SYM-AM-18-092

PROCEEDINGS
OF THE
FIFTEENTH ANNUAL ACQUISITION RESEARCH SYMPOSIUM

THURSDAY SESSIONS
VOLUME II

Acquisition Research:
Creating Synergy for Informed Change

May 9–10, 2018

March 30, 2018

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL

Cybersecurity: Converting Shock Into Action (Part 1)

Paul Shaw, CAPT, USN (Ret.)—is a Professor of IT (cyber security emphasis) at Defense Acquisition University. Shaw retired from the Navy after 30 years of service (active and reserve). He is a former Naval Aviator and Aeronautical Duty Officer (AEDO). Shaw is a Doctorate of Science (DSc) candidate in Cybersecurity at Capitol Technology University (expected completion: 2018). He has also earned five master's degrees (systems engineering, IT, international relations, finance, and management) and a BS in ocean engineering (USNA).

Robert Tremaine—is the Associate Dean for Outreach and Mission Assistance at the Defense Acquisition University West Region. He has over 30 years of experience in air, missile, and space weapon systems acquisition. Col Tremaine holds a BS from the U.S. Air Force Academy and an MS from the Air Force Institute of Technology. He is Level III Defense Acquisition Workforce Improvement Act certified in both Program Management and Systems Planning, Research, Development, and Engineering. Col Tremaine is a graduate of the Canadian Force Command and Staff College in Toronto, Ontario, Canada; and the U.S. Army War College in Carlisle Barracks, PA. He also completed a military research fellowship in association with the Harvard Business School.

Introduction

BIGBADABOOM-2. That's the name of a recent cybersecurity breach affecting 5 million stolen credit card and debit card holders (O'Brien, 2018). Unfortunately, these breaches are becoming all too common. At an alarming rate, nation states and malign actors are better equipped to conduct cyberattacks than ever. The risk is growing. Some adversaries will be able to disrupt critical infrastructure against the United States in a crisis short of war (Coates, 2018). To make matters worse, cyber threat actors are more threatening and their abilities more sophisticated. While "abilities" are just as important to defend against cyberattacks, attitudes are just as vital when it comes to the selection of the required learning strategies given their connection to necessary cybersecurity behaviors. Unfortunately, the DoD's current approach for the acquisition community won't easily fulfill the stated and implied security and resilience imperatives anytime soon unless attitudes (a critical catalyst) start to change. The learning strategies required that embody it trace back to Bloom, Krathwohl, and Harrow—all research leaders in their respective fields. Their works speak to the importance of the affective domain (i.e., the way our attitudes affect our learning behaviors). This study explores the impact of the DoD's overall implied cybersecurity learning strategy and associated actions taken to date—all intended to safeguard the efficacy of the DoD's weapon systems and supporting infrastructure. Also included is a case study discussion to demonstrate the cybersecurity actions taken by one particular organization to better prepare themselves for their assigned cybersecurity duties despite the DoD's good intentions. The learning outcome of this case study could serve as a forerunner for other DoD acquisition organizations as they consider how to implement a robust, effective and sustainable cybersecurity program. The researchers firmly believe that the DoD will be hard pressed to achieve the desired gains in security and resilience without recognizing that the critical cybersecurity behaviors and concomitant attitudes at the individual, team, and organizational levels come first. And, that might come as a shock.

Background

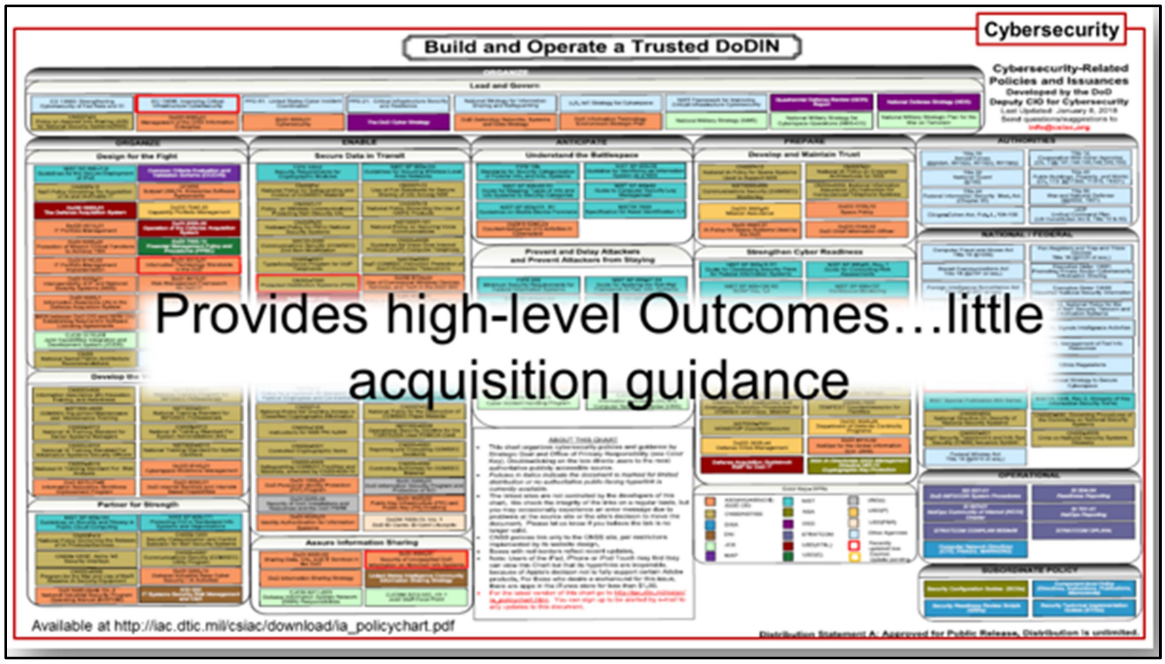
Like any emerging challenge as complex as cybersecurity, organizations will test the outer edges of their learning envelopes. To better guide this research pursuit, the authors used four specific questions to better isolate these and other learning implementation limitations currently found in the DoD's cybersecurity learning strategy. The answers were both informative and instructive:

