SYM-AM-19-038

PROCEEDINGS
OF THE
SIXTEENTH ANNUAL ACQUISITION RESEARCH SYMPOSIUM

WEDNESDAY SESSIONS
VOLUME I

Acquisition Research:
Creating Synergy for Informed Change

May 8–9, 2019

Published: April 30, 2019

Approved for public release; distribution is unlimited.

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

Cybersecurity: Converting Shock Into Action (Part 2)

Paul Shaw—Defense Acquisition University

Robert L. Tremaine—Defense Acquisition University

Abstract

Last year, the authors presented Part 1, which focused on a discussion on policy/directives and then explored the efficacy of the DoD's cybersecurity strategy and associated actions taken to date—all intended to safeguard the efficacy of DoD systems. The goal of the research in Part 2 is centered on the design and implementation of the cybersecurity training intended to achieve the key cybersecurity behaviors to meet that end. The Kirkpatrick Learning Level framework is used to help translate learning objectives into security and resilience critical behaviors for organizational oversight. The process of translating Knowledge, Skills, and Attitudes (KSAs) into learning objectives and workplace behaviors is also discussed. However, what the workforce actually applies in the workplace is the most important part of the equation, especially its correlation to expected outcomes. Part 2 addresses just that. The DoD will be hard-pressed to achieve any mission assurance objectives for security and resilience without recognizing that (1) cybersecurity critical learning behaviors require commitment at all levels—individual, team, and organizational; and (2) cybersecurity must be viewed as more of a dilemma where emerging threats will surface continuously and must be assessed with regular frequency to ensure the viability of the DoD's weapon systems' lethality.

Introduction

In March 2019, the Secretary of the Navy (SECNAV) released an extensive *Cybersecurity Readiness Review*. His uncomplimentary readiness review reinforced the findings of numerous other reports (e.g., reports by the Director National Intelligence [DNI]; Office of Management and Budget [OMB]; Government Accountability Office [GAO]; DoD Inspector General [IG]; Defense Science Board [DSB]; Director, Operational Test and Evaluation [DOT&E]; and other government agencies, think tanks, etc.) that concluded a cyberattack by an advanced cyber threat could easily inflict significant mission impact to the DoD. Simply stated, the DoD (and perhaps other federal agencies) is (are) not achieving their required mission assurance outcomes for cybersecurity and cyber resiliency. The response to the quintessential question for DoD cyber risk management (i.e., can the DoD as a collective handle a co-evolving, intelligent cyber threat?) is not good. Almost every assessment of the DoD and its supporting infrastructure has reaffirmed that it is woefully unprepared for attacks from a cyber peer. Even worse, the DoD continues to fall further behind year after year, and that might come as a shock to those who would depend on the DoD to prevent a catastrophic event by a cyber peer.

The DoD already has significant cybersecurity issues (i.e., Significant Mission Impact) and faces a learning culture with little understood obstacles, including the following:

- Cybersecurity is a complex, dynamic, and ambiguous domain and is becoming a <u>dilemma</u>.
- Cybersecurity Knowledge, Skills, and Attitudes (KSAs) exist (e.g., Newhouse et al., 2017) but are only sporadically <u>translated into critical learning behaviors</u>.
- The forgetting curve is no stranger to cybersecurity. Cybersecurity requires an <u>ongoing commitment to a workplace learning environment</u> for competencies to flourish.

- Formal (and tailored) training is only a learning antecedent. What the workforce actually applies (and practices) in the workplace with regular frequency is vitally important.
- Reinforcement of the critical behaviors is dependent on leadership's persistence to establish and maintain a strong learning culture.

Given its complexity, domain ambiguity, and dynamic nature, cybersecurity cannot depend on incidental learning. While a lot of good work has been done with cybersecurity core knowledge and tasks (e.g., Newhouse et al., 2017), it has yet to be translated into the critical behaviors required to fully embody cybersecurity learning gains. Newhouse et al. (2017) has numerous applicable KSAs for most cybersecurity workers, and the KSAs can be easily translated into Bloom's Taxonomy action verbs. However, using any learning application framework (e.g., Kirkpatrick or Brinkerhoff) to translate learning objectives into critical behaviors for organization oversight of security and resilience as far as their realization goes has not yet been implemented. The process of translating KSAs into learning objectives and behaviors is discussed with various representative groups. National Initiative for Cybersecurity Education (NICE) KSAs (Newhouse et al., 2017) have only connected learning objectives and behaviors described as follows:

- K0106—Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities
- K0110—Knowledge of adversarial tactics, techniques, and procedures
- K0112—Knowledge of defense-in-depth principles and network security architecture
- S003—Skill in evaluating the adequacy of security designs
- S0027—Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes
- S0054—Skill in using incident handling methodologies

What the workforce applies in the workplace is the most important aspect for cybersecurity learning. It is the reason for this research pursuit—and the more strategic challenge for the entire cybersecurity learning discipline, ahead.

