Cybersecurity: Converting Shock into Action Part 2

Paul Shaw
Professor, Cybersecurity
Defense Acquisition University

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

THE WALL STREET JOURNAL.

U.S. Edition ▾ | March 13, 2019 | Print Edition | Video

Navy, Industry Partners Are 'Under Cyber Siege' by Chinese Hackers, Review Asserts

Hacking threatens U.S.'s standing as world's leading military power, study says

SUMMARY

DEPARTMENT OF DEFENSE

CYBER STRATEGY

2018

STRATEGIC COMPETITION IN CYBERSPACE

The United States' strategic competitors are conducting cyber-enabled campaigns to erode U.S. military advantages, threaten our infrastructure, and reduce our economic prosperity. The Department must respond to these activities by exposing, disrupting, and degrading cyber activity threatening U.S. interests, strengthening the cybersecurity and resilience of key potential targets, and working closely with other departments and agencies, as well as with our allies and partners.

Background

Current state of the DoD—Cyber Shock

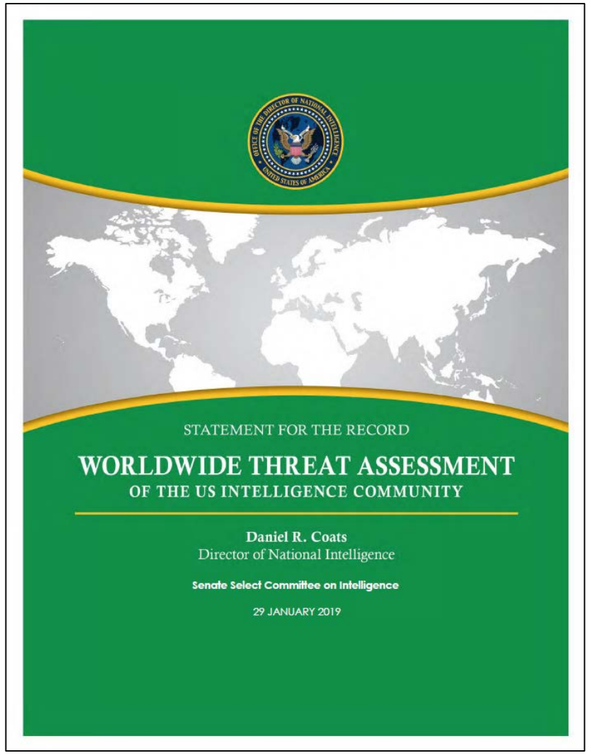
THE SECRETARY OF THE NAVY
WASHINGTON DC 20350-1000

October 12, 2018

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Cybersecurity Review

Securing the Navy's Cyberspace domain is one of my highest priorities and requires the active engagement of our entire enterprise. Our complex, interconnected, global networks are critical to our operational success and provide us with tremendous military advantage. However, that reliance also makes us a target for disruptive and damaging attacks. Attacks on our networks are not new, but attempts to steal critical information are increasing in both severity and sophistication. We must act decisively to fully understand both the nature of these attacks and how to prevent further loss of vital military information.



THE WALL STREET JOURNAL.

U.S. Edition ▾ | March 13, 2019 | Print Edition | Video

Navy, Industry Partners Are 'Under Cyber Siege' by Chinese Hackers, Review Asserts

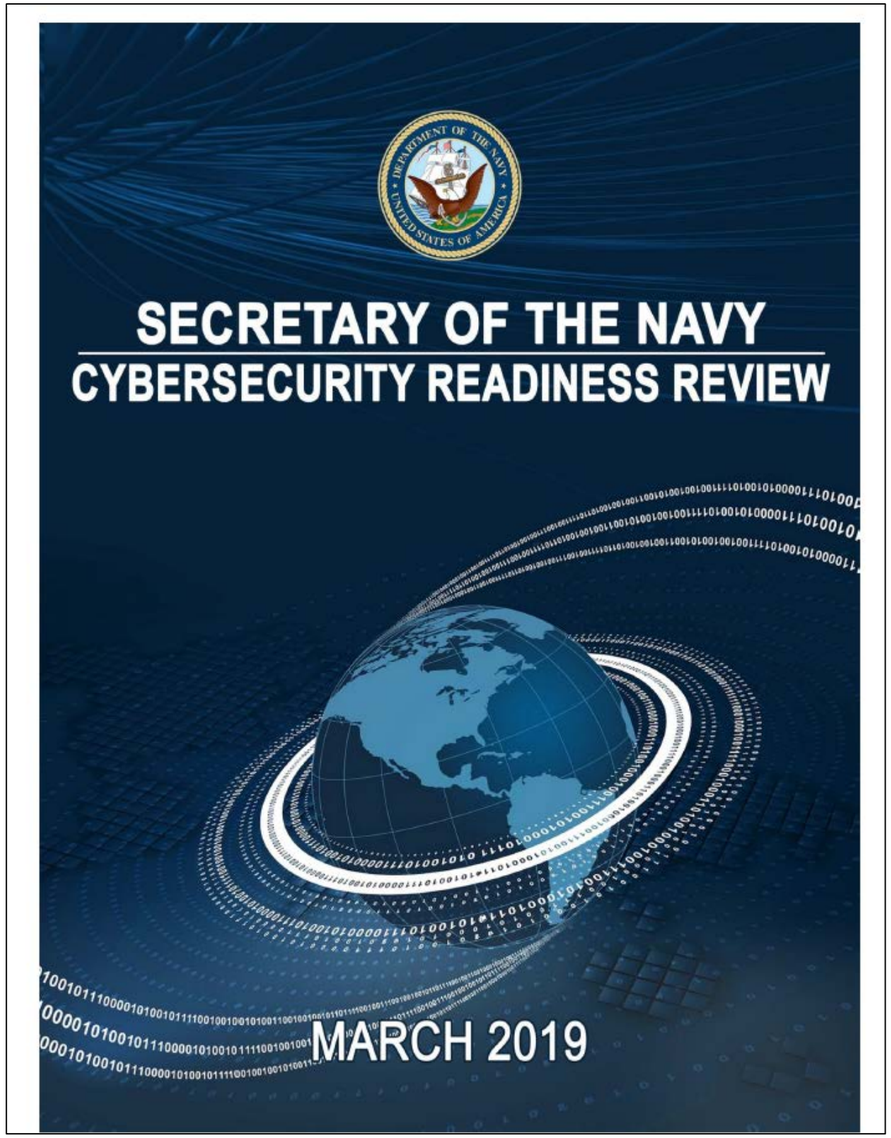
Hacking threatens U.S.'s standing as world's leading military power, study says

"Our adversaries and strategic competitors will <u>increasingly use cyber capabilities</u>—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners." (p. 5)

Background

Environmental Scan—DoN Readiness

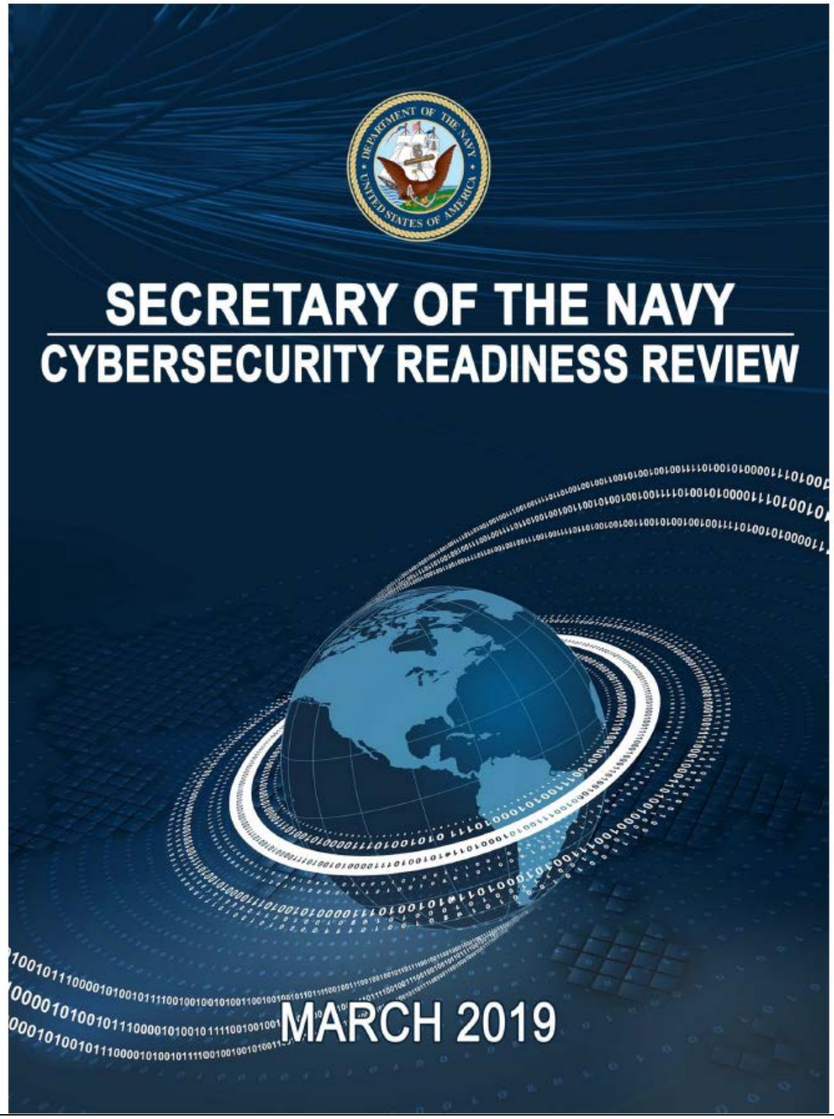
"To restate, the DON culture, processes, structure, and resources are ill-suited for this new era. The culture is characterized by a lack of understanding and appreciation of the threats, and inability to anticipate them, and a responsive checklist behavior that values compliance over outcomes, antiquated processes and governance structures that are late to respond to dynamic threats, and an enterprise whose resources are consumed by force structure and platforms that deprive the information systems and capabilities required for warfighting and defense in this environment. The net-net is that the DON is preparing to fight tomorrow's kinetic war, which may or may not come, while losing the global cyber enabled information war." (p. 7)



Background

Environmental Scan—DoN Readiness

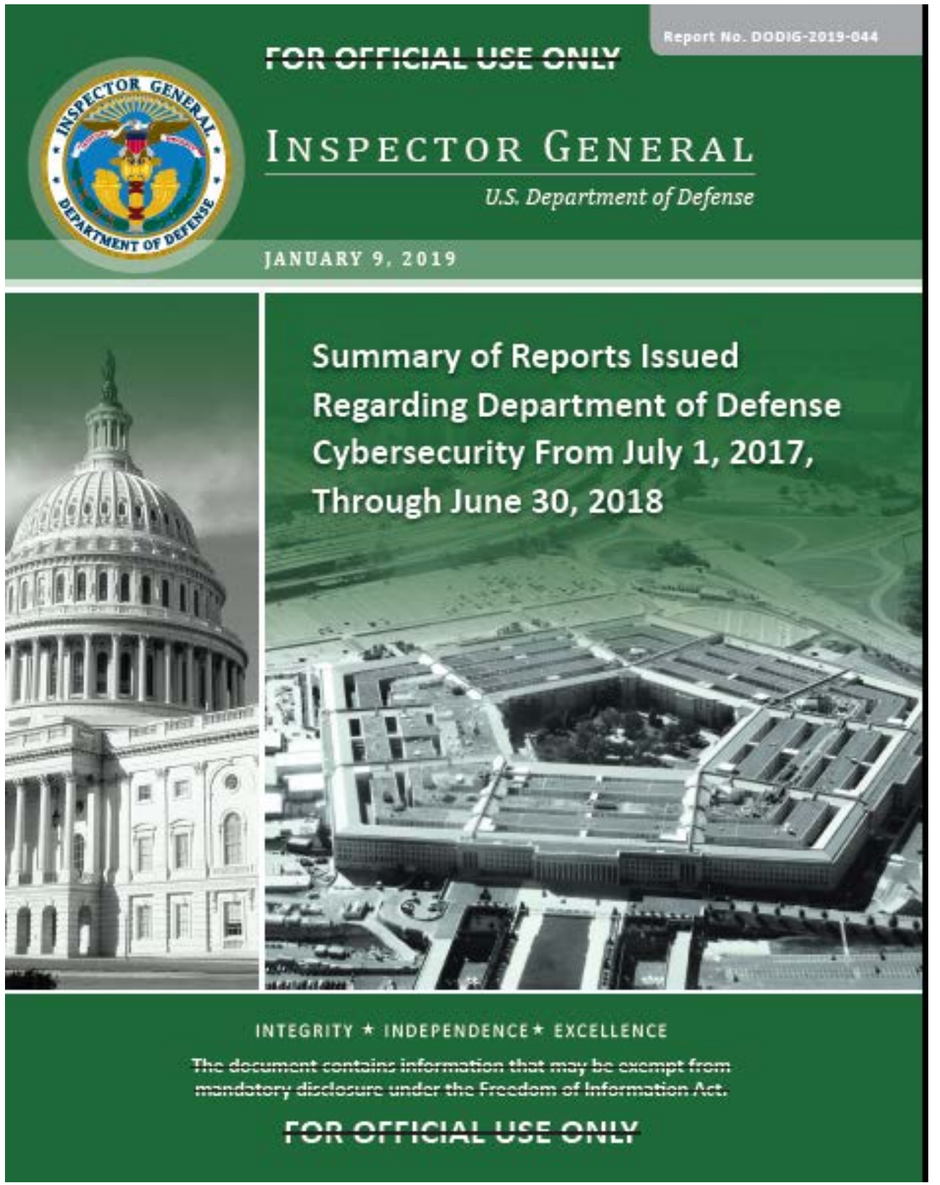
"Whereas the private sector has acknowledged the existentiality of the cyber threat and pivoted aggressively towards technology being core to their business success, the DON has yet to do the same in a meaningful way. … Despite these initiatives, the progress made to date in changing DON's information resilience and cybersecurity culture has been insufficient to bring about meaningful change. A real appreciation of the cyber threat continues to be absent from the fabric of DON culture. Senior leaders occasionally articulate the importance of cybersecurity, but do not fully understand how to convert their words into action, and to making it real." (p. 12)



Environmental Scan—DoD is at Risk

Managing Cybersecurity Risk

"However, the DoD needs to continue focusing on managing cybersecurity risks related to governance, asset management, information protection processes and procedures, identity management and access control, security continuous monitoring, detection processes, and communications. The largest number of weaknesses identified in this year's summary were related to governance, which allows an organization to inform its management of cybersecurity risk through the policies, procedures, and processes to manage and monitor the organizations regulatory, legal, risk, environmental, and operational requirements." (p. ii)



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.

+ 1 New Framing Assumption

Cybersecurity Must be Viewed as a Dilemma Instead of a Problem

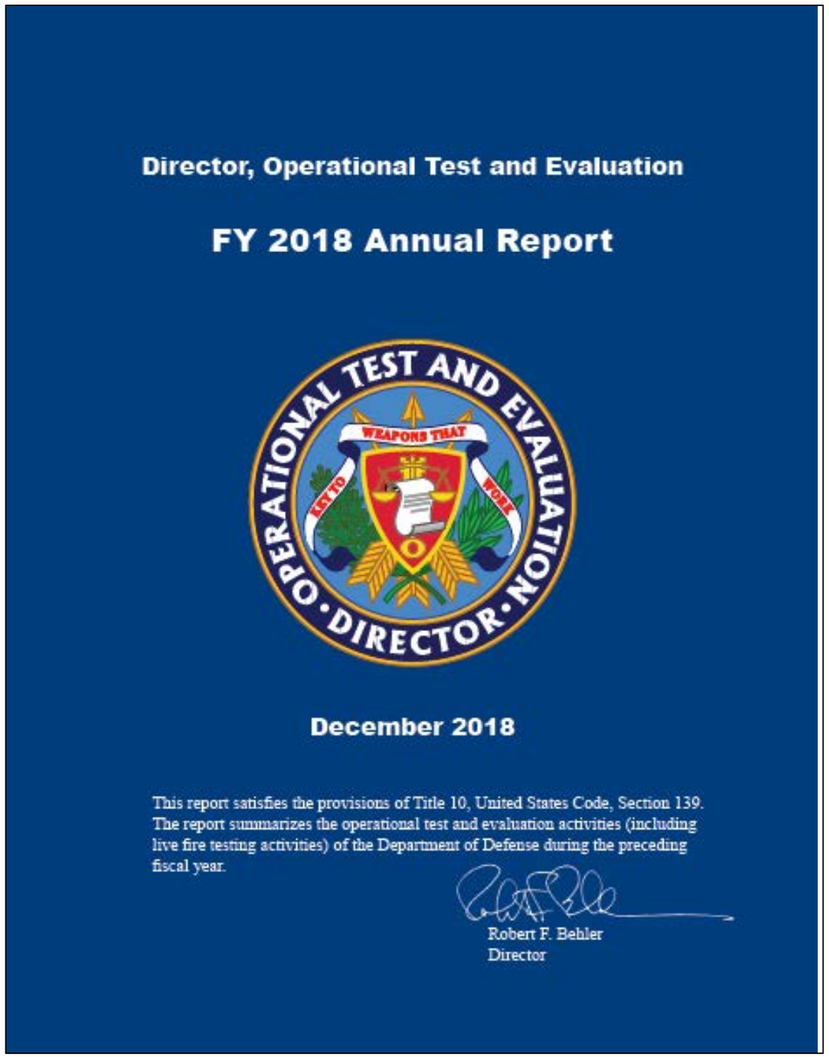
Solving a Problem

Fixing a Broken Car

Managing a Dilemma

Security in the Middle East

Test Data



- "DOD missions and systems remain at risk from adversarial cyber operations. Operational tests continued to discover mission-critical vulnerabilities in acquisition programs,…"
- "Recent advances in cyber technologies indicate that automation – and even artificial intelligence – are beginning to make profound changes to the cyber domain. Warfighters and network defenders must prepare for the onslaught of multi-pronged cyber-attacks across both critical mission systems and the multitude of supporting systems and networks that enable these missions…"
- "DOT&E performed an assessment of a major command which identified several vulnerabilities that could impact mission assurance. Senior leadership at the command self-reported to senior DOD leadership that the command's mission assurance posture was potentially degraded, and made mitigation of these vulnerabilities a top priority."
- "Test and assessments in FY18 again found that low-capability attack techniques too often posed a risk for disrupting operational missions"…

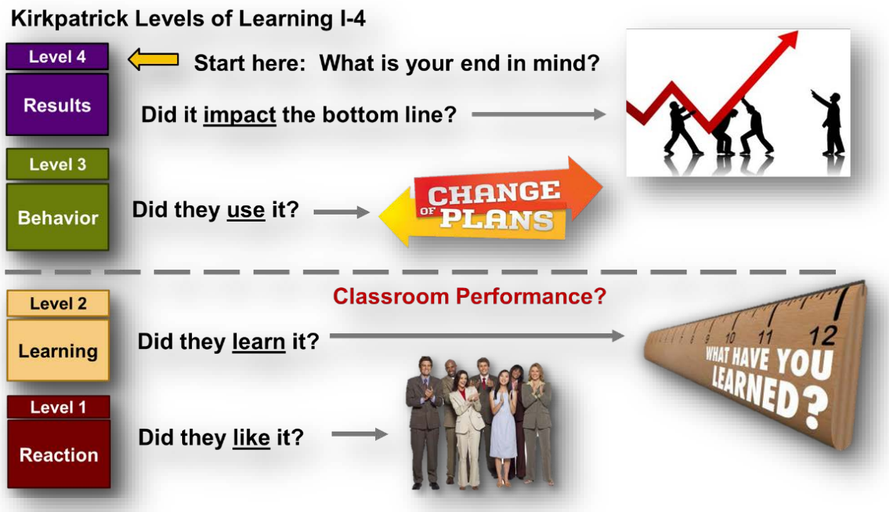
Problem Statement

Problem Statement. What we found: In support of DoD's cybersecurity strategy and policy, Program offices are solving specific instances of their problems and dismissing daily Cybersecurity Risk Management.

Discovery: After conducting over 70+ Cybersecurity workshops with various DoD customers and learning their competencies, it is abundantly clear their behaviors need to change to support security management and security engineering practices in order to achieve Cybersecurity imperatives…or lose to an evolving cyber threat.

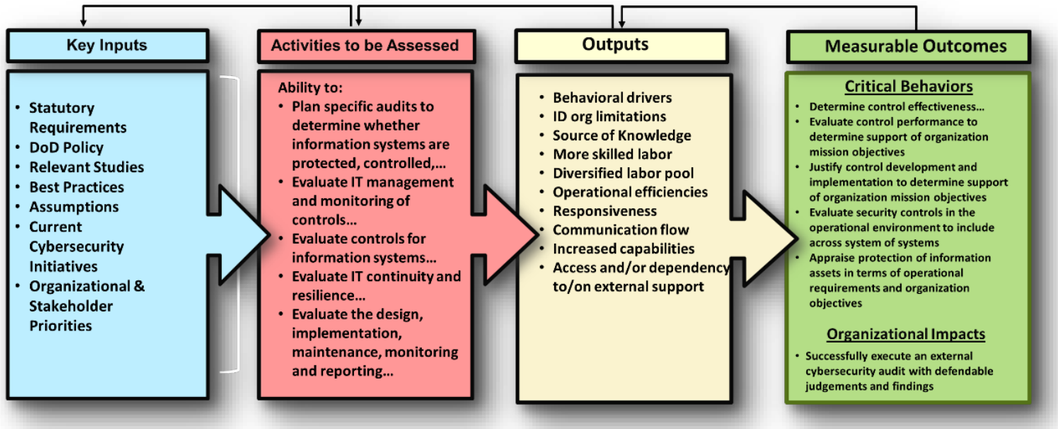
Goal: Implementing a robust, effective, and sustainable Cybersecurity Program requires a long-term and ongoing commitment.

Research Tools

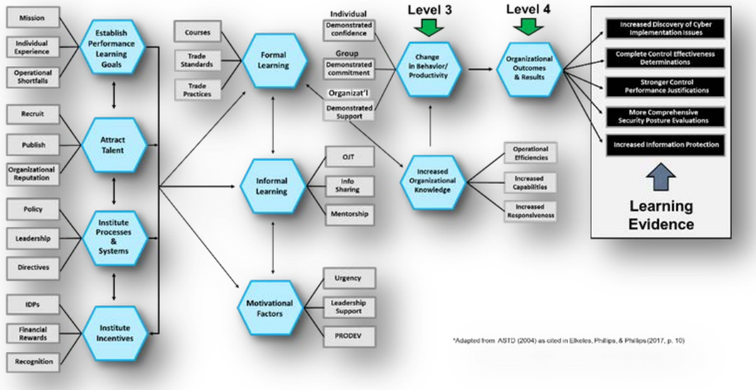


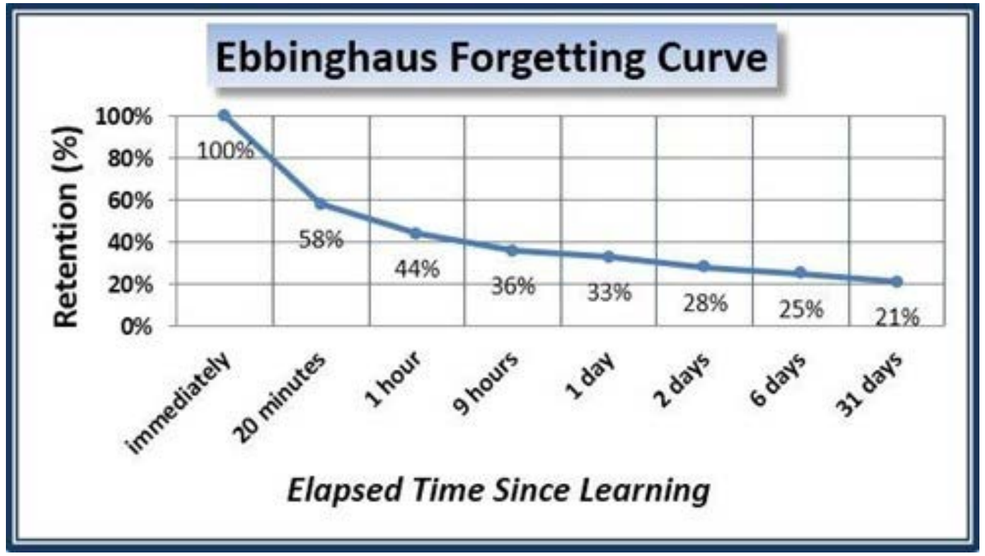
New World Kirkpatrick® Model: Kirkpatrick learning Levels.
Adapted from "Four Levels of Training and Evaluation."

Logic Model

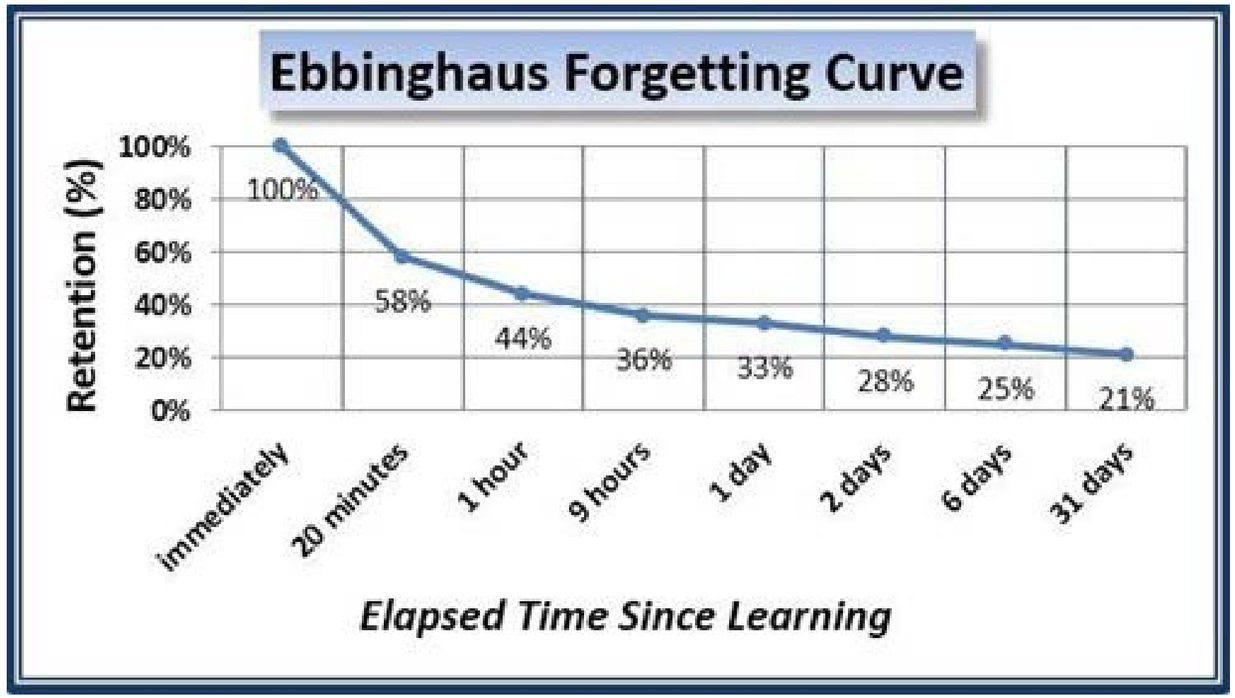


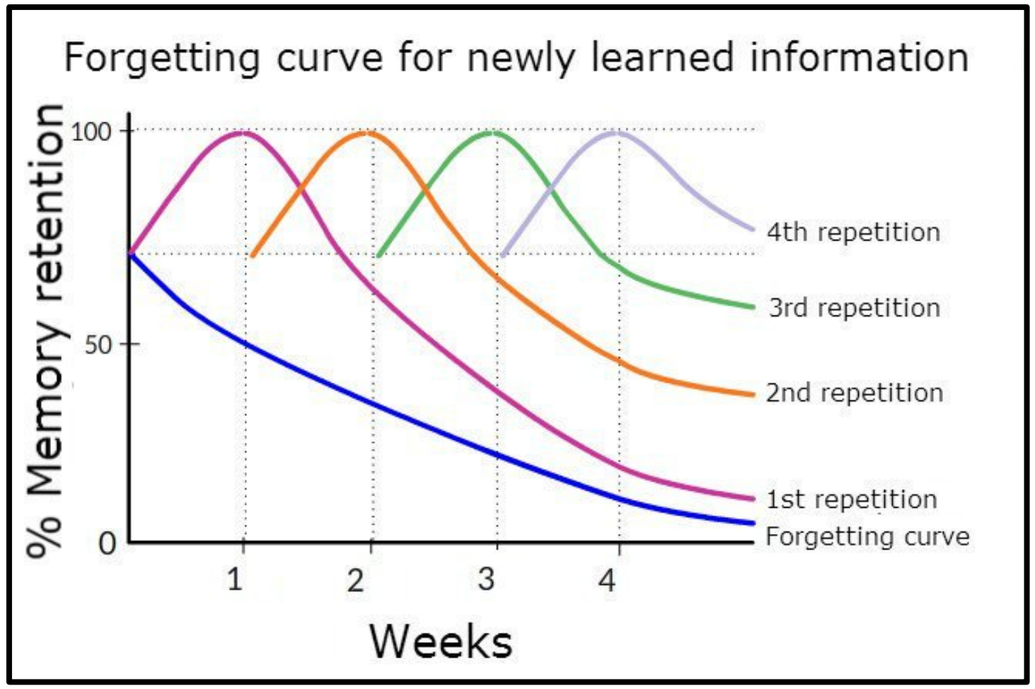
Learning & Performance Value Chain





Herman Ebbinghaus' Forgetting Curve



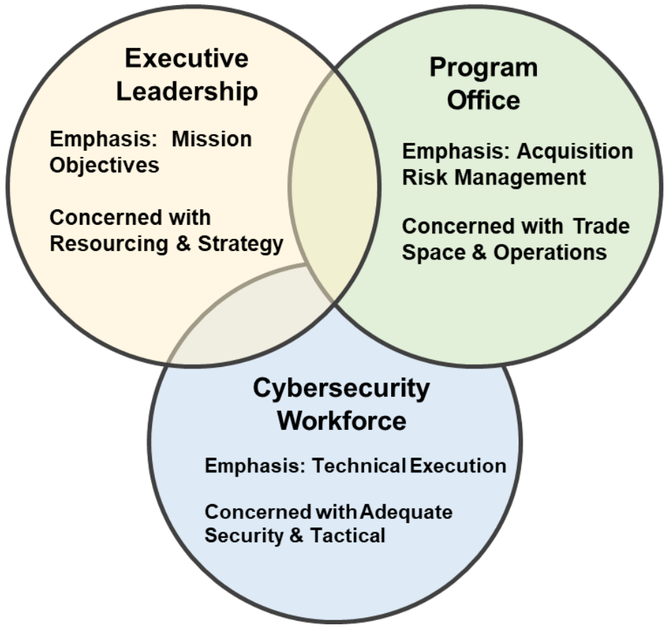


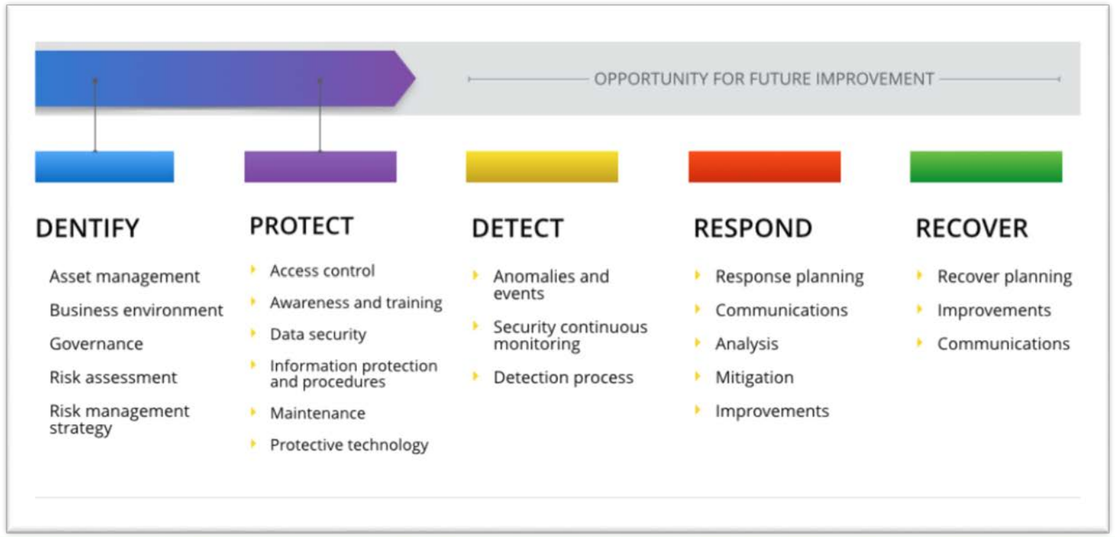
80% of what we learn we forget in 30 days if there is no reinforcement

The more relevant the training, the better the recall: R = e^(-t/s)

Participants Details

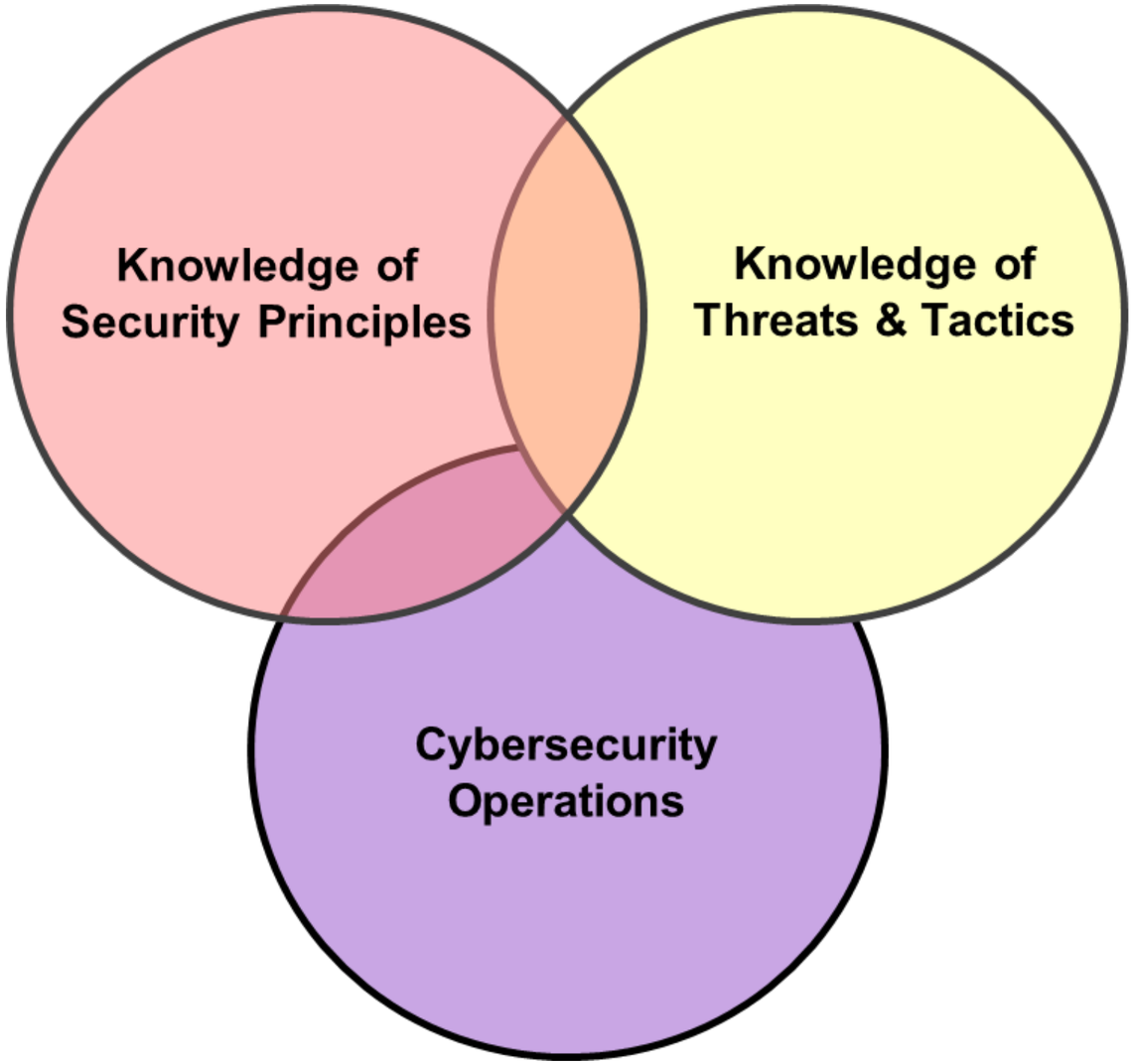
Case Study





Workshop Outcomes

- Determine program cybersecurity requirements and mission objectives
- Employ cybersecurity engineering oversight to assess DoD security posture and cyber hygiene implementation
- Apply best practices in cybersecurity risk management to their projects
- Reinforce behaviors to overcome the Forgetting Curve
- Follow-up after workshops to monitor execution of behaviors and achievement of cybersecurity objectives



Workplace Behaviors

Construct a comprehensive and holistic system view while addressing stakeholder security and risk concerns

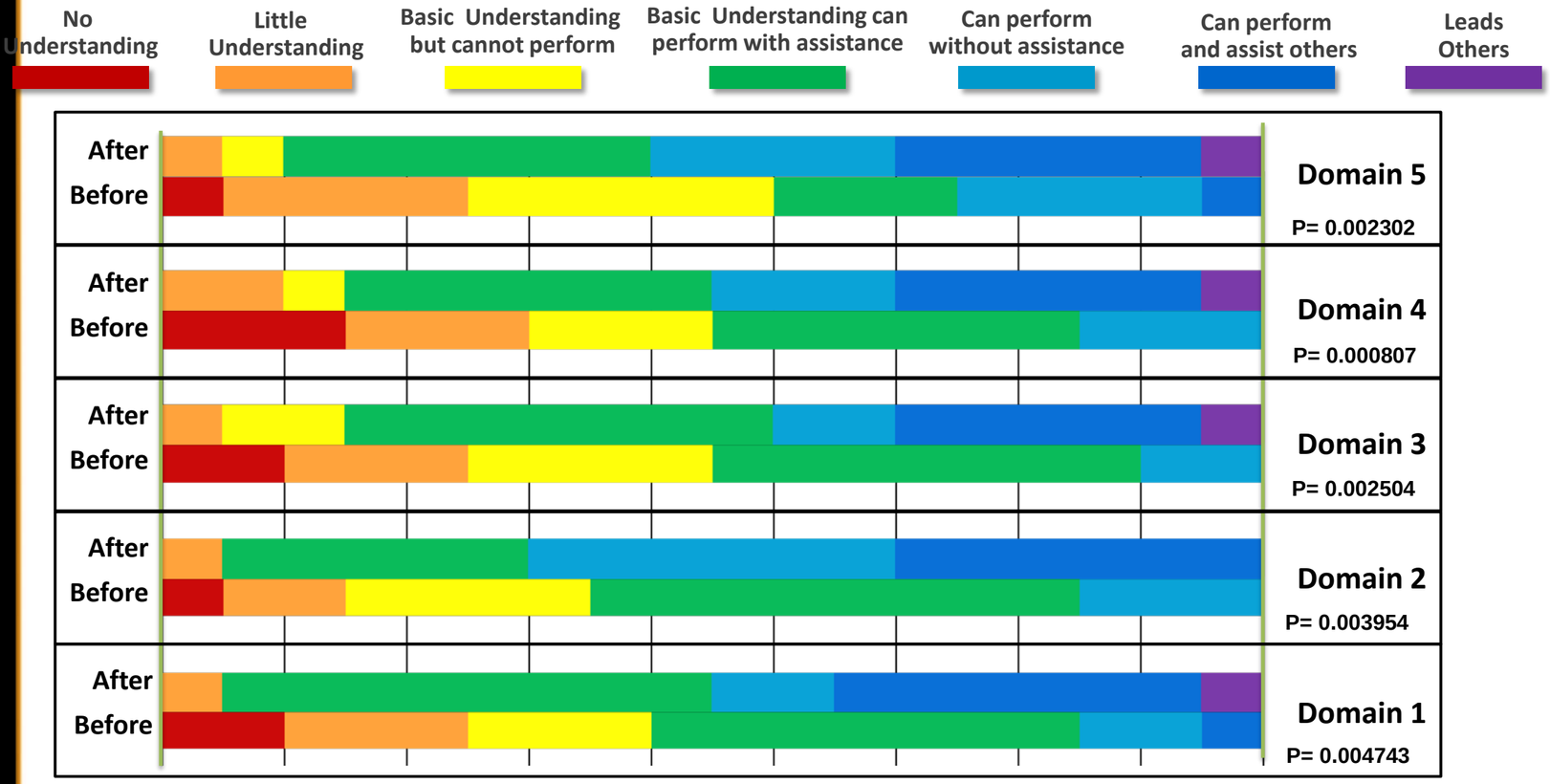
Apply learning across AoAs, requirements, engineering, and risk trade-off analyses to achieve a cost-effective security architectural design for protections that enable mission/business success; and

Evaluate the effectiveness and suitability of the security elements of the system as an enabler to mission/business success

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.

Qualitative Comments

- Right now, as a novice, I would say my biggest challenges are ensuring I have a full and complete understanding of all the components, and having a clear vision of putting all this into play …
- The biggest challenge is simply a matter of scope vs. resources. We all face this of course, so finding time to keep momentum requires focus that is sometimes difficult.
- I was impressed that the training was compressed into two days. So much material was covered! … I think that improvement will come from continuing the activity so it is not a one and done …
- This workshop helped me better understand the requirements and how to convey that importance to our customers …
- When looking at the security posture of an asset, I will now ask the questions to determine what the priority result is for this asset and then look at the systems needed to attain that goal / result. …
- I'm standing up a lab for a new C2P effort … It is aimed at replacing the legacy C2P over the next decade. I expect to apply the techniques learned in this workshop during our IPTs …
- This course has made me more important as a resource to others around me … Already, leaving the class, was able to connect to a resource in the Cloud Broker to the O(ffice)365 Broker …

Qualitative Comments

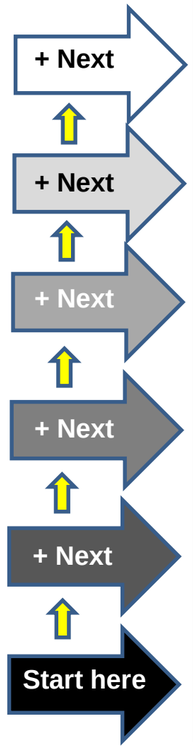
Interest in Cyber Profession …

- I am a systems administrator but am looking to make cyber my focus so currently looking at all the options available to me to make the switch.
- This week, I have attended your workshops. I am very interested in an educational path that will ultimately end up in a professional career in Cyber Security. Do you have any recommendations on how to start in the field?

Working with Teams to make a Difference …

- I wanted to reach out and say thank you for the relevant class last week. I got a lot out of it. I'm the guy in the back that asked all the questions and stumped you on the RFI GFI question….I appreciate your patience with my questions. It will be a team effort to look at how we do things and change course where we need to do better. Your class was a great tool to help me do this. I recommended it to my team.
- I want to exercise the strategies that my xxxxx team is coming up with for the maturity model against what I learned last week. It will provide cyber engineering experiential learning for the xxx team, reinforce recently acquired knowledge through application for me, and get eye to eye conversations going between entities (e.g., HSI, SE, CE, IT, PM) that otherwise may not interact first person during initial concepts of strategic planning.
- I am getting a lot out of the workshop and am planning to work with the Divisions and IPTs within the Department to schedule them for this workshop. … The SECNAV report is simply documenting a severe lack of leadership attention to a critical area. We have placed our Navy in a precarious position of not having a capability in dealing with two of our fieriest adversaries.

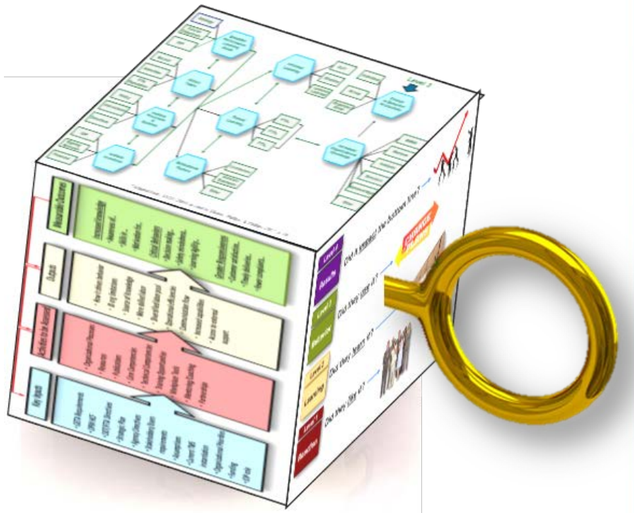
The Why: Cybersecurity is fast becoming the single biggest threat to our National Security in the 21st century



What can you do?	How can you do it?
Frequently test your cybersecurity knowledge through…	…The application, verification, and evidence of the critical learning behaviors demonstrated
Embody the learning accelerators and reduce the learning inhibitors through…	…Challenging work, practice…and recognize the risks associated with the forgetting curve…
Access all cybersecurity learning assets through…	…Publications, workshops, job aids, mentors….
Build your cybersecurity learning plan by your…	…IDP, self-education, and participation in communities of practice…
Understanding your role in the cybersecurity domain and determine your…	…Responsibilities, ownership, accountability…
Understanding the cybersecurity domain by learning the…	…Threats, policy, standards, trends, markets, consequences…

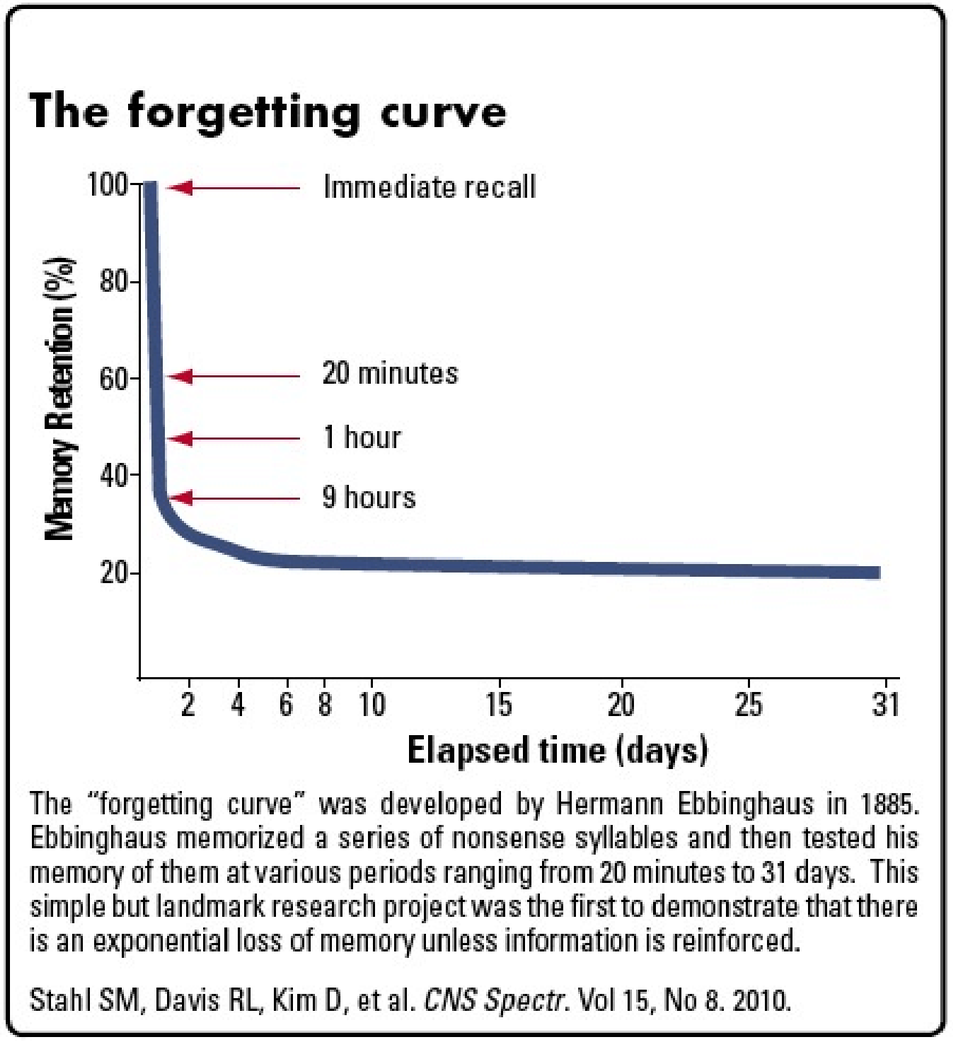
SUMMARY

- The DoD still has significant cybersecurity issues with Significant Mission Impacts
- Cybersecurity is a complex, dynamic and ambiguous domain and requires treatment as a dilemma instead of as a problem
- Cybersecurity KSAs exist (e.g. NIST SP 800-181) but are only sporadically translated into behaviors
- The forgetting curve is in full effect: cybersecurity requires an on-going customer commitment and interaction before critical behaviors can influence outcomes
- Formal (and tailored) training is the starting point. What the workforce applies in the workplace after the learning is more critical
- Commitment to customer outcomes requires on-going interaction
- Reinforcement of the behaviors is dependent on organizational commitment to ensure the changes in critical behaviors flourish



Back-Ups

Herman Ebbinghaus' Forgetting Curve



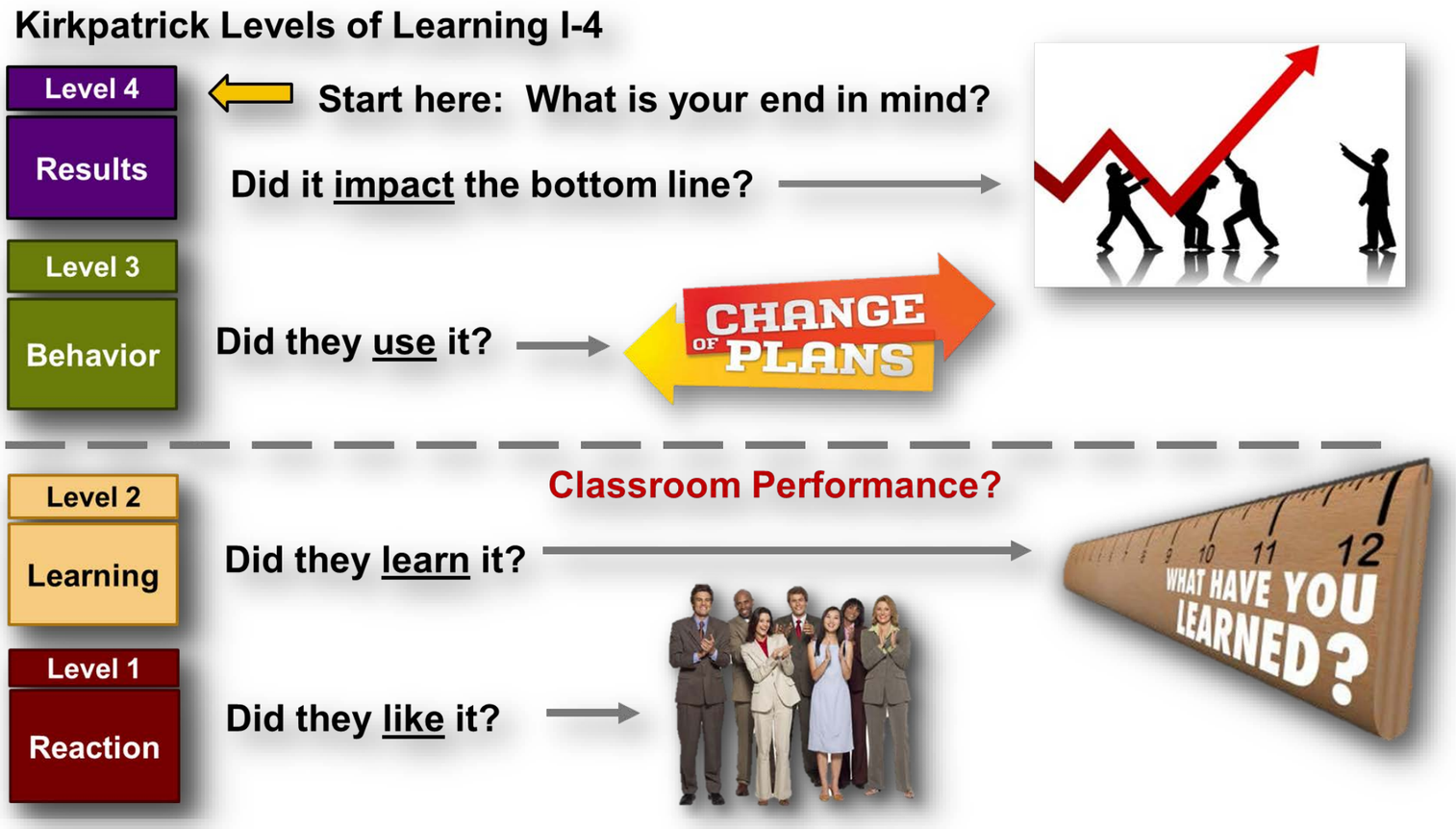
The "forgetting curve" was developed by Hermann Ebbinghaus in 1885. Ebbinghaus memorized a series of nonsense syllables and then tested his memory of them at various periods ranging from 20 minutes to 31 days. This simple but landmark research project was the first to demonstrate that there is an exponential loss of memory unless information is reinforced.

Stahl SM, Davis RL, Kim D, et al. *CNS Spectr*. Vol 15, No 8. 2010.

80% of what we learn we forget in 30 days if there is no reinforcement

The more relevant the training, the better the recall

R = e^(-t/s)



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."