1. **Have the DoD's actions (e.g., policy directives, tools, methods, etc.) met the stated and implied expectations for protection and resilience in the acquisition community?**

   Not really. Results of the independent assessments of the DoD's cybersecurity reports from the Defense Science Board and the DoD's testing community collectively signaled severe concerns about whether or not the DoD can accomplish its core missions and keep its critical assets intact. In 2015, a RAND Corporation report found that "cybersecurity risk management does not adequately capture the impact to operational missions and that cybersecurity is mainly added onto systems, not designed in (Snyder et al., 2015, p. ix)." Rand went on to say that the policies governing cybersecurity are better suited for simple, stable, and predictable environments leading to significant gaps in cybersecurity management. The consequences could include the following:

   - prescriptive solutions for military system cybersecurity that favor security controls over more sound system security engineering,
   - emphasis of processes and security controls for information technology systems over more tailored military systems solutions,
   - implementation of tactical security controls over more strategic mission assurance imperatives, and
   - overreliance on standardized and formalized security control compliance as a means to achieve cybersecurity (Snyder et al., 2015, p. viii).

To communicate cybersecurity imperatives, the DoD Chief Information Officer (CIO) regularly updates (about every three weeks) the policies affecting cybersecurity in a summary chart called "Build and Operate a Trusted DoDIN" (see Figure 1). Aside from the microscope nature of the details, the chart is largely outcome-based only (http://iac.dtic.mil/csiac/ia_policychart.html). Many of these high level outcomes exceed the security capabilities of the DoD's current systems capabilities recommended by the DoD DIACAP and now Risk Management Framework (RMF) process. Many of the other outcomes are either slightly mentioned in current acquisition documents or absent. The disconnect is readily apparent. How programs actually capture the DIACAP/RMF processes appear to be more compliant dominant and presumably driven by official approval of the system instead. These programs also tend to depend on a "cookie cutter" approach where they sometimes use a template overlay for security controls. Without thinking more critically about every likely eventuality along with leveraging the testing community's expertise to confirm operational objectives beforehand, these same programs face looming cost and schedule risks. The OCX program reinforces the repercussions when they do. Raytheon fully underestimated the cybersecurity requirements by discounting the impact of COTS and free and open source software. It represented one of several factors that contributed to a multi-year schedule delay and cost increase estimated to exceed $1 billion (Kendall, 2016).



Note. This chart is updated frequently by the DoD CIO.

Figure 1. Build and Operate a Trusted DoDIN

What are the metrics and have they been effective?

The answer is no.

- Most systems have rudimentary security requirements for implementing metrics. They generally include the following:
  - exercising logical access controls with certain frequency,
  - managing software inventories at certain intervals,
  - implementing information security management in accordance through prescribed methods, and
  - monitoring/detecting data exfiltration.

  While NIST 800-53 security controls recognize these type of metrics as a good start, programs fall short of implementing a dynamic evaluation approach that includes testable standards with the proviso that they need to evolve as a part of a system's inherent system security architecture.
- Most Program Office requirements fall short of testing at levels that mimic likely operational conditions and scenarios. Systems designers normally concentrate on the threats to and subsequent actions required in the context of information exchanges within their system where they believe they could be more easily exploited. Alternately (and more effectively), the testing community uses external stimuli they expect to see surface in an operational environment that could easily (and frequently) exploit security and resilience gaps. They don't treat systems as adiabatic in any way, shape or form. This effect is especially evident when high level requirements go beyond basic system behaviors (from inside the system to the system's exchange of information requirements).

- In an independent assessment conducted by the Office of Management and Budget (OMB) with *Federal Information Security Modernization Act of 2014: Annual Report to Congress* for FY 2016, the DoD's information security program received an uncomplimentary rating (p. 44). From a scale of 1 (lowest) to 5 (highest), the DoD earned grades on the lower end of the scale compared to all federal agencies that earned grades on the higher end, ranging from 4 to 5. The DoD's grades were consistently on the low end:
    - Identify—Level 2 Defined
    - Protect—Level 2 Defined
    - Detect—Level 1 Ad Hoc
    - Respond—Level 2 Defined
    - Recover—Level 2 Defined

Can these shortcomings be overcome? It requires a change of approach, culture, and workforce attitudes.

Is the DoD headed in the right direction?

The answer is partly.

- The DoD has reinforced "cybersecurity as a requirement for all DoD programs across the life cycle" (DoD CIO, 2014, p. 155).
- The DoD has recognized that all systems must manage "risk commensurate with the importance of supported missions and the value of potentially affected information or assets" (DoD CIO, 2014, p. 2). Moreover, the DoD's cyber strategy emphasizes the need to:
    - not defend every network against all threats;
    - identify, defend, & prioritize most important for mission;
    - be able to operate in degraded & disrupted environments; and
    - use technology & innovation to stay ahead of threat (p. 13).
- The DoD emphasizes the need for systems to be both secure and resilient. Security mechanisms afford a defense against a cyberattack or allow a system to maintain operations. Resilience can reset a system, even if the cyberattack is not detected or understood (Defense Science Board, 2016), or allow it to operate in a degraded mode. Critical cyber components could implement resilience for performance of critical functions, regardless of fault cause or nature (Defense Science Board, 2013).

  Systems like WIN-T changed their thinking to incorporate threat-based engineering and developed multiple threat models. They assumed comprise and adopted a continual testing process strategy and cybersecurity that became an inherent part of the engineering processes across their systems. Cybersecurity was no longer a separate solution.

More specificity is warranted. The DoD's high-level policy has many cybersecurity elements at the outcome level to guide programs, although noticeable gaps in acquisition guidance persist for the effective implementation of key objectives in a meaningful way (i.e., how to better respond to realistic conditions that the operational test community will impose). The DOT&E annual report dated January 2018 indicated that "despite improvements in network defenses, *almost every assessment and test demonstrated that DoD network defenses still contain exploitable problems* that provide cyber adversaries opportunities for

access to DoD networks" (p. 318). If the DoD were to compel the acquisition workforce to go beyond a "compliance construct" for cybersecurity, more systems might just pass various Adversarial Assessments in Operational Test and fulfill Operational Commanders' mission assurance needs. This requires a change of approach, culture, and workforce attitudes.

What industry best practices should the DoD adopt and why?

Industry best practices have concentrated their efforts on resilience, trustworthiness, and continual testing. Intel, Google, Microsoft, Netflix, and others have boosted their security posture by going beyond traditional security activities that focus just on system protection. For example,

- Intel employs a Trusted Execution Technology to ensure their operating kernels are of a known trusted state.
- Google verifies that all servers in their data centers operate from a globally distributed trusted image.
- Microsoft's evolving security posture continually evaluates threat activities.
- Netflix conducts cybersecurity testing with the Simian Army in continuous mode and digitally stresses their content delivery infrastructure to influence responsive systems engineering actions.

All these companies have adopted a security posture of adaptability and innovative thinking in response to impending cyber threats. They don't think for a second they won't be compromised. Their active measures are also consistent with comments made by the Director of Operational Test and Evaluation FY 2016 Annual Report, where he said, "Cybersecurity tests will demonstrate active defense from attacks, measure the effectiveness of the cyber defenses, and assess the mission impacts resulting from cyber-attacks" (Behler, 2018, p. 447). These cybersecurity strategies align with the September 2016 Defense Science Board report on Cyber Defense Management, which suggested "examining the attack data to determine what is working well, what is not, where changes need to be made, and where investment is required to better defend against troublesome or emerging threats to move beyond a compliance approach towards a more dynamic performance evaluation" (p. 11). Will this type of thinking eventually become pervasive in the DoD? It requires a change of approach, culture, and workforce attitudes.

Assumptions

As with any research study, assumptions generally help characterize the research constraints as well as the prevailing environmental domain. For cybersecurity, it's no different. While strikingly provocative, the following assumptions reinforce today's cybersecurity operating envelope:

- Cybersecurity is a decaying function—static cybersecurity assures a declining security posture.
- NO SYSTEM is without malware—every system has an inherent vulnerability just waiting to be exploited.
- Organizations rely too much on 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., outcome level is typically characterized as “design for the fight”).
- Most programs undershoot “adequate security”—many operate under a false sense of security until they discover they did not sufficiently manage realistic and likely operational risks.
- The DoD may not be proactive enough to exploit its own systems to withstand advanced threats.

Research Tools Used

Several tools were ideally suited for this research pursuit. The first, a high-level logic model (see Figure 2), would set the flow, narrow the focus, and underpin the researcher’s end-in-mind. In the past two decades, its usefulness has also been recognized by others. Clarke (2004) used diagramming since they link categories with categories to form a substantive theory of action that shows “at a glance if outcomes are out of sync with inputs and activities.” They help researchers “make sense of relationships that may not have been previously explicit” (Buckley, Waring, 2013). Spaulding and Falco (2013) found they “provide linkages between activities and outcomes as well as to serve as a framework for developing quality and purposeful activities.” For cybersecurity, there are no perfect solutions. However, “living” models like logic models could expose these new truths during a project’s life cycle, especially when the operating environment can be so dynamic and ambiguous at the same time.

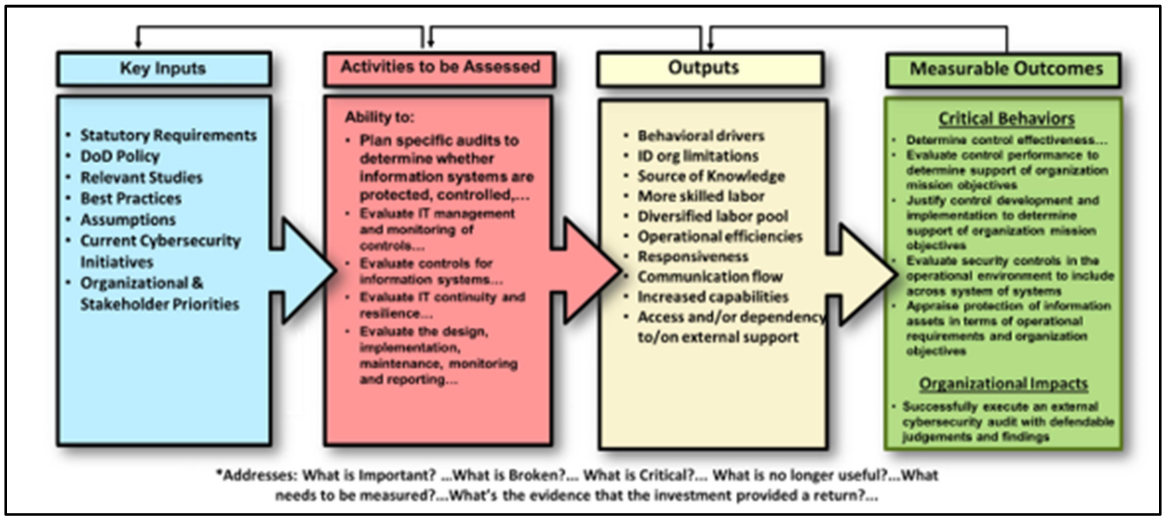


Figure 2. High Level Logic Model That Guided This Research

Kirkpatrick’s Learning Levels was the second tool selected because “Logic Models don’t show why activities are expected to produce outcomes” (Clark, 2004). The Kirkpatrick would show why and help verify if the learning stuck long enough to change the way the learners operated back on-the-job to be highly effective. The authors were especially interested in determining if what a cohort group learned in an objective-driven workshop resulted in any behavioral changes back in the workplace. Among the various learning tools available, Kirkpatrick’s four levels of learning seemed well suited to help characterize the learners’ journey to demonstrate the achievement of their indispensable “critical behaviors.” In its simplest form, Figure 3 depicts the Kirkpatrick’s learning levels.

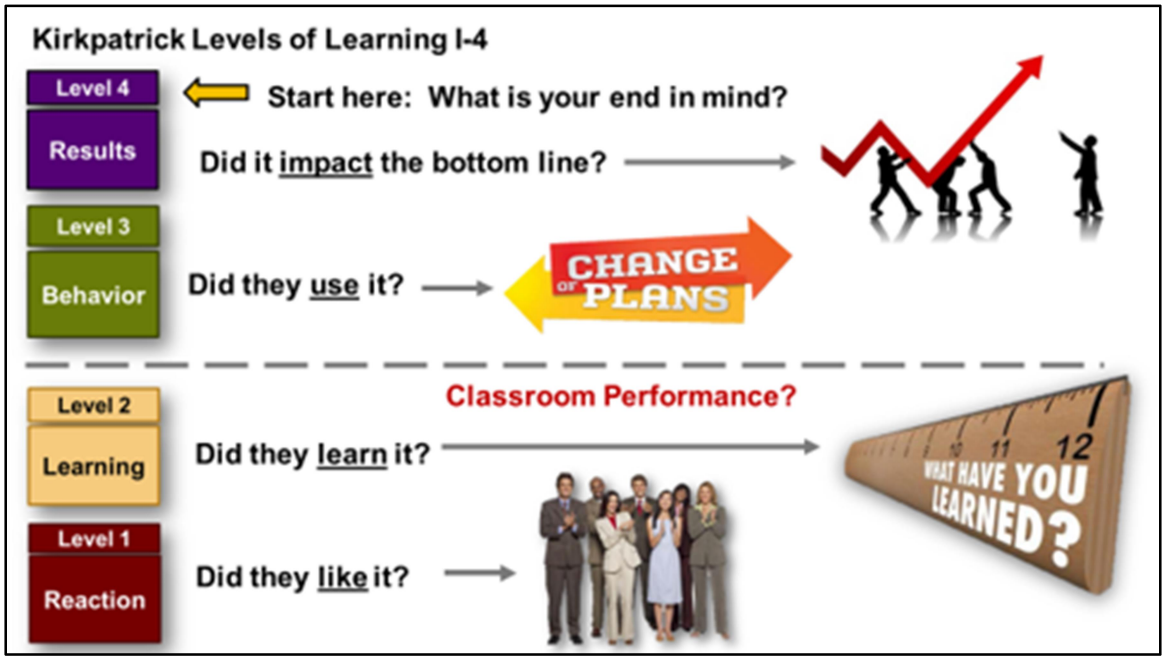


Figure 3. Kirkpatrick Learning Levels
(Kirkpatrick, 2016)

Incorporating both the Logic and Kirkpatrick Learning tools into a Performance Learning Value chain tool would provide a fully embodied visual representation (see Figure 4). It would also help show the learning dependencies leading to the learning evidence. Without the evidence, it would be hard to prove any link(s) to the initial and/or ongoing learning investment made by any organization.

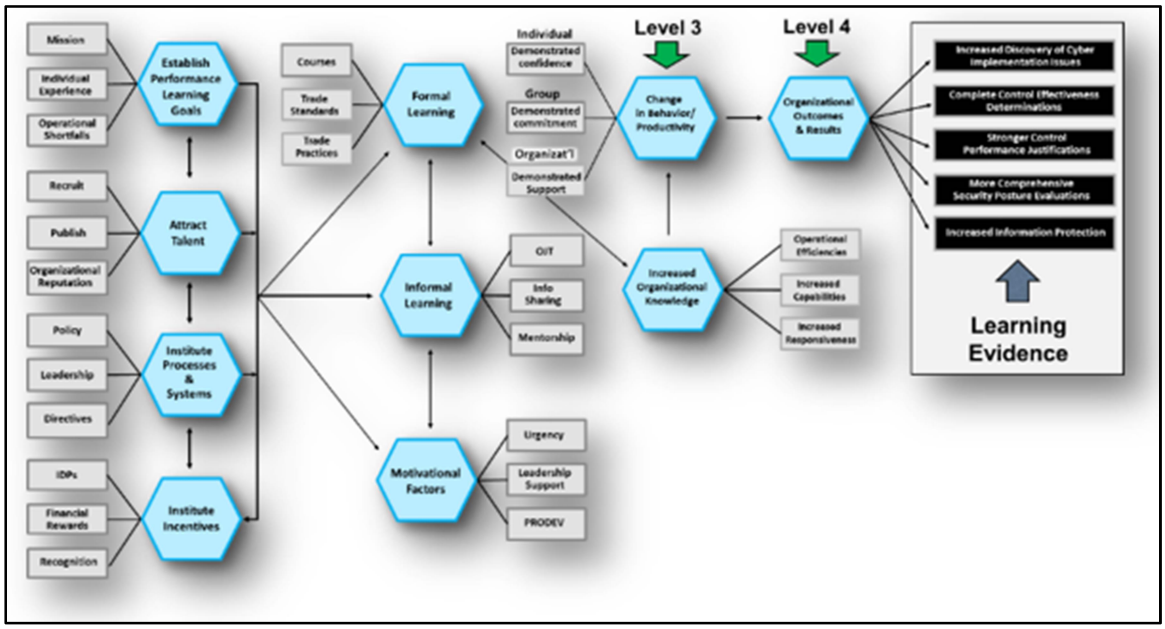


Figure 4. Performance Learning Value Chain
(Adapted from ASTD, 2004, as cited in Elkeles, Phillips, & Phillips, 2017, p. 10)

To help build greater cybersecurity knowledge and raise awareness for acquisition professionals, DAU conducted a variety of workshops—over 35 in the last three years across various DoD components and program offices. During these workshops, the following common themes surfaced from the engaging discussions:

- Current DoD cybersecurity guidance is at the strategic outcome level and generally forces program offices to take more time translating these outcomes into operation and tactical outputs.
- Enterprise cyber intelligence and warning signs can be difficult to translate into cybersecurity risk for probability and impact to their system because cyber threats are so fluid.
- Cybersecurity threats force program offices to spend more time on something that is so dynamic and sometimes difficult to translate their needs based on how they might impact their systems today.
- Risk mitigation strategies aren't tightly connected to mission assurance imperatives in the face of a hostile environment imperatives.
- Program offices may too quickly acquiesce (and accept higher risk levels) to cybersecurity design decisions because of their inability to change in their acquisition life cycle stage or to accept the perils of their inherent legacy design.
- Program offices still have to convince their resource sponsors and MDA of the needs and consequences to address potential cyber vulnerabilities.

The three models discussed previously were not used in the cybersecurity workshops. However, they set the stage for a more comprehensive case study assessment.

Case Study

For most organizations that seek to connect their learning gains in class (level II) with objective applications in their workplace afterwards (Level III), the bridge between level II and Level III can be a difficult challenge. Without it, what evidence can organizations use to confirm that the resources they allocated to Level II learning gains actual paid off? The Assistant Auditor General for Financial Management & Comptroller Audits who reports to the Naval Audit Agency graciously volunteered to participate in this case study. They wanted to ensure their auditors could apply what they learned in what they considered to be a vital functional domain—cybersecurity. Figure 5 represents the current instantiation of the Naval Audit Service Directorates. Earlier, a couple of their personnel attended DAU's cybersecurity awareness workshops. They left with a very strong feeling that their cohort group needed the same experience. Later, and after several subsequent interactions between DAU and the Naval Audit directorate's team leads as well as their leadership, the directorate welcomed a way to confirm the critical cybersecurity behaviors expected of them in the prosecution of their all audit responsibilities were met.

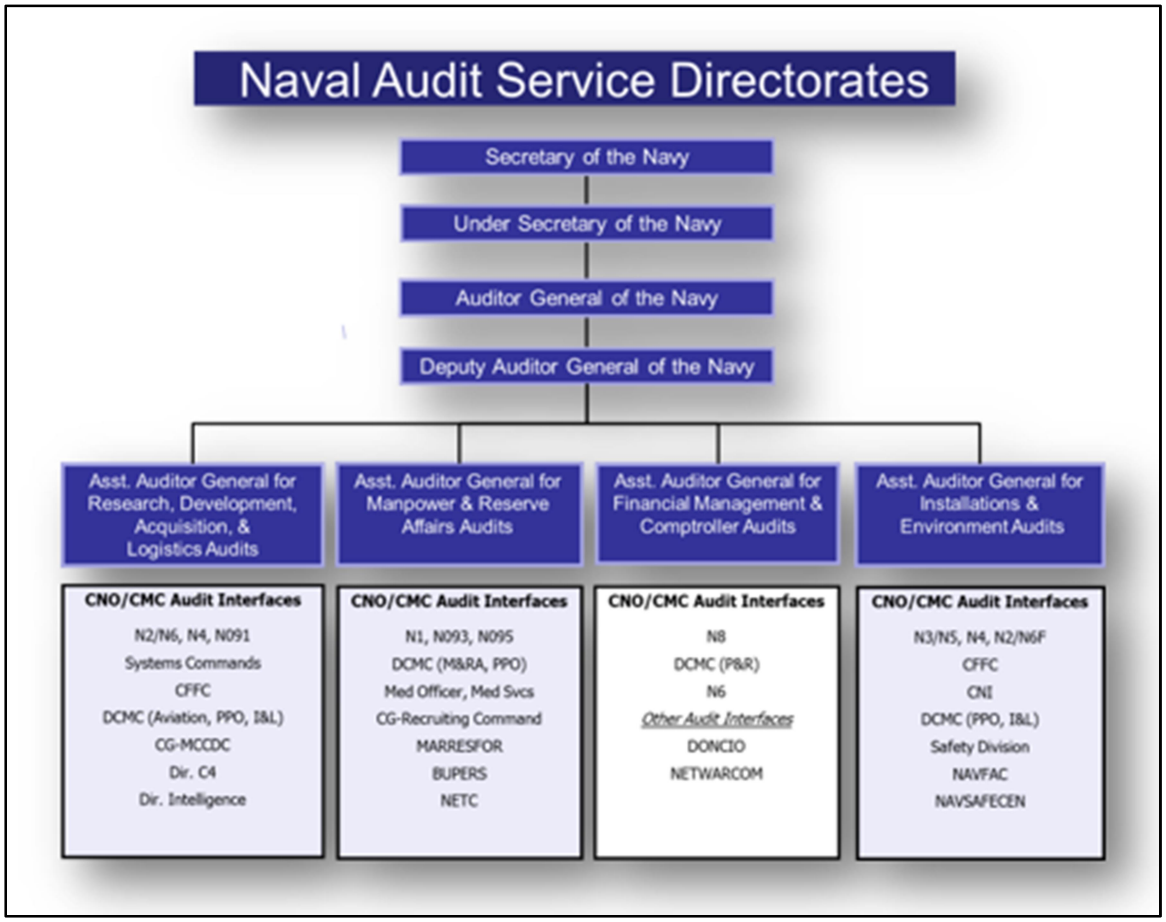


Figure 5. Naval Audit Services Directorate Structure

The cybersecurity workshop customized for the Naval Audit Services Directorate addressed the following learning objectives (i.e., Learning Level II):

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

The learning objectives cut across the five domains that constituted the team's responsibilities (see Figure 6).

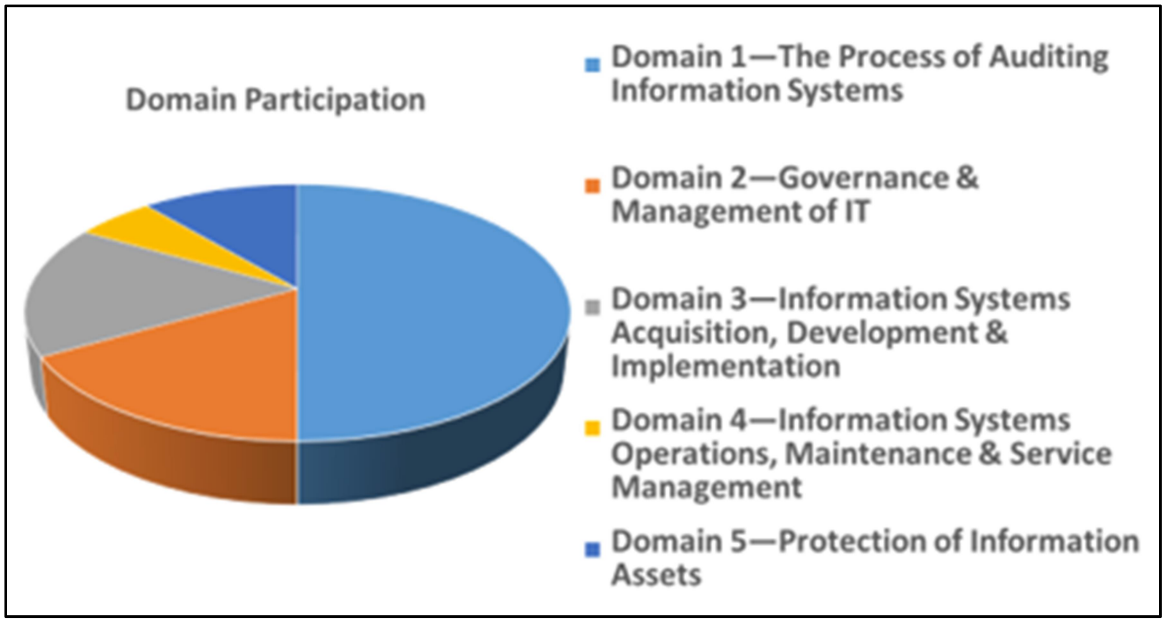


Figure 6. Domain Participation

The directorate's intact teams who attended the workshop also previously committed to connecting Level II learning objectives with the Level III critical behaviors. Just as importantly, their leadership committed to what Kirkpatrick calls its required drivers (i.e., monitor, encourage, reinforce, and reward) to assure their Level III achievements (Kirkpatrick, 2016, p. 56). Without them, a key feedback mechanism would be missing, and accountability opportunities would be lost.

Results and Findings

Figure 7 summarizes what 19 respondents had to say about their Level II learning levels "before and after" after the workshop. There were 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.

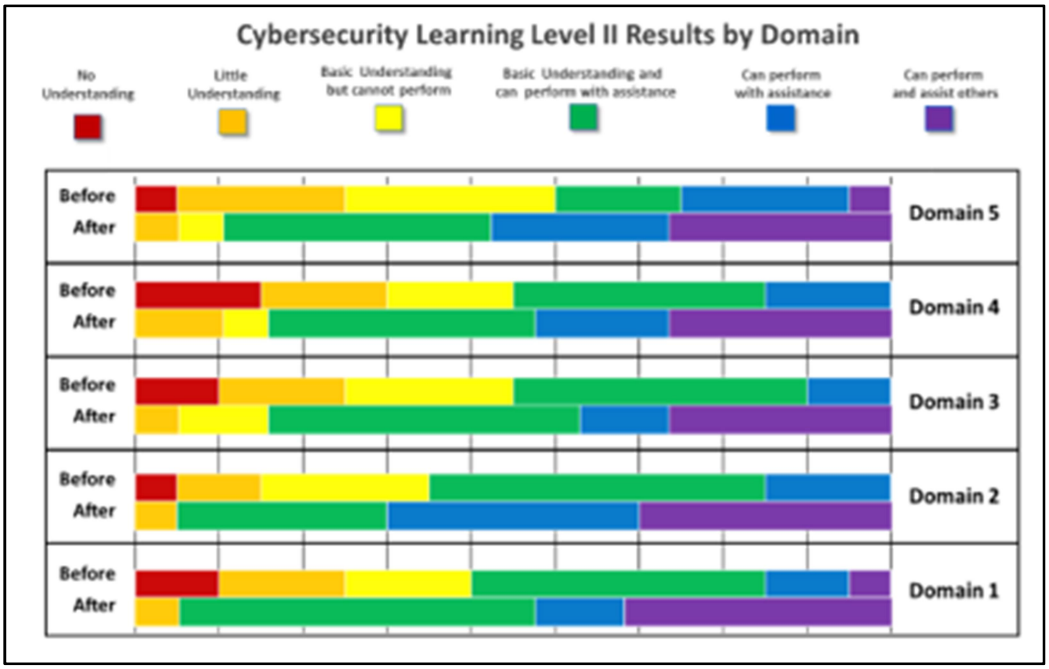


Figure 7. Cybersecurity Workshop Results

The respondents also provided a number of illuminating comments when asked, "What initial successes will likely occur as you consistently apply what you learned?" Here's what they had to say:

- We plan to incorporate all the concepts we learned in 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.
- Also, I plan to work with the audit team to develop potential audit topics that involve cybersecurity within the DoN.
- 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.
- 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.

However, the more important aspect surrounding the abilities and attitudes of the learners to apply what they learned in the workshop back on-the-job (i.e., Level III) that doesn't atrophy, and what results their learning afforded. Furthermore, what will happen and what needs to happen to strengthen the bridge between Level II and Level III? Here are the Level III critical behaviors that were jointly developed up front with the team:

- Auditor determines control effectiveness and makes audit findings on controls for organization evaluation.
- Auditor evaluates control performance to determine support of organization mission objectives and makes audit findings on controls for organization evaluation.
- Auditor justifies control development and implementation to determine support of organization mission objectives and makes audit findings on controls for organization evaluation.
- Auditor evaluates security controls in the operational environment to include across system of systems and makes audit findings on controls for organization evaluation.
- Auditor appraises protection of information assets in terms of operational requirements and organization objectives to make audit findings and recommendations.
- Auditors are able to successfully execute an external cybersecurity audit with defendable judgements and findings by reviewing information, work products, or systems outputs based on a set of accepted auditing criteria.

The achievement of these Level III critical behaviors represents the litmus test. Through a suitable dose of feedback (i.e., monitor, encourage, reinforce, and reward), Level III critical behaviors and Level IV results can be achieved, later.

Extendability

The generalizability and extendibility of the claims from this research should be able to be prove validity through independent repeatability (Creswell, 2015). The NIST 800-181 National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework defines tasks, knowledge, skills, and abilities of numerous groups throughout the Cybersecurity Workforce. Using these workforce tasks, knowledge, skills, abilities, attitudes, learning objectives, and critical behaviors should be extendable to other workforce groups. Measurement issues of study constructs can easily exploit instruments like the Kirkpatrick model. However, caution should be taken to avoid use of just a single measure (Lund Research Limited, 2012). There is more than one interaction and measurement in any research project. Addressing these considerations would reduce the burden of proof for validity and broader extendibility.

Conclusion

Despite the DoD's good intentions in their policy declarations, focusing on the cybersecurity behavioral changes in the acquisition community is an equally important consideration that doesn't appear to be highly visible. The number of cyber threat actors who have the ability to exploit DoD's systems is growing at a staggering rate, while too many people involved in the acquisition community may not have fully embraced (or even understand) their role in cybersecurity. It's vitally important to elevate the acquisition community's knowledge of all cybersecurity risks in order to more carefully plan, decide, and act for the inescapable and impending cybersecurity threats. Admittedly, the danger signs are very telling, and they're not all good. No one would argue that cybersecurity is taking center stage as our dependency on the internet continues to increase.

Following a particular organization responsible for auditing the implementation of cybersecurity imperatives has been quite informative and has highlighted instrumental triggers and influencers that are so central to the achievement of desired learning outcomes.

The personnel involved in the case study is still underway. In Part 1 of a two-part research project, the authors helped reinforce which critical behaviors the participants had to embody to assess mission assurance. Time will tell if it resulted in any expected gains. In the interim, the Assistant Auditor General for Financial Management & Comptroller Directorate intends to monitor, encourage, reinforce, and reward the behaviors required by their daily duties to guide them—and convert shock into action. Part II will address their successes as well as any particular challenges they faced through ample objective evidence.

From a macro viewpoint, what steps should the DoD take now to translate their high-level outcomes into achievable acquisition behavioral changes?

- Ensure that programs don't stop cybersecurity development and testing at the interfaces, and instead compel programs to instinctively develop in a real world environment.
- Publish the critical cybersecurity competencies and proficiency levels required by all defense acquisition professionals.
- Recognize that any new policy requires a companion discussion on learning behavior implications and compel the services to report annually on their actions to address them.

What steps should YOU take to better prepare for your cybersecurity acquisition responsibilities? In many cases, it comes down to personal attitudes. Here are several that require more immediacy:

- Don't outsource your cybersecurity thinking to someone else. Take time to learn the risks and issues. Be prepared for all eventualities.
- Think critically about cybersecurity. Open your apertures, think beyond compliance, and build a more robust cybersecurity posture.
- Daily exercise the cybersecurity critical behaviors incumbent in your duties and hold your colleagues accountable to the same standards.
- Always assume compromise and set the lowest threshold for trust in all system interfaces. Never trust another system, especially if unexpected behavior occurs.

References

Barrett, M., Maron, J., Pilitteri, V., Boyens, J., Witte, G., & Feldman, L. (2017). *The cybersecurity framework: Implementation guidance for federal agencies* (Draft NISTIR 8170). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://csrc.nist.gov/csrc/media/publications/nistir/8170/draft/documents/nistir8170-draft.pdf

Behler, R. (2018). *Director, Operational Test and Evaluation FY 2017 annual report*. Retrieved from http://www.dote.osd.mil/pub/reports/FY2017/

Clarke, H. (2005). *Theories of change and logic models: Telling them apart*. Retrieved from http://www.theoryofchange.org/wp-content/uploads/toco_library/pdf/TOCs_and_Logic_Models_forAEA.pdf

Coates, D. (2018). *Worldwide threat assessment of the U.S. intelligence community*. Retrieved from Director, National Intelligence, website: https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

Creswell, J. (2014*). Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Thousand Oaks, CA: Sage.

Creswell, J. (2015). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (5th ed.). Upper Saddle River, NJ: Pearson.

Cyber Security and Information Systems Information Analysis Center. (2018). The DoD cybersecurity policy chart. Retrieved from http://iac.dtic.mil/csiac/ia_policychart.html

Defense Science Board. (2016). *Cyber defense management*. Retrieved from https://www.acq.osd.mil/dsb/reports/2010s/Cyber_Defense_Management.pdf

Director, Operational Test & Evaluation. (2017). *Cybersecurity OT&E—guidance* (Ver. 3.0). Retrieved from http://www.dote.osd.mil/docs/TempGuide3/Cybersecurity_OT&E_Guidance_3.0.pdf

DoD. (2015). *The DoD cyber strategy*. Washington, DC: Author. Retrieved from https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

DoD, Chief Information Office. (2014). *Cybersecurity*. (DoDI 8500.01). Washington, DC: Author. Retrieved from http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf

Elkeles, T., Phillips, J. J., & Phillips, P. P. (2017). *Chief talent officer: The evolving role of the chief learning officer* (2nd ed.). Routledge.

Gilmore, J. (2017). *Director, Operational Test and Evaluation FY 2016 annual report*. Washington, DC: DoD. Retrieved from http://www.dote.osd.mil/pub/reports/FY2016/

Hall, J. (2017). *Developmental Test and Evaluation FY 2016 annual report*. Washington, DC: DoD. Retrieved from https://www.acq.osd.mil/dte-trmc/docs/FY2016_DTE_AnnualReport.pdf

Helen, K. (2014). Power-up your research with diagrams and models. Retrieved from http://www.qsrinternational.com/nvivo/nvivo-community/blog/power-up-your-research-with-diagrams-and-models

Kendall, F. (2016). Next Generation Operational Control System (OCX) Nunn-McCurdy Certification Basis of Determination and Supporting Documentation, Under Secretary Secretary of Defense (AT&L), Letter to the Senate Arms Service Committee. Retrieved from https://myclass.dau.mil/bbcswebdav/institution/Courses/Deployed/ACQ/ACQ404/Archives/Student%20Materials/Student_Materials/5%20SAMC%20Class%20Prep%20Readings%20FY17-1%20Nov%2014-18/z%20-%20Additional%20Material/USD%28AT%26L%29%20Oct%2016%20Ltr%20to%20Congress%20Re%20OCX%20Certification.pdf

Kirkpatrick, J., & Kirkpatrick, W. (2016). *Four levels of training and evaluation*. Alexandria, VA: ATD Press.

Lund Research Limited. (2012). *Threats to external validity*. Retrieved from http://dissertation.laerd.com/external-validity-p3.php

Newhouse, W., Keith, S. Schribner, B., & Witte, G. (2017). *National initiative for cybersecurity education (NICE) cybersecurity workforce framework* (NIST Special Publication 800-181). Washington, DC: National Institute for Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

O'Brien, M. (2018, April). Data breach affects Saks, Lord and Taylor. *San Diego Union-Tribune*, p. A2. Retrieved from https://www.nbcsandiego.com/news/business/Data-Breach-Hits-Saks-Fifth-Avenue-Lord--Taylor-Stores--478488543.html

Office of Management and Budget (OMB). (2016). *Managing information as a strategic resource* (OMB A-130). Washington, DC: Author. Retrieved from https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource

Office of Management and Budget (OMB). (2017). *Federal Information Security Modernization Act of 2014: Annual report to Congress.* Washington, DC: Author. Retrieved from https://www.hhs.gov/sites/default/files/fy_2016_fisma_report%20to_congress_official_release_march_10_2017.pdf

Snyder, D., Power, J., Bodine-Baron, E., Fox, B., Kendrick, L., & Powell, M. (2015). *Improving the cybersecurity of the U.S. Air Force military systems throughout their life cycles*. Santa Monica, CA: RAND. Retrieved from https://www.rand.org/pubs/research_reports/RR1007.html

Spaulding, D., & Falco J. (2012). *Action research for school leaders*. Pearson.

Under Secretary of Defense for Acquisition, Technology, & Logistics (USD[AT&L]). (2015). *Operation of the defense acquisition system* (Incorporating change 3, August 10, 2017). Washington, DC: DoD. Retrieved from http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002_dodi_2015.pdf

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL
555 DYER ROAD, INGERSOLL HALL
MONTEREY, CA 93943

www.acquisitionresearch.net