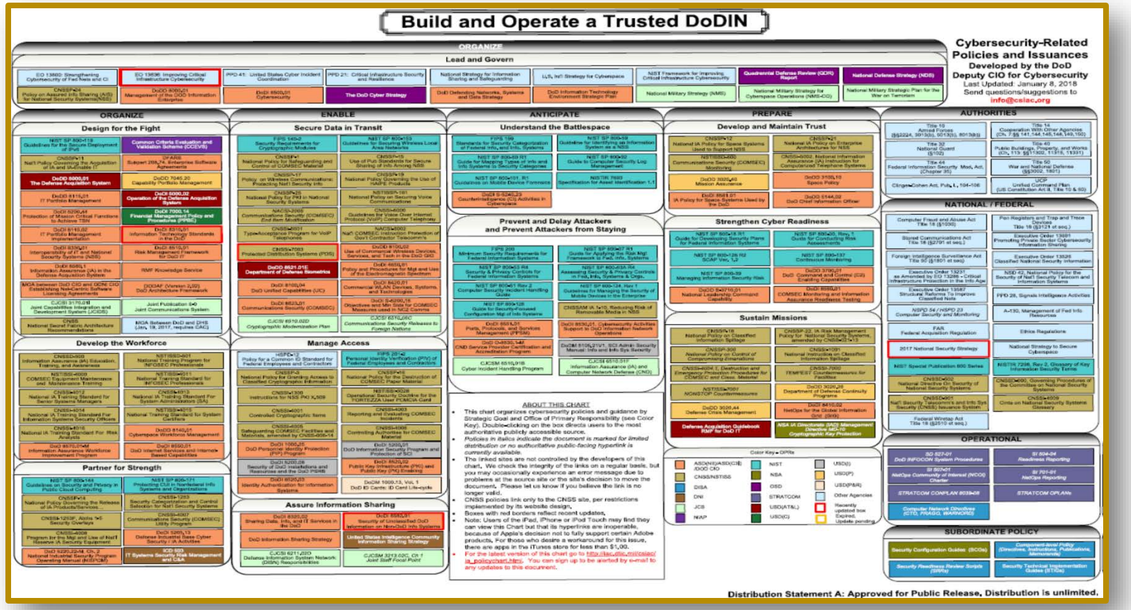
Cybersecurity: Converting Shock into Action

Paul Shaw
Professor, Cybersecurity
Defense Acquisition University

Rob Tremaine
Associate Dean for Outreach
& Mission Assistance
DAU West Region

Research Focus: Defense Acquisition Workforce



Active AT&L Workforce Count 2018	4th Estate	Air Force	Army	Navy	Total
Auditing	4,120	0	0	0	4,120
Business - Cost Estimating	80	498	257	564	1,399
Business - Financial Mgmt	528	2,080	1,737	2,203	6,548
Contracting	7,939	8,289	7,943	6,515	30,686
Engineering	2,125	9,178	9,084	22,615	43,002
Facilities Engineering	91	573	4,207	5,604	10,475
Industrial/Contract Property Mgmt	268	18	47	67	400
Information Technology	1,038	1,334	1,735	3,179	7,286
Life Cycle Logistics	3,118	3,301	7,011	6,470	19,900
Production, Quality and Manufacturing	5,281	431	1,395	3,449	10,556
Program Management	1,828	5,892	3,305	6,223	17,248
Program System Engineer	8	0	0	0	8
Purchasing	520	62	389	439	1,410
Science and Technology Manager	120	2,668	469	519	3,776
Test and Evaluation	370	3,170	1,860	3,357	8,757
Unknown	7	1	8	24	40
Totals	27,441	37,495	39,447	61,228	165,611

Source: DataMart as of 31 Dec 2017

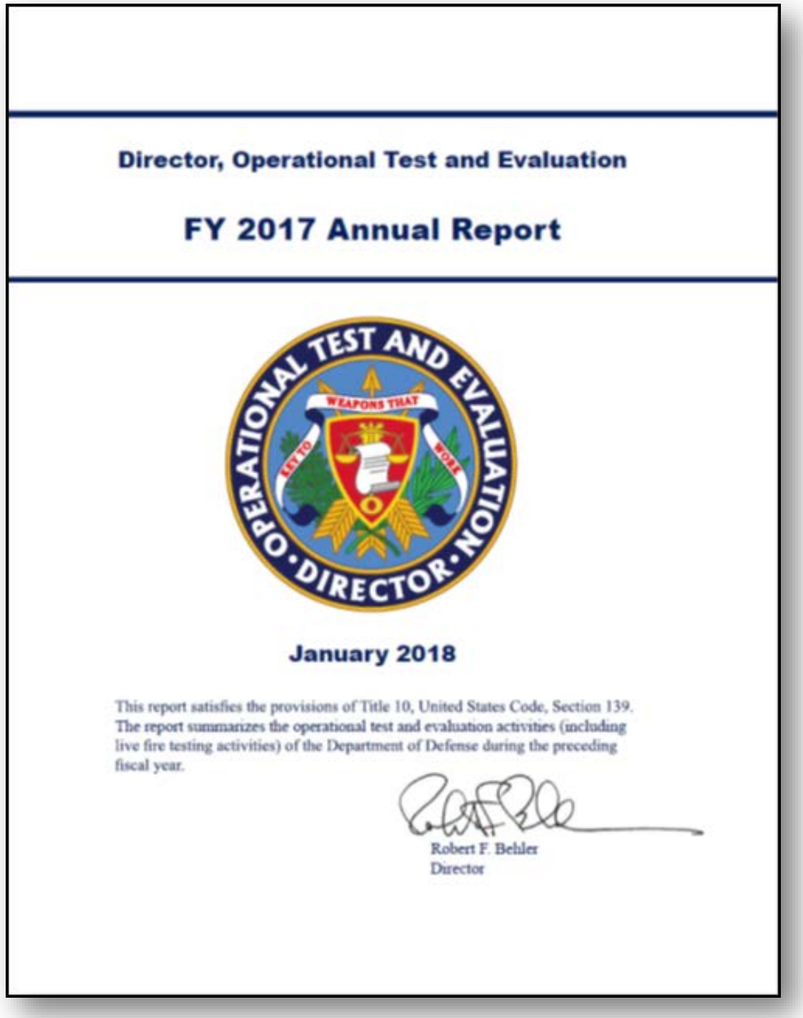
Environmental Scan—Inherent Security Holes and Malicious Actors

The Public domain…and threat of COTs

- **Meltdown** and **Spectre** vulnerabilities: for years chipmakers have taken steps to prioritize performance and speed at the expense of security.
- **Heartbleed** and **Shellshock** demonstrated the challenges with wide-scale and real-time patching, but these issues had been dormant for decades and proved the impossibility of issuing replacements.
- **Shadow Brokers** breached the spy tools of the elite NSA-linked operation known as the Equation Group, and offered a sample of alleged stolen NSA data and attempted to auction off a bigger trove. They also stole NASA's Windows exploit known as EternalBlue to infect targets in two high-profile ransomware attacks.
- **WannaCry,** a ransomware strain spread around the world, walloping hundreds of thousands of targets, including public utilities and large corporations. It temporarily crippled National Health Service hospitals and facilities in the United Kingdom, hobbling emergency rooms, delaying vital medical procedures, and creating chaos for many British patients.
- **Petya/NotPetya/Nyetya/Goldeneye**, a more advanced variation of **Wannacry**, it disrupted utilities like power companies, airports, public transit, and the central bank, just the latest in a series of cyber assaults against the Ukraine.
- **Wikileaks CIA Vault 7** detailed individual tools for things like using Wi-Fi signals to track a device's location, and persistently surveilling MACs by controlling the fundamental layer of code that coordinates hardware and software.

Background

Current state of the DoD—Maneuver Undetected



Director, Operational Test and Evaluation

FY 2017 Annual Report

January 2018

This report satisfies the provisions of Title 10, United States Code, Section 139. The report summarizes the operational test and evaluation activities (including live fire testing activities) of the Department of Defense during the preceding fiscal year.

Robert F. Behler
Director

- "DOD missions and systems remain at risk from adversarial cyber operations…"
- "Assessments during Combatant Command training exercises confirmed that DOD cyber defenses are improving, but not enough to stop adversarial teams from penetrating defenses, operating undetected, and degrading missions…"
- "Tests and assessments continue to identify previously undetected vulnerabilities…"
- "Despite improvements in network defenses, almost every assessment and test demonstrated that DOD network defenses still contain exploitable problems…"

Framing Assumptions

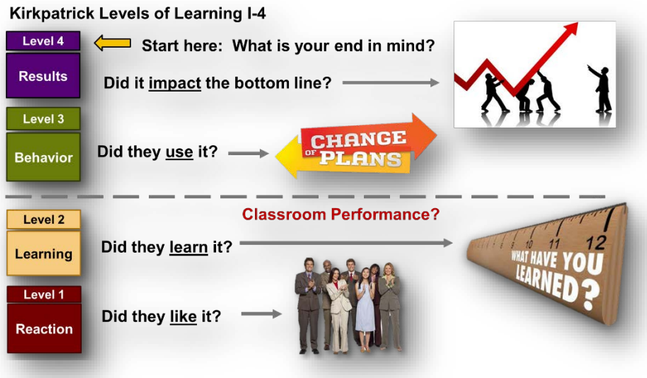
- Cybersecurity is a decaying function— static cybersecurity assures a declining security posture
- NO SYSTEM is without malware — every system has an inherent vulnerability that is just waiting to be exploited
- People over rely on the technology for security and don't sufficiently consider the people and process components
- The seemingly most secure system often fails to acknowledge that it can be affected by a higher level threat (e.g. any system can be misconfigured)
- Cybersecurity Policy stands at the Outcome level; Acquisition guidance and implementation below the outcome level is subjective (i.e. "Design for the Fight" is an example of an Outcome Level)
- Most programs undershoot "adequate security" —most operate under a false sense of security until they discover they did not sufficiently manage realistic and likely operational risks
- DoD may not be proactive enough to exploit its own systems to withstand advanced threats
  - **Example**. Netflix: champion of self-imposed chaos. They developed Chaos Monkey in 2011 to test the resiliency of their IT infrastructure. The tool works by intentionally disabling computers in Netflix's production network to test how remaining systems respond to outages.

Problem Statement

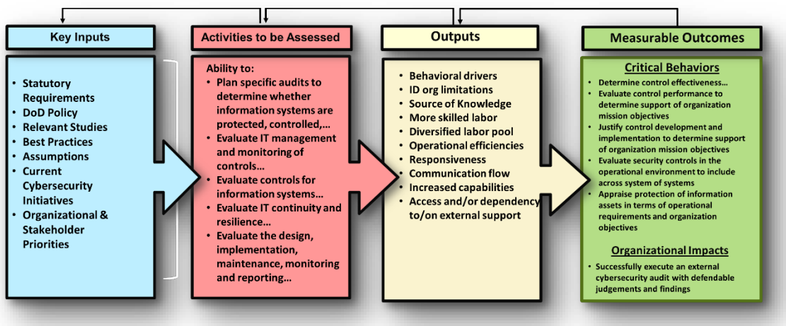
Problem Statement: This research study starts with a discussion on policy/directives and then explores the efficacy of DoD's cybersecurity strategy and associated actions taken to date—all intended to safeguard the efficacy of DoD systems.

Goal: Develop a Cybersecurity approach customized for DoD Acquisition organizations that characterizes what it takes to implement a robust, effective and sustainable Cybersecurity Program

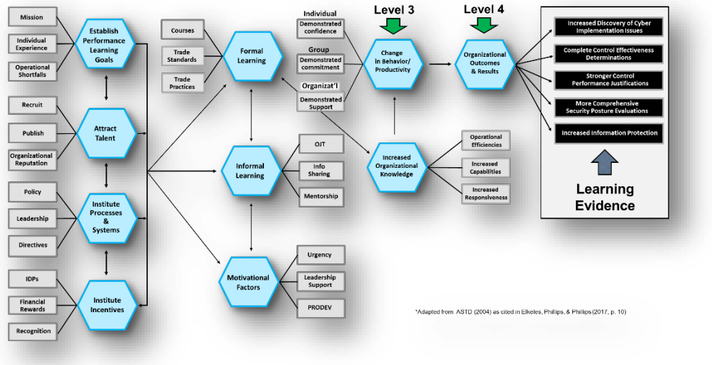
Kirkpatrick Learning Levels

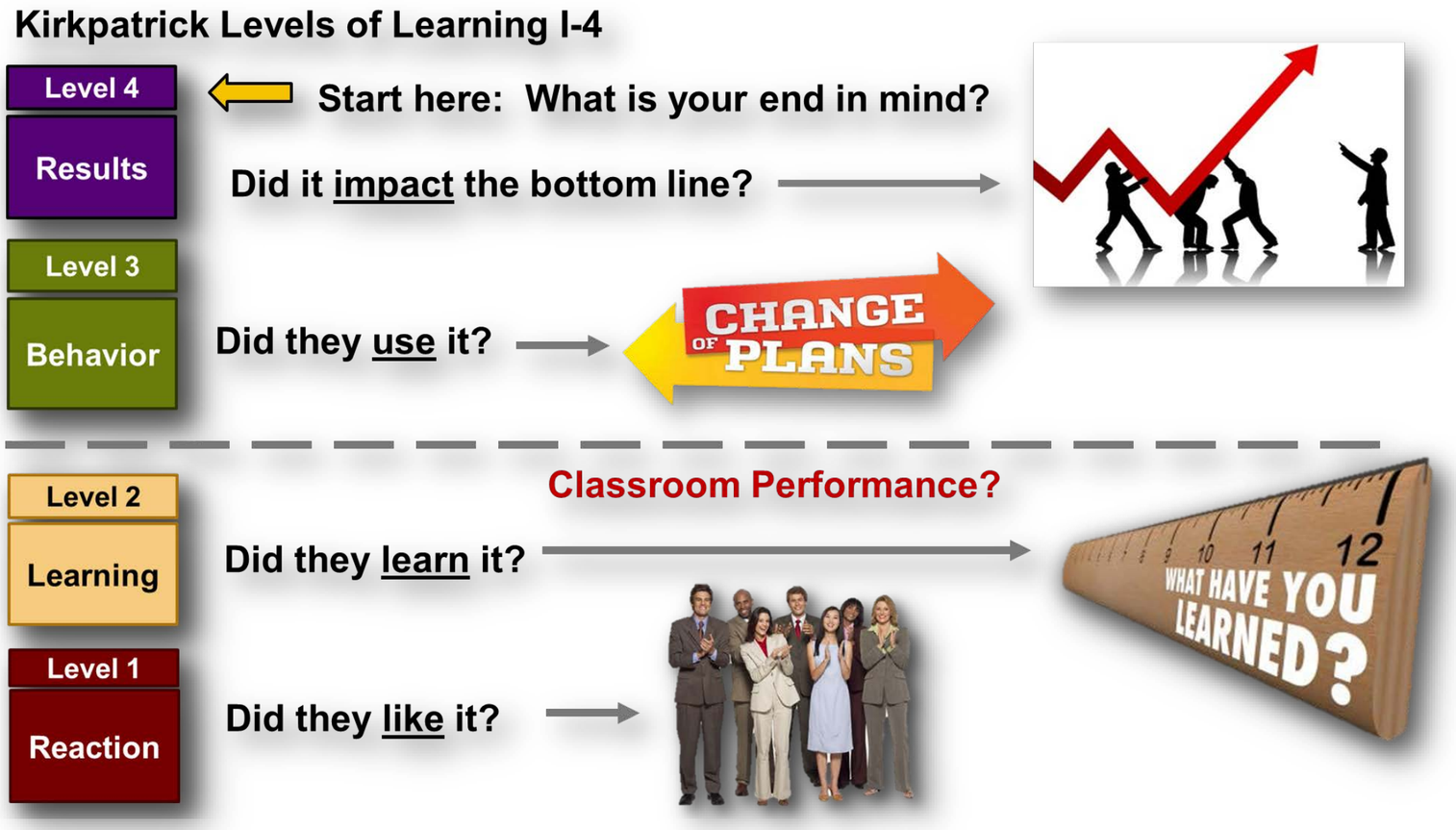


Logic Model



Learning & Performance Value Chain





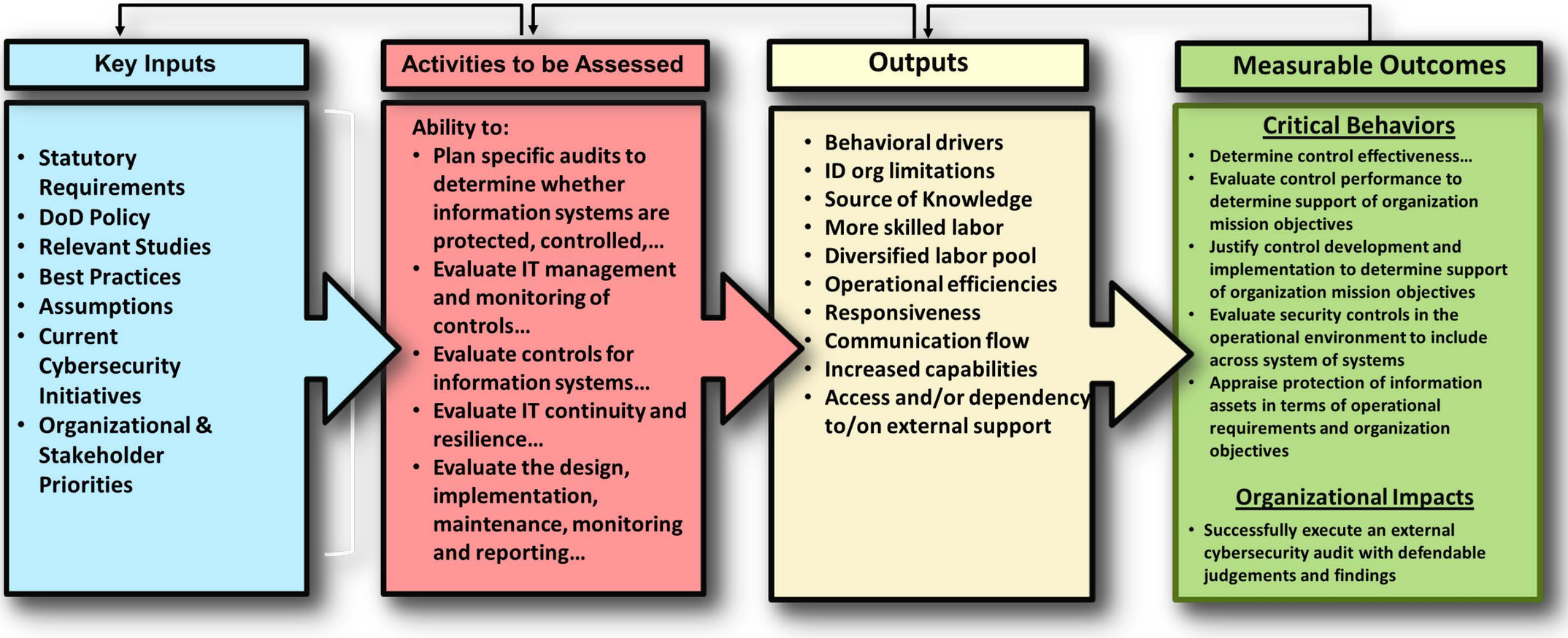
New World Kirkpatrick® Model: Kirkpatrick learning Levels. Adapted from "Four Levels of Training and Evaluation."

Levels 3 and 4

- The data substantiates the training effectiveness
- Measures on-the-job performance and accompanying behavioral changes due to training and reinforcement
- Affords the evidence that organizations would expect to see from their investment

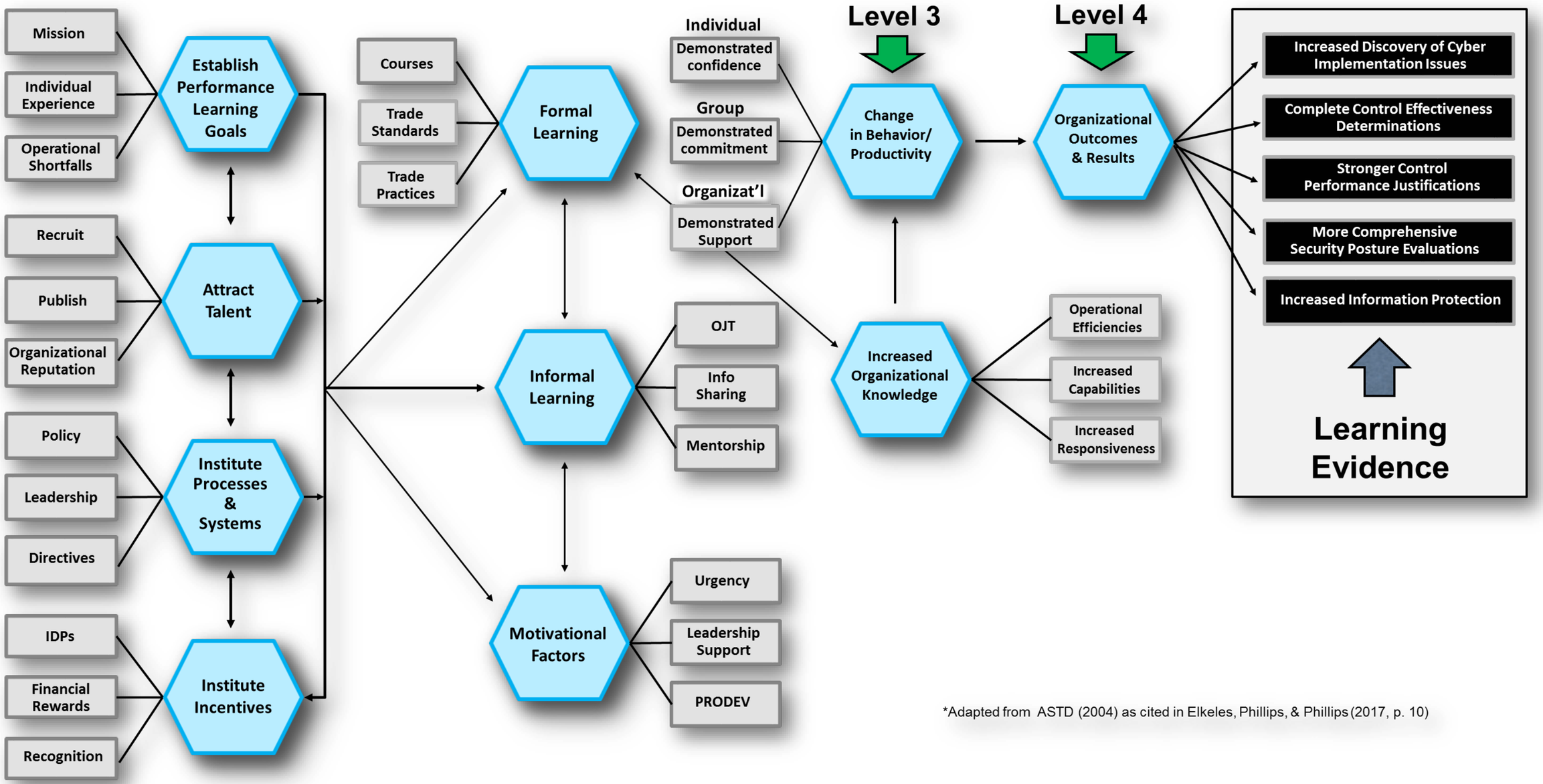
Training effectiveness data is key to demonstrating the value that the training has contributed to the organization…and that stakeholders find valuable."

A Logic Model in Action for CyberSecurity*



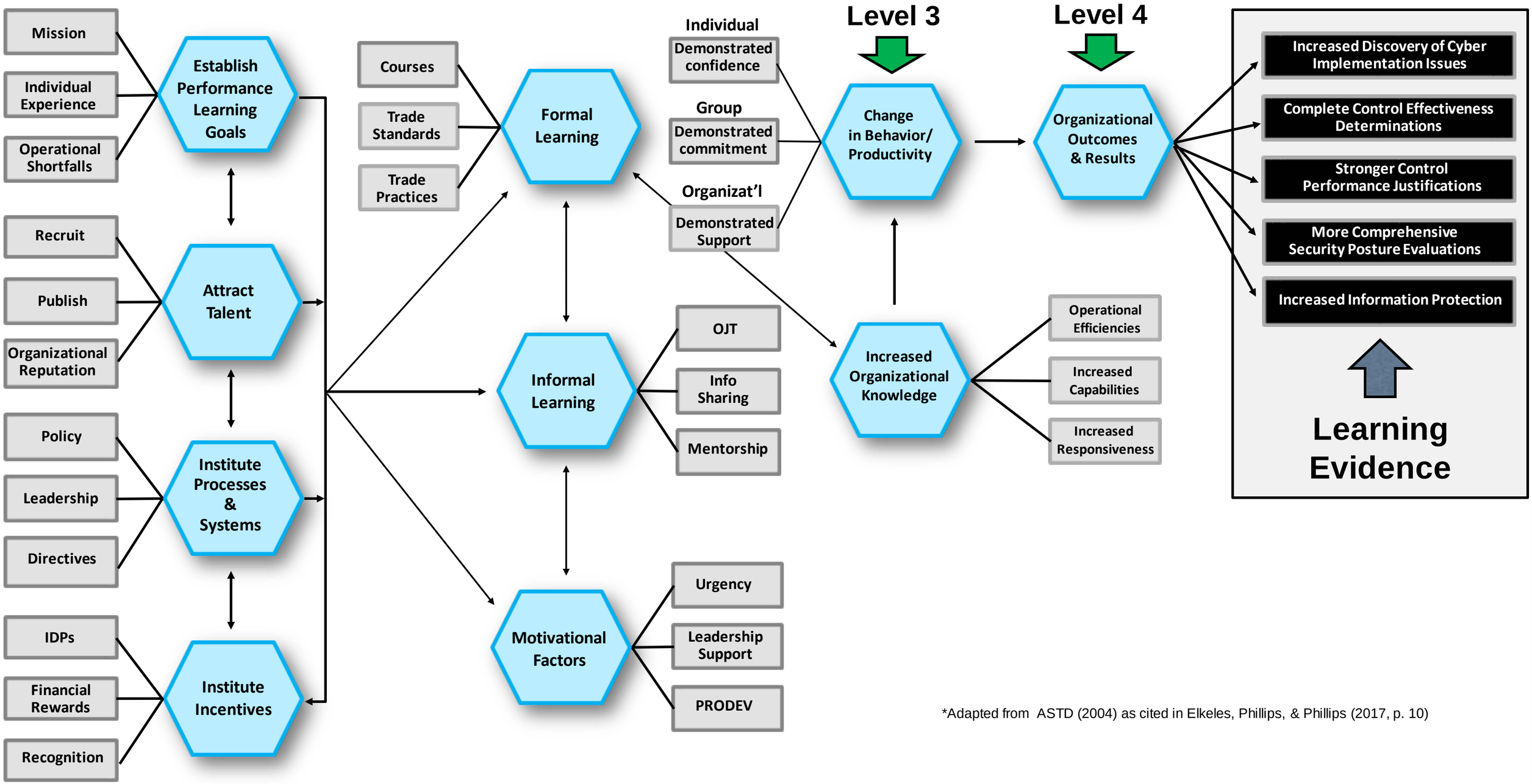
*Addresses: What is Important? …What is Broken?… What is Critical?… What is no longer useful?…What needs to be measured?…What's the evidence that the investment provided a return?…

Research Tools



*Adapted from ASTD (2004) as cited in Elkeles, Phillips, & Phillips (2017, p. 10)

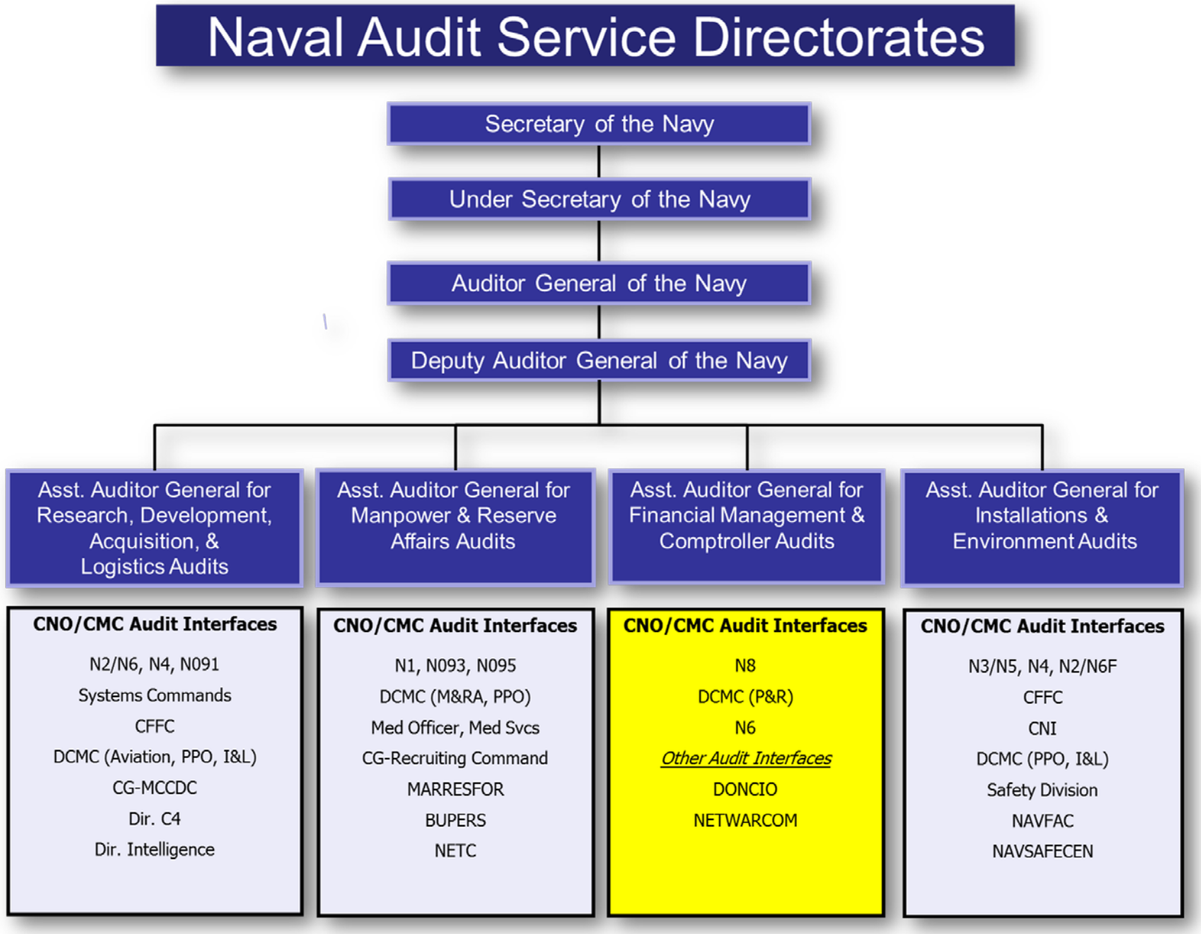
Cybersecurity Performance Learning Development Value Chain



*Adapted from ASTD (2004) as cited in Elkeles, Phillips, & Phillips (2017, p. 10)

Participants Details

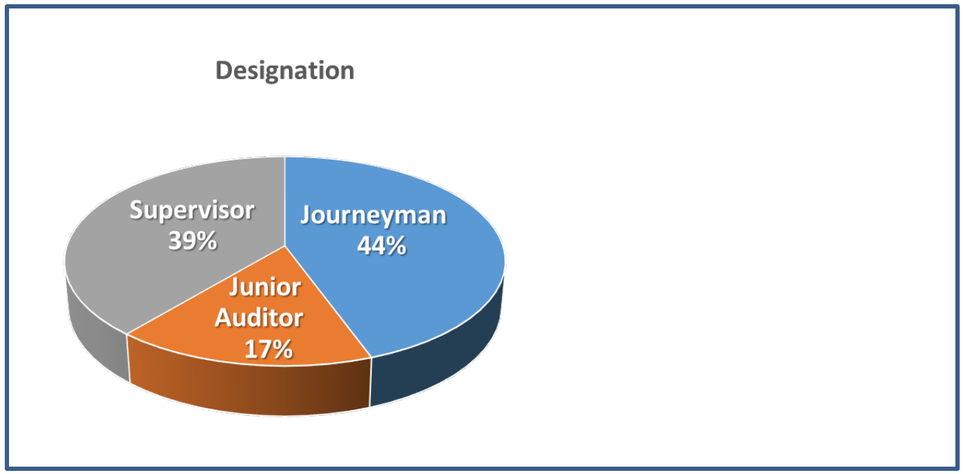
Case Study

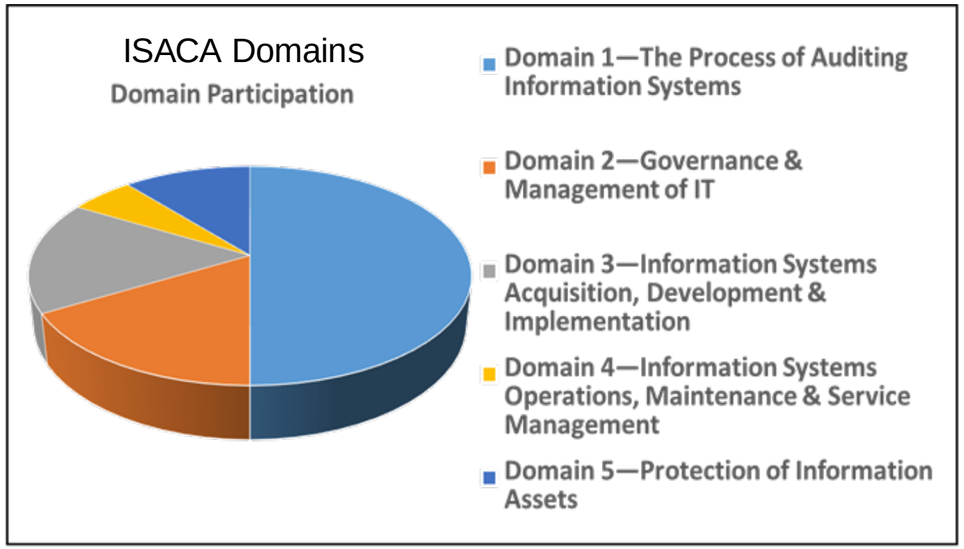


Workshop Expectations

- Directorate welcomed a way to confirm critical cybersecurity behaviors expected of them in the prosecution of their all audit responsibilities
- Learning had to reinforce execution of tasks and realization of behavior
- Develop a learning strategy to monitor pre-audit engagements that better scopes audit objectives
- End-of-workshop survey would evaluate their confidence to execute the critical behaviors

Learning objectives cut across the five domains that constituted the team's responsibilities





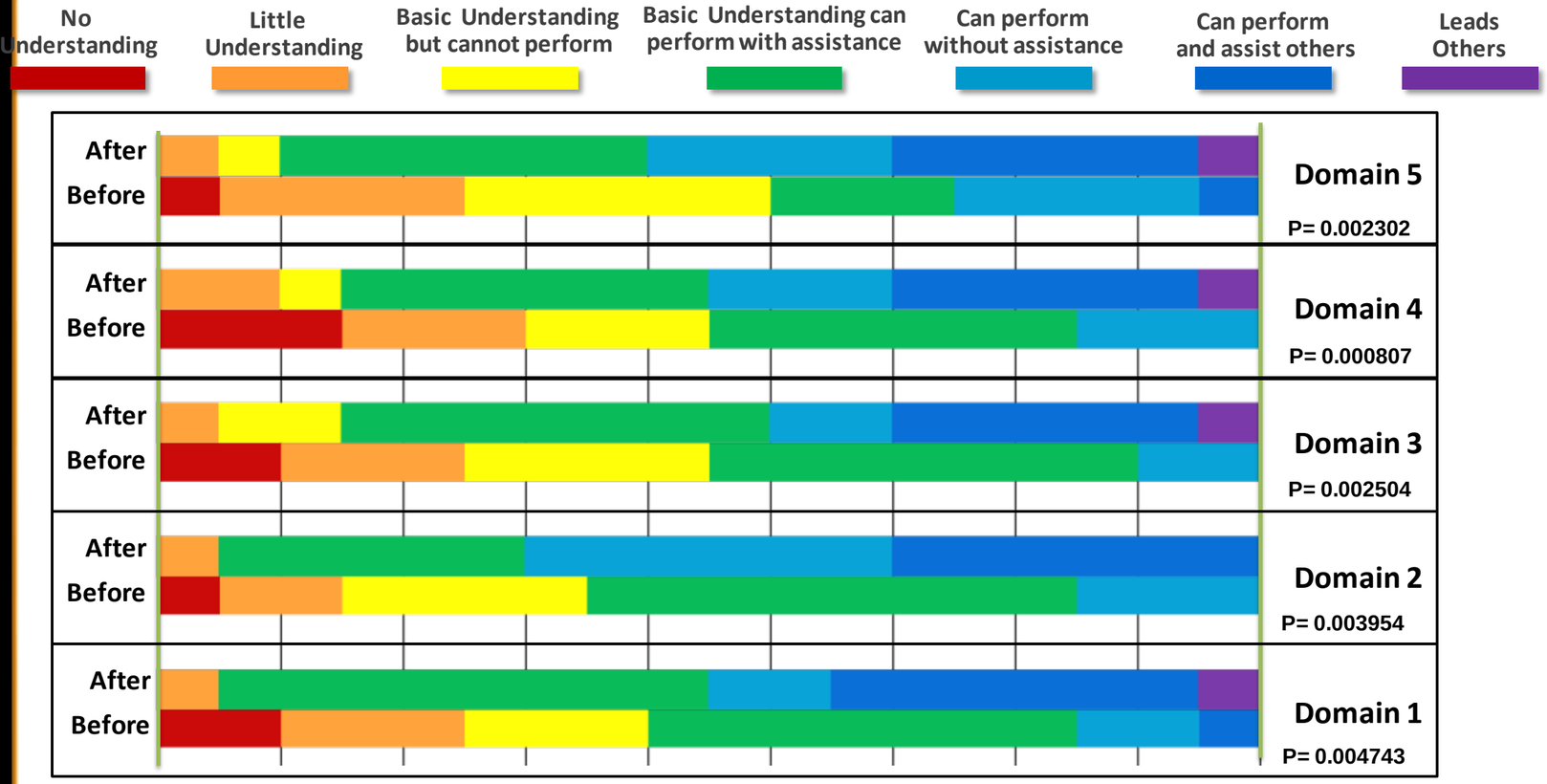
Workplace Behaviors

- D1: Determine the effectiveness of security controls in support of risk management
- D2: Evaluate the performance of security controls in support of organizational mission assurance objectives
- D3: Justify security control development and implementation in support of organization mission assurance objectives
- D4: Evaluate security controls at system interfaces and that span system of systems
- D5: Appraise protection of information assets in context of a threat level for protected information assets

Quantitative Results

Part 1: Initial Findings

Cybersecurity Learning – Results by *ISACA Domain



Note: Using an Anova Test for a comparison of the Means & Standard Deviations of the "Before" & "After" values of Attitudes on the Behaviors by Domain.

In all 5 domains, we can reject the Null Hypothesis that "the training had no effect on the Auditor's attitude for the behaviors." We accept the Alternate Hypothesis, "the training has a statistically significant effect on attitudes towards the behaviors."

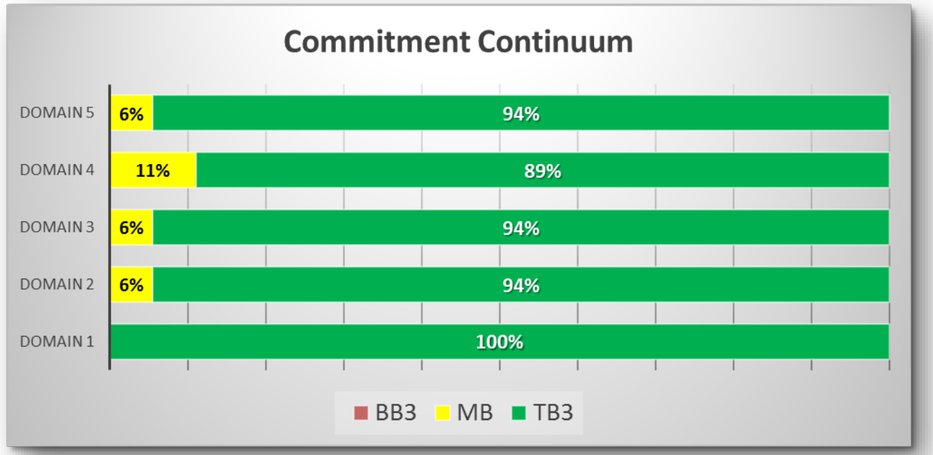
***ISACA (Information Systems Audit and Control Association—110,000 strong in 180 countries)**

Learning Level 2

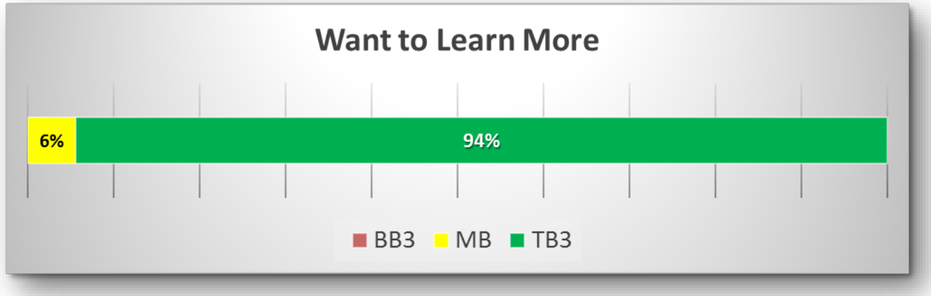
- **Figure summarizes what nineteen respondents had to say about their level II learning levels "before and after" after the workshop.**
- **Noticeable shifts and distinctions from this highly interactive and "hands on" event in each learning category without exceptions.**
- **Domain 2 had the most significant shift where the respondents no longer needed assistance after the workshop.**
- **Domains 1 and 2 virtually eliminated their lack of understanding for any domain afterwards.**

Quantitative Baseline—Will Have a Follow-on

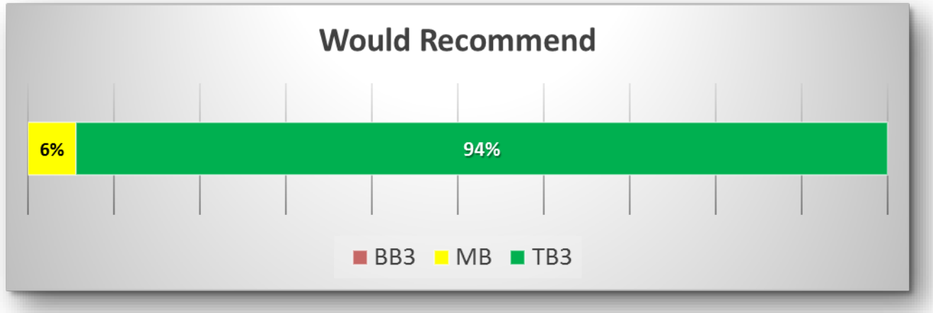
Part 1:
Initial Findings



I am committed to apply what I learned



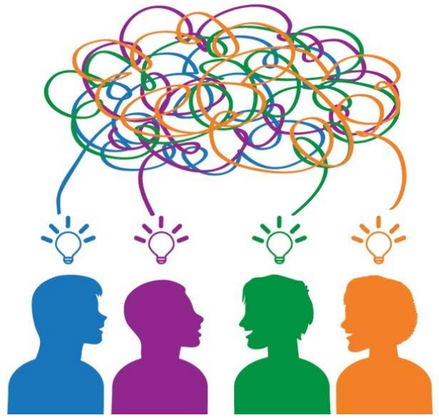
I would like to learn more about other cyber security practices that I can apply on the job.



I recommend this workshop to my co-workers.

Qualitative Comments

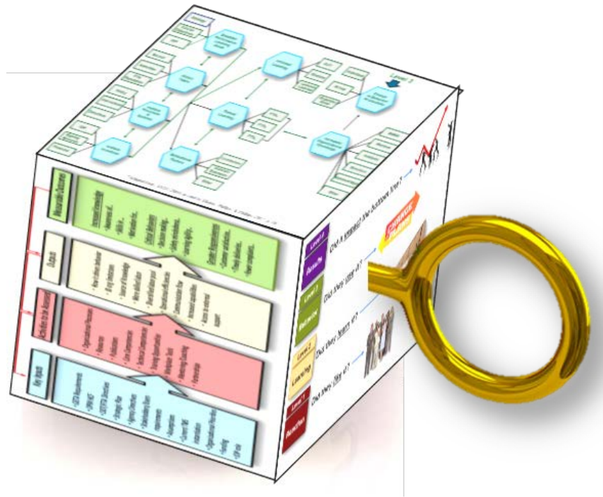
Part 1:
Initial Findings



- We plan to incorporate all the concepts we learned in future audits future cybersecurity audits
- Being able to plan and execute an audit using Cybersecurity and cyber resilience concepts and policies/guidance on a system or process.
- To be able to initiate an audit in Cybersecurity with the training, tools, and material provided in confidence.
- I will more often consider risks concerned with access to any naval systems that are applicable to assigned future audits.
- I plan to work with the audit team to develop potential audit topics that involve Cybersecurity within the Department of Navy.
- Be able to identify potential Cybersecurity internal control weakness regarding people and processes.
- Cybersecurity attack vulnerability minimized.
- I will pursue more knowledge in this area to get a better understanding of “how to.”
- Agencies will be better prepared to tackle cyber obstacles they may have not known existed prior to the audit.
- I think the senior Navy leadership will start seeing our capabilities and request more Cybersecurity audits.

SUMMARY

- Cybersecurity is a complex, dynamic and ambiguous domain
- Incidental learning is not conducive to cybersecurity
- A lot of good work has been done on core knowledge and core tasks of Cybersecurity (e.g. NIST SP 800-181) although it hasn't been translated into critical behaviors
- The attitude component of Knowledge, Skills, and Attitude (KSA) is tightly coupled to the achievement of cybersecurity critical behaviors
- Formal (and tailored) training is only the starting point. What the workforce applies in the workplace as a result of the learning is the most important aspect for achieving the outcome—and it's up to the organization to monitor, encourage and enforce it!



There's Hope

Extra, extra
Read all about it

Win-T failed OT Adversarial Assessment Twice in last couple of years—directed by Mr. Kendall (USD (AT&L)) to change approach before next OT.

…and they Changed their Approach for Increment 2:

- Program Office went to agile programming, with incremental capability drops
- Cybersecurity became part of overall engineering, instead of seeking a separate cybersecurity solution
- Independent and frequent testing for all capability drops
- Assumption of breech (assume compromise). Lowest level of trust between their system components and other systems
- Development of threat models, with over 10 million simulations of threat models on their system.
- Acclimated both Resource Sponsor and Milestone Decision Authority on WIN-T's approach

"WIN-T Increment 2 is survivable. WIN-T Increment 2 demonstrated a robust cyber network defense to protect against an operationally realistic cyber threat opposing force." (DOT&E, 2018, p. 130)