Problem Statement: This research continues previous work that started with the DoD's cybersecurity strategy and policy. After conducting over 70 cybersecurity workshops with various DoD customers, cybersecurity assistance has transitioned to assisting program offices with their more chronic cybersecurity risk management challenges instead of a program's acute cybersecurity shortcomings.

Research Goals:

- Assist program offices with their commitment to harbor critical learning behaviors that support security management and security engineering that may lead to essential cybersecurity risk management practices for an evolving cyber threat.
- Demonstrate that implementing a robust, effective, and sustainable cybersecurity program requires a long-term and ongoing commitment and a transition from solving a problem to managing a dilemma.

The researchers posit that the DoD will be hard-pressed to achieve the desired mission assurance objectives for security and resilience without recognizing cybersecurity risk management, and that the achievement of security engineering critical behaviors must predominate at the individual, team, and organizational levels. Implementing a robust, effective, and sustainable cybersecurity risk management program will always be a foreboding challenge for program offices. Unlike decades ago, they now have to build systems that anticipate and survive a constant evolving cyber threat attack the minute systems are fielded, without the luxury of a crystal ball. Over a three and half year period, in executing over 70 cybersecurity workshops, DAU has refocused on how to best manage this dilemma versus how to solve a problem. The ability to understand this change means that learning KSAs need to be viewed and embodied as critical behaviors. In DAU's cybersecurity workshops, learners have the opportunity to practice these behaviors in rigorous case studies. Application of these behaviors beyond the classroom and back in their workplace is where the transformation begins, or where it can easily end before it begins. Without reinforcement, or time to practice, these vitally critical cybersecurity behaviors will likely succumb to the forgetting curve and place the systems they support at risk.

Background

Last year, the authors presented Part 1 and focused on a discussion on policy/directives and then explored the efficacy of the DoD's cybersecurity strategy and associated actions taken to date—all intended to safeguard the efficacy of DoD systems. The researchers intended to develop a cybersecurity approach customized for DoD acquisition organizations that characterized what it takes to implement a robust, effective, and sustainable cybersecurity program. This year, Part 2 focuses on the achievement of key cybersecurity behaviors to meet that end, including the following:

- Determining the effectiveness of security controls in support of risk management
- Evaluating the performance of security controls in support of organizational mission assurance objective
- Justifying security control development and implementation in support of organization mission assurance objectives
- Evaluating security controls at system interfaces and that span system of systems
- Appraising protection of information assets in context of a threat level for protected information assets

In addressing the above behaviors, it has become quite evident that cybersecurity for program offices is more of a dilemma than a problem. Program offices have a continual need to adapt their security posture over time to a co-evolving intelligent threat. Problems usually have solutions that can be applied to correct a risk that materialized (AKA the issue) at some point. When a car is broken, a diagnostic tool in the hands of a skilled technician can quickly determine the cause and the remedy required to return the car to working order. On the other hand, finding peace in the Middle East is a dilemma, and dilemmas cannot be solved anywhere near as easily. Instead, they require ongoing vigilance that balances a huge and complicated array of competing needs. Given its complexity, cybersecurity is a challenge where organizations need to continually test the outer edges of their learning envelopes with the understanding that there is no silver bullet.

To continue to guide this research pursuit, the authors used the same four questions to better isolate the learning implementation hurdles currently found in the DoD's Cybersecurity Strategy. The answers continue to be both informative and instructive:

1. **Have the DoD's actions (e.g., policy directives, tools, methods, etc.) met the stated and implied expectations for cybersecurity protection and resilience?** (Updated in Part 2)

The answer is still no. The DoD is vulnerable to crippling cyberattacks by cyber peers that could impose significant loss of life, equipment, and ability to execute mission.

DOT&E's assessment in their FY2018 annual report to Congress (Behler, 2019) can be summarized with the following comments:

> DOD missions and systems remain at risk from adversarial cyber operations. Operational tests continued to discover mission-critical vulnerabilities [emphasis added] in acquisition programs. (p. 229)
>
> Test and assessments in FY18 again found that low-capability attack techniques too often posed a risk for disrupting operational missions [emphasis added]. (p. 232)

The tone of the current DOT&E summary is very similar to previous warnings from their annual reports of FY15, FY16, and FY17 (Behler, 2018; Gilmore, 2017; Hall, 2017).

An uncomplimentary review provided in the March 2019 SECNAV *Cybersecurity Readiness Review* summarizes,

> 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 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)

These results are reinforced by numerous other open source reports from the DNI, the OