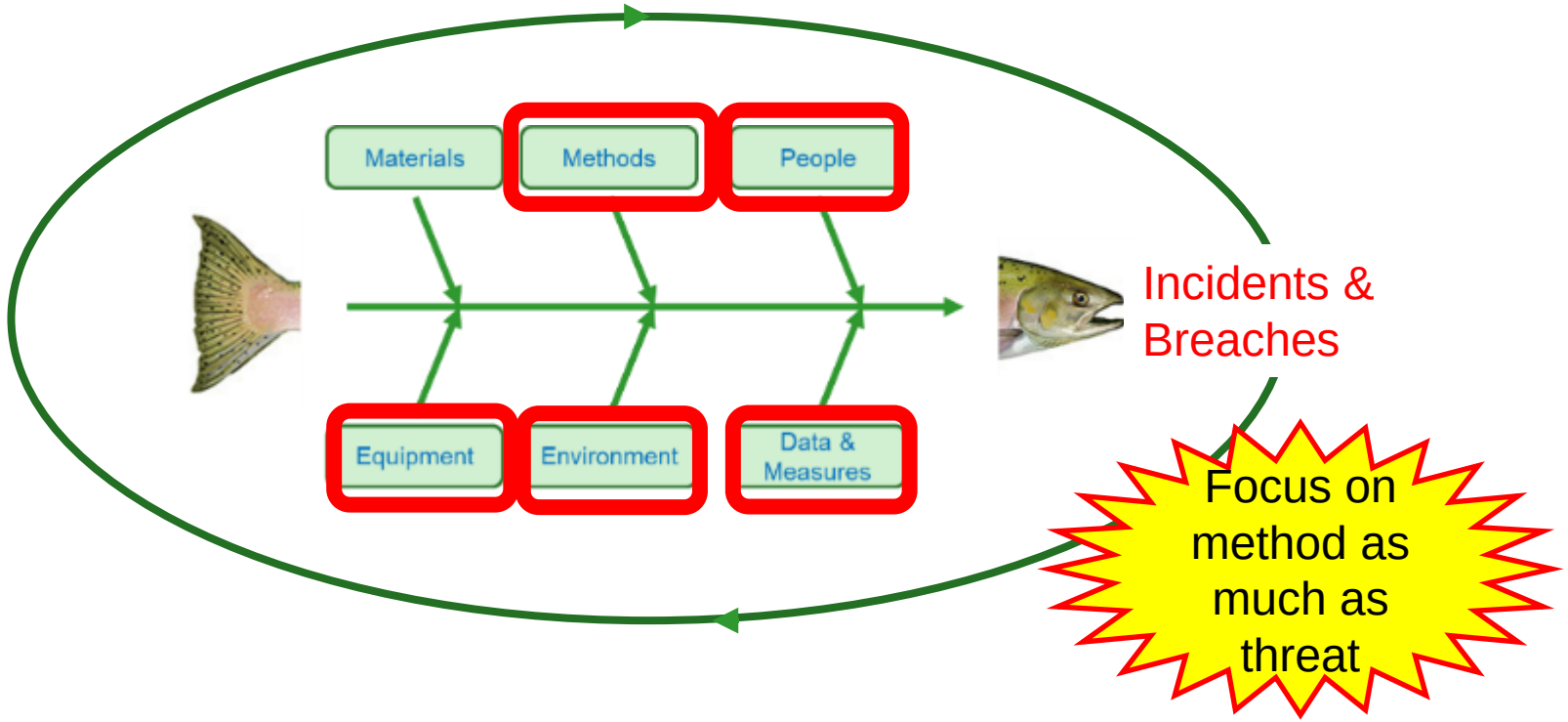
Or, more painfully, why do cyber teams continue to lose?

Adversaries win when they better understand “how it works,” so…

To outthink your adversaries…

Start by learning “how it works” better than your adversaries

And learn the cause of incidents and breaches. They are mostly self-inflicted.

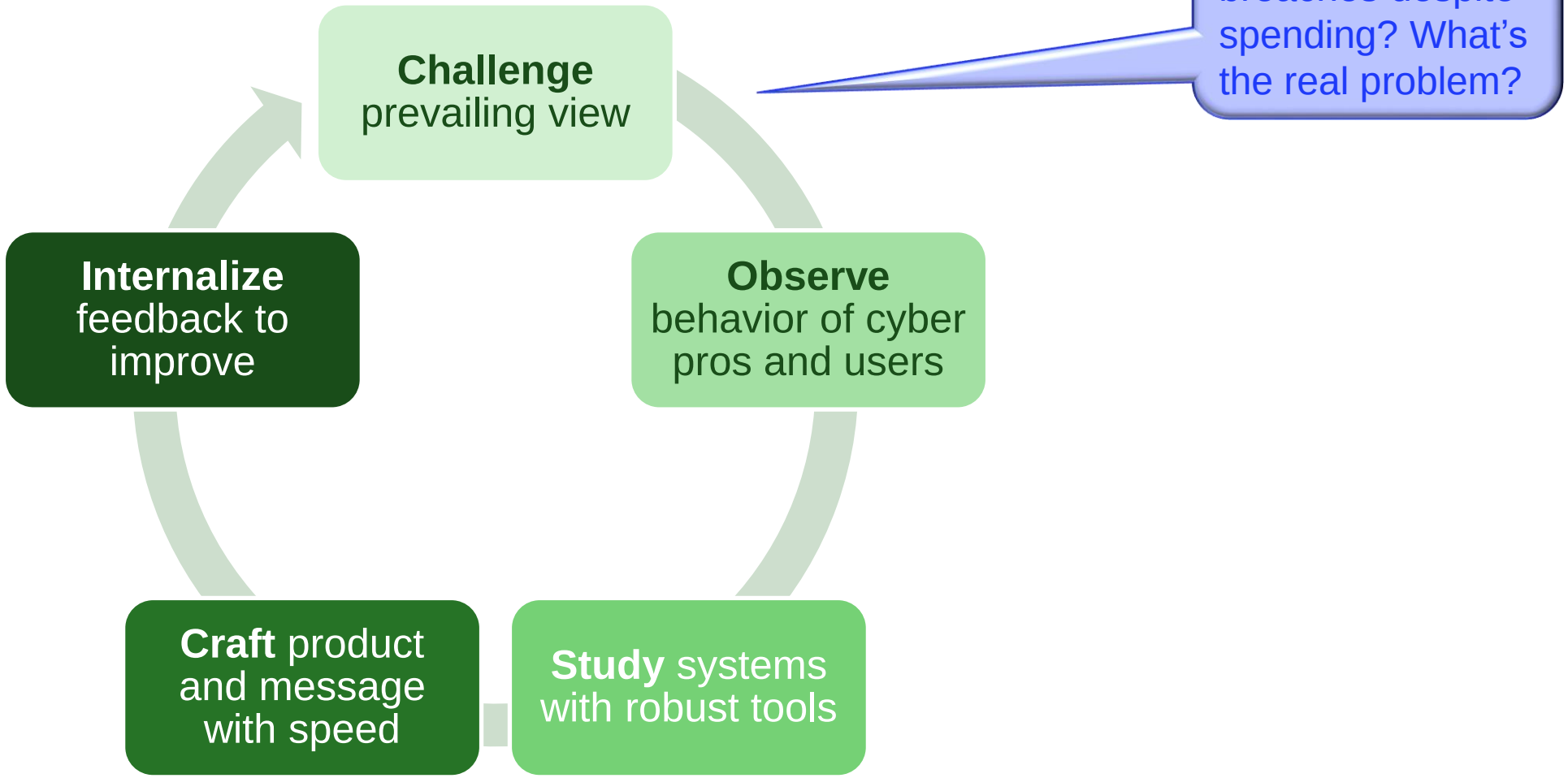


Kaoru Ishikawa, 1915-1989

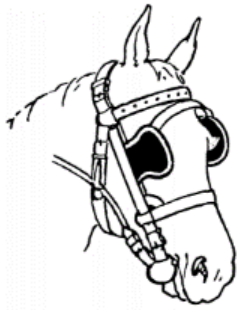
What does it take to sound the alarm?!

Your opportunity -- our world, safer with design

Design thinking DO cycle to achieve better outcomes



Structural Blindness & Cognitive Bias



Errors in structure of our organization, processes, communication and information

Errors in how we encode, interpret and process information that affect our judgments and decisions

Example 1 – As root cause is the method, do “frameworks” meet the design tests of effectiveness?

- **Are they fragile – highly sensitive to assumptions?**
- **Are they frozen in time?**
- **Do they fence out new thinking and improvement?**
- **Are they implemented as intended by their designers?**
- **Do they meet the design definition “A framework is a network of interlinked concepts that provide a comprehensive understanding of a phenomenon.” -- Yosef Jabareen**

Many “frameworks” include “controls.”
But they are not designed to achieve the presumed objective.

- **Two types of “controls”…**
  - Financial reporting (ICFR)
  - Automated -- far more reliable, “work like a light switch”

- COBIT 5 AN ISACA® FRAMEWORK **stopped fuzzy use of word “controls” in 2012**

Example 2 – The 20 Center for Internet Security (CIS) Controls

- **Basic CIS Controls (a.k.a., "hygiene")**
  - 1. Inventory and Control of Hardware Assets
  - 2. Inventory and Control of Software Assets
  - 3. Continuous Vulnerability Management
  - 4. Controlled Use of Administrative Privileges
  - 5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
  - 6. Maintenance, Monitoring and Analysis of Audit Logs
- **Foundational CIS Controls**
  - 7. Email and Web Browser Protections
  - 8. Malware Defenses
  - 9. Limitation and Control of Network Ports, Protocols and Services
  - 10. Data Recovery Capabilities
  - 11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
  - 12. Boundary Defense
  - 13. Data Protection
  - 14. Controlled Access Based on the Need to Know
  - 15. Wireless Access Control
  - 16. Account Monitoring and Control
- **Organizational CIS Controls**
  - 17. Implement a Security Awareness and Training Program
  - 18. Application Software Security
  - 19. Incident Response and Management
  - 20. Penetration Tests and Red Team Exercises

CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

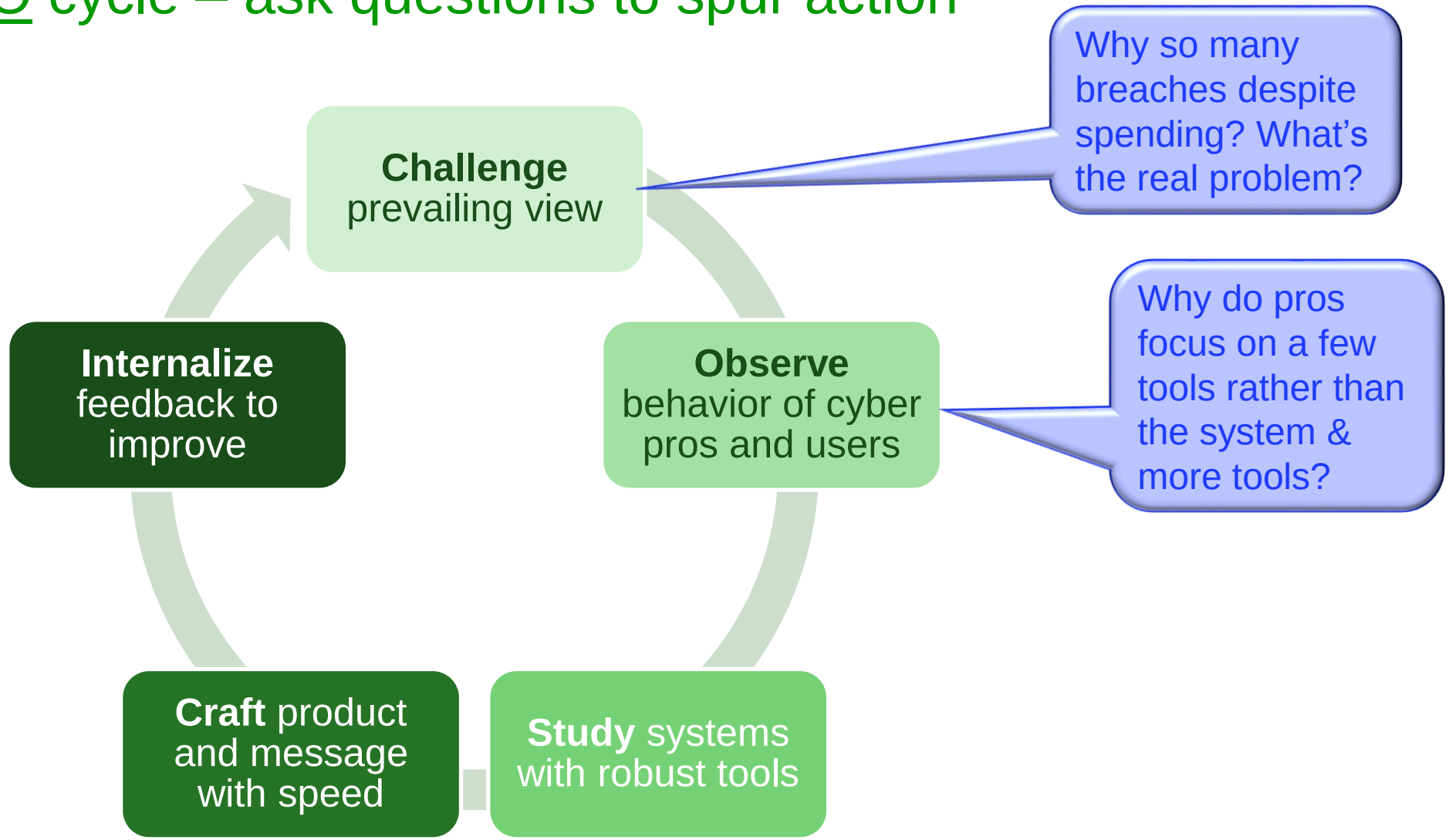
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	Implementation Groups		
					1	2	3
5.1	Applications	Protect	Establish Secure Configurations	Maintain documented security configuration standards for all authorized operating systems and software.	●	●	●
5.2	Applications	Protect	Maintain Secure Images	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.		●	●
5.3	Applications	Protect	Securely Store Master Images	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.		●	●
5.4	Applications	Protect	Deploy System Configuration Management Tools	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.		●	●
5.5	Applications	Detect	Implement Automated Configuration Monitoring Systems	Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		●	●

Source: CIS Controls V7.1, p22

Would CIS controls protect your grandmother's "secret sauce?"

- **Maintain** documented shelf configuration
- **Maintain** secure images of shelves
- **Store** those images in secure location
- **Deploy** system to prevent changing shelves
- **Utilize** SCAP-compliant system to alert if shelf is changed

Design thinking DO cycle – ask questions to spur action



The best tools and ingredients cannot make a delightful meal

In cyber, like cooking, need systems skill of “how it works”

Example 3

What is one of the most common attack vectors?

How many cyber teams talk to users to understand their behavior?

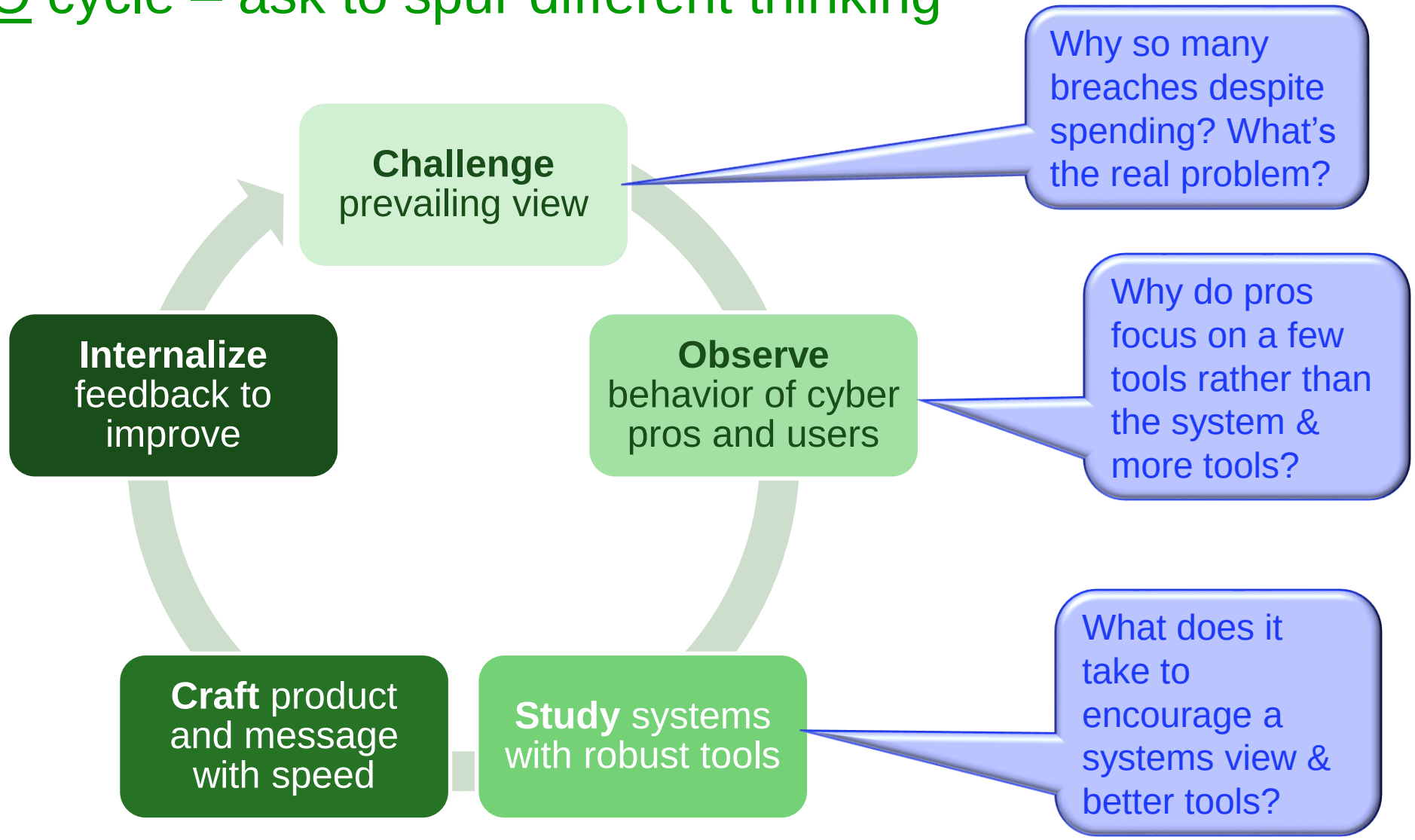
What is the problem? Who is responsible?

Reframe the problem?!

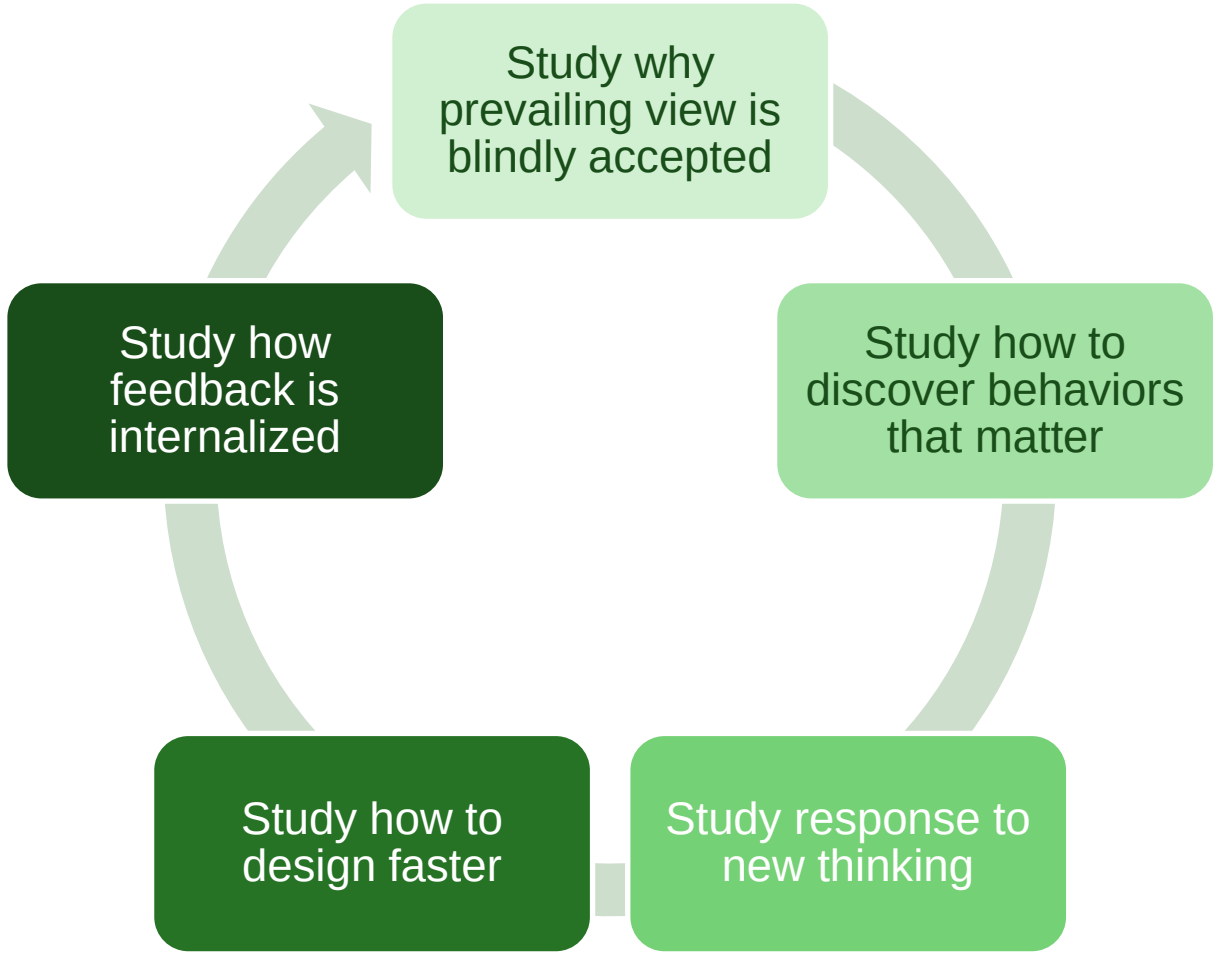
Is it the Cyber team or the user?

https://www.campussafetymagazine.com/safety/email-phishing-scam-manor-isd/

Design thinking DO cycle – ask to spur different thinking



The DO cycle must first be *designed* by the design thinking PLAN cycle

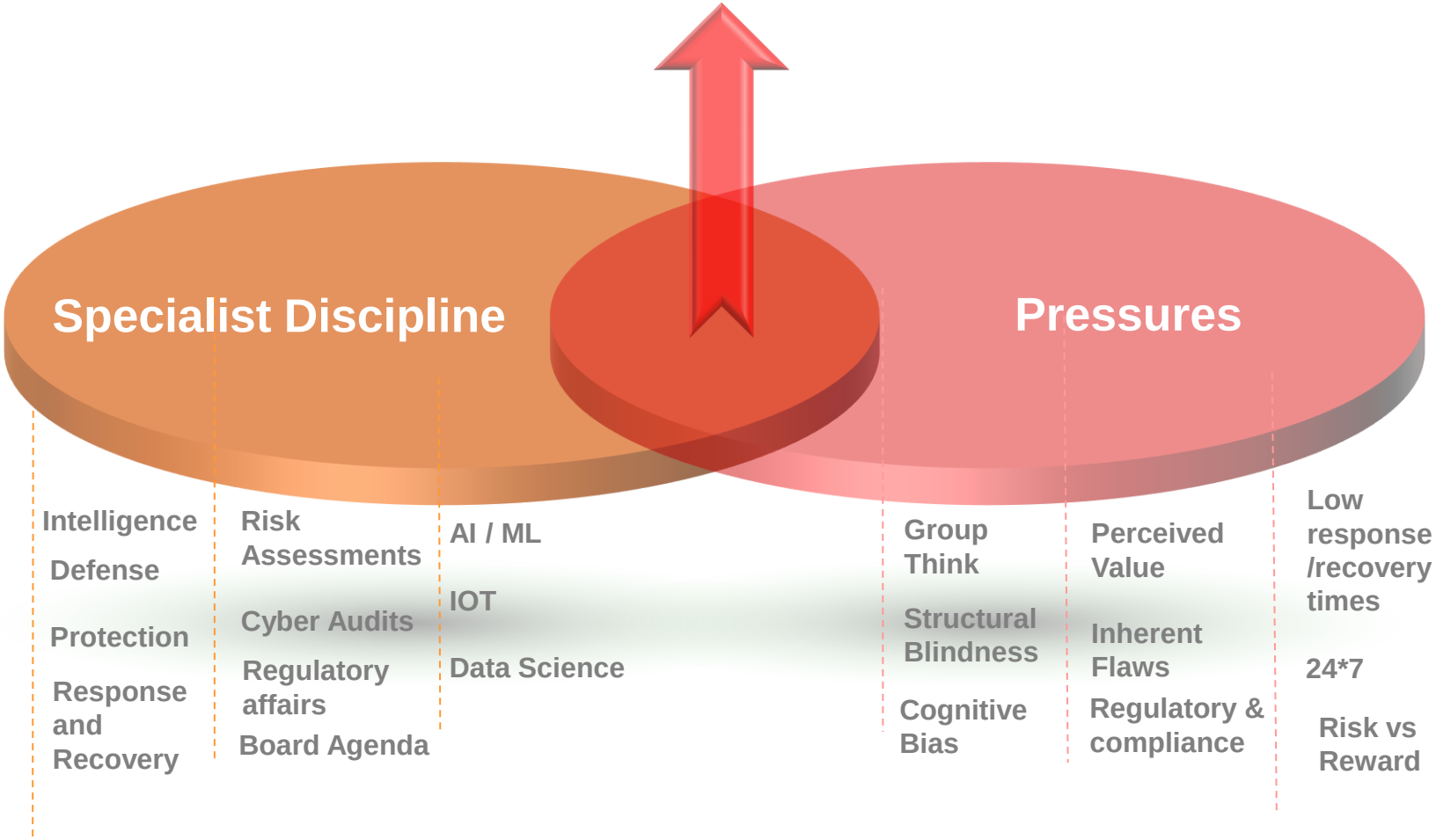


Be empowered to make a difference – whatever your role

- **Design and cyber expertise**
- **Exercise and practice**
- **Share your voice and discover each teammate's experience**
- **Invigorate your team -- be a multiplier**
- **Gain business insight (e.g., how do you make money?)**
- **Now**

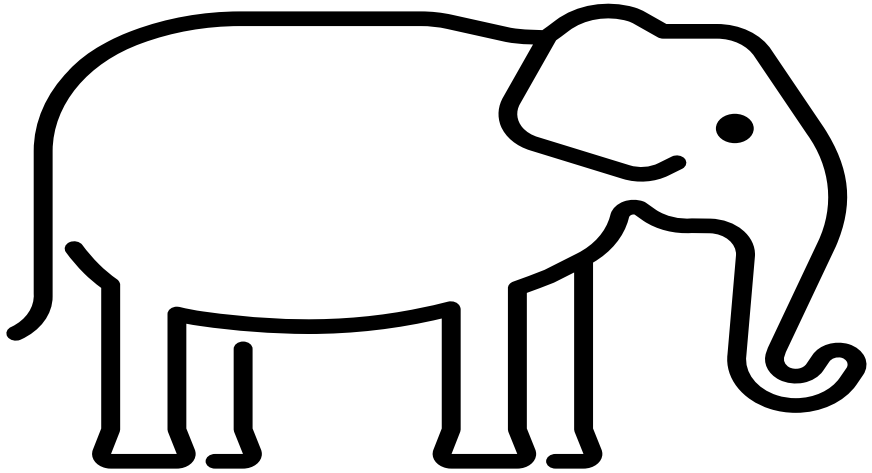
Differentiate Yourself

Cybersecurity needs design thinking **intervention**!

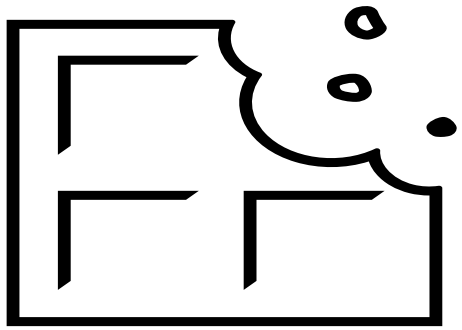


Infusing design thinking in your work

How do you eat an elephant?!



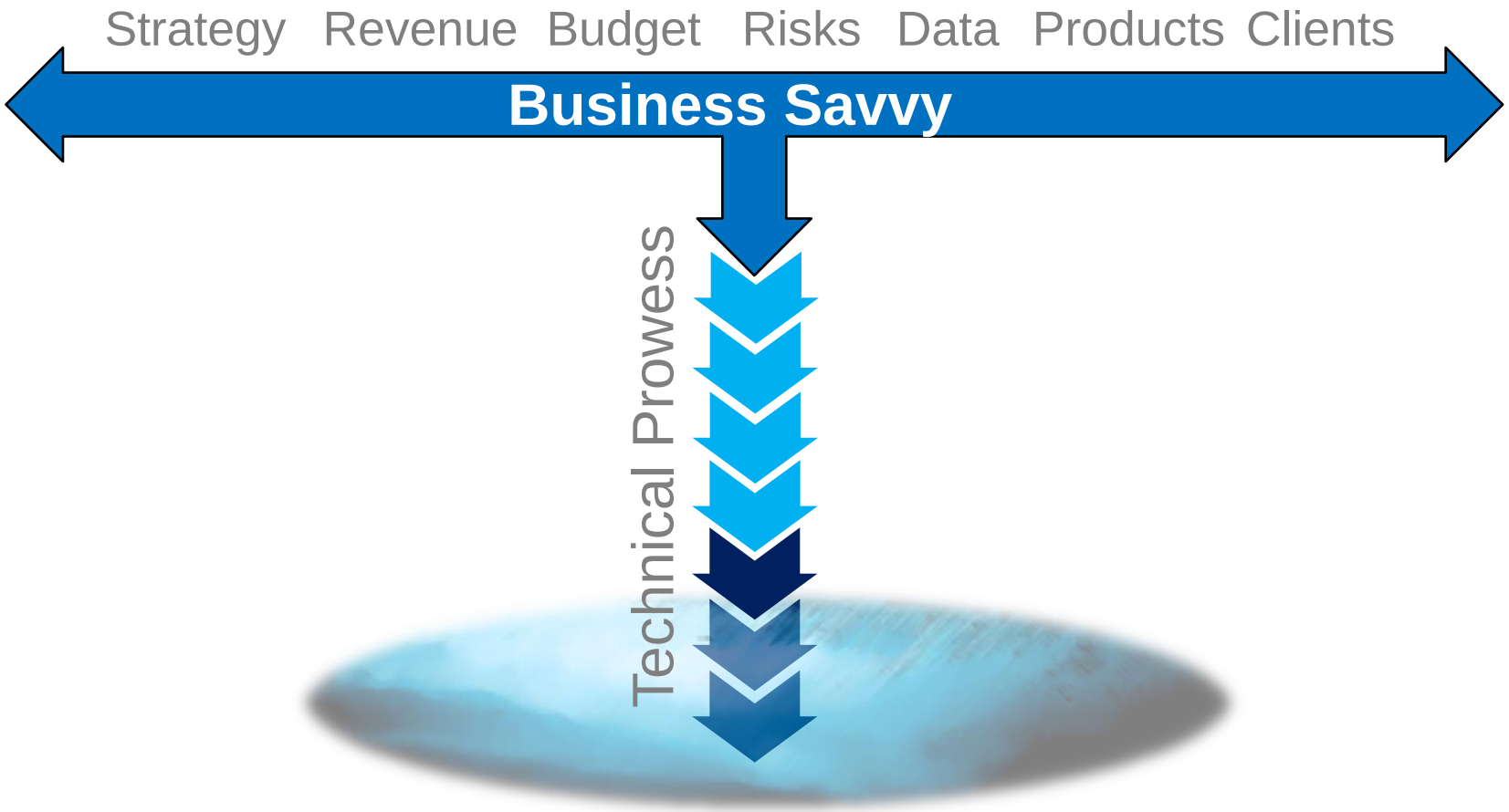
One bite at a time!



Individual contributors - Start with yourself

- Ask distinctive questions
  - Why have we done it this way?
  - What is? – Reframe the problems
  - What if? – Develop alternative views
  - Could we? – Explore possibilities
  - What works? – Iterative solution finding

Individual contributors - Start with yourself

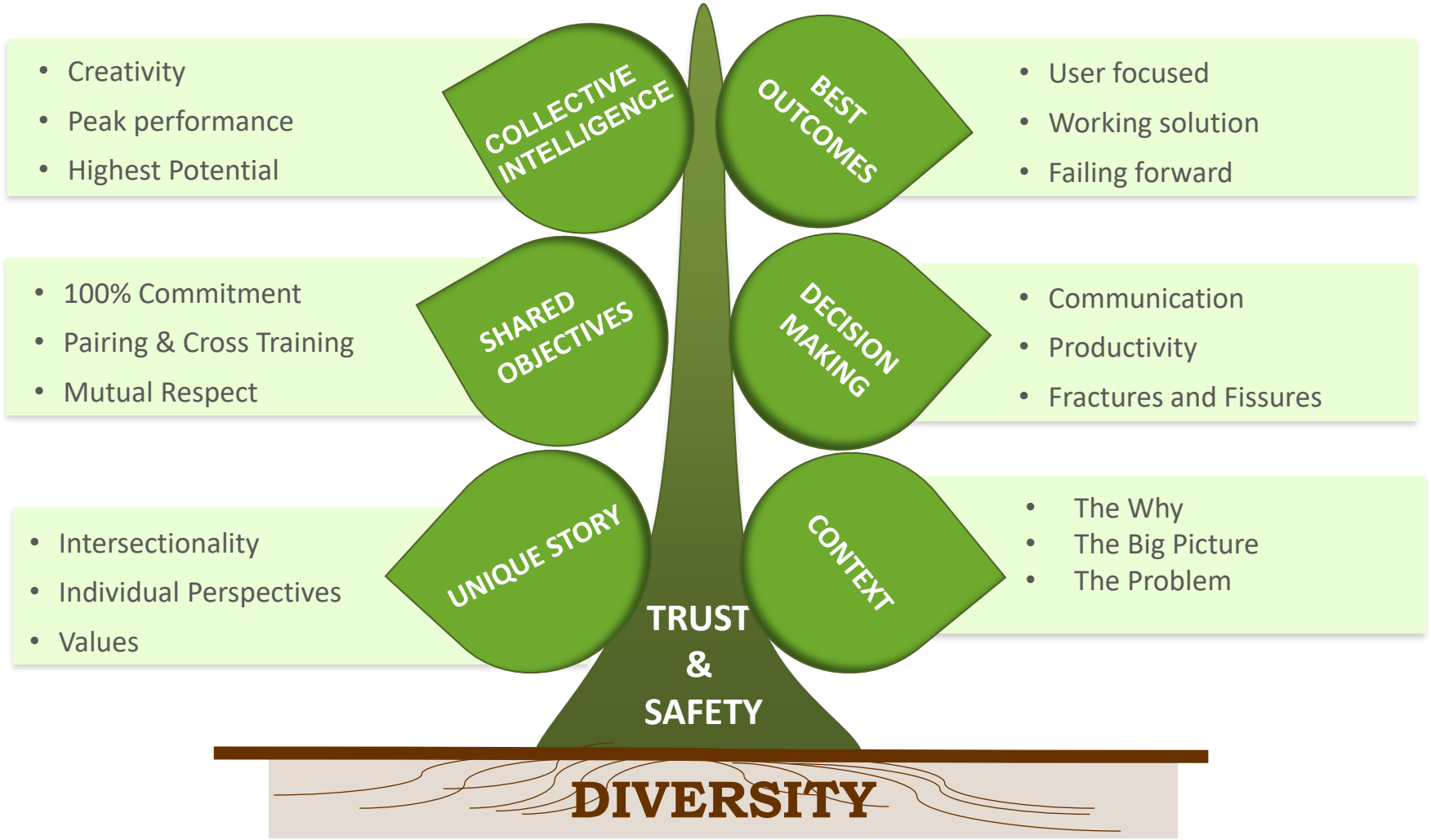


YOU + 1 + [….. MORE] = TEAM!

Design thinking succeeds through diverse, high performing teams

TRADITIONAL TEAMS	DESIGN THINKING TEAMS
• Focus on problems	• Reframe problems
• Process driven	• Solution focused
• “Group Think”	• Divergent Thinking
• Conforming	• Breaking the mold!
• Cross-functional	• Multi-disciplinary and Cross-functional
• Segmented data	• Users, empathy and broader data
• Siloed & Hierarchical	• Collaborate and Cocreate

Managers: Grow into a diverse, design thinking, high performing team



Design success depends on organizational integration

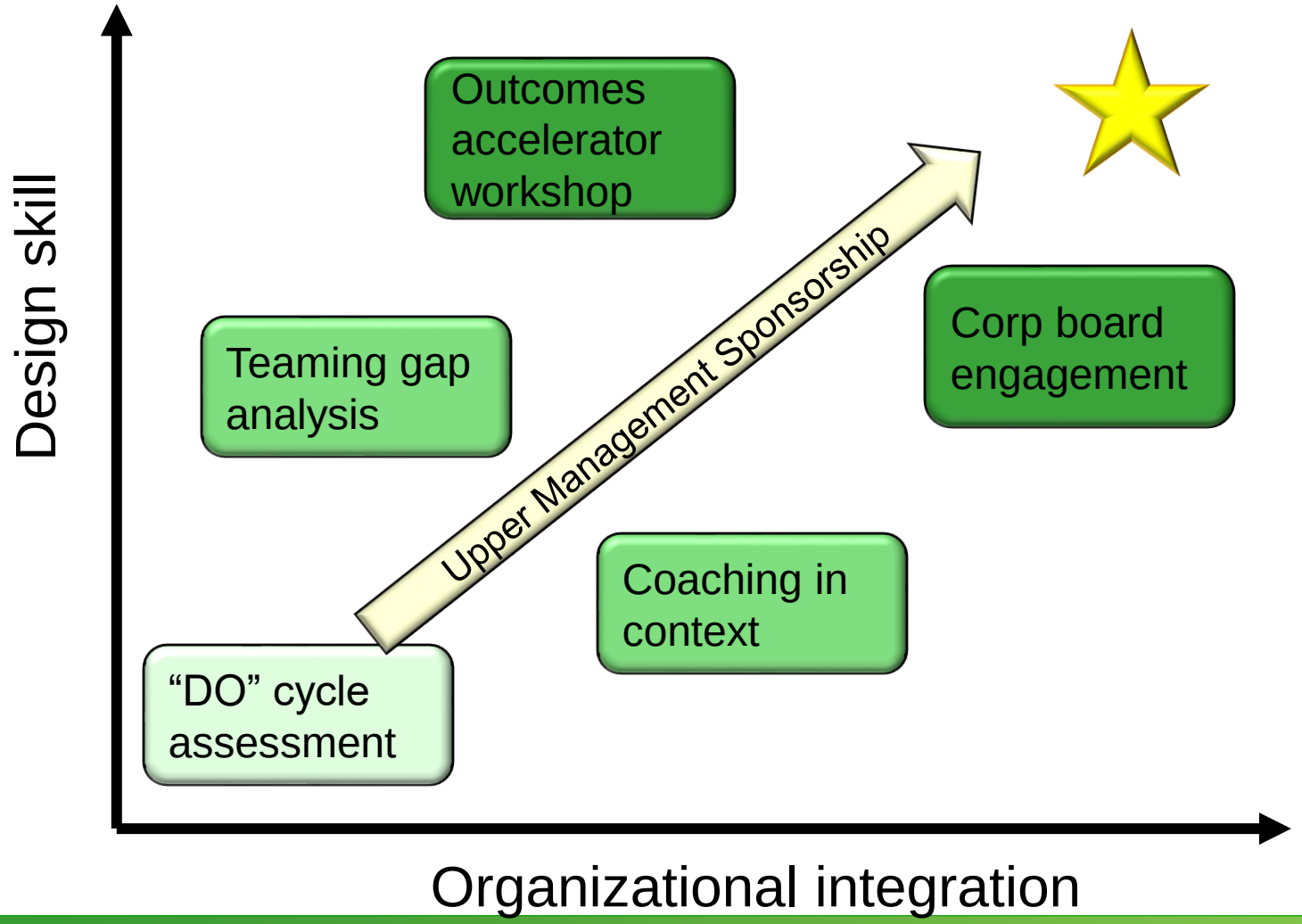
Merle Crawford

Karl Weick

Noel Tichy

MICHIGAN ROSS

Steps to improving design maturity and outcomes



Outthinking and outmaneuvering adversaries…

Apply Design thinking principles

- **Challenging** prevailing view and "trusted sources"
- Designing **teams** that can see broadly, think clearly and take action to solve problems
- **Reevaluating** math, method and tools

Join the ThinkDesignCyber community today!

https://www.thinkdesigncyber.com/contact

THANK YOU!

Brian <at> valuebridgeadvisors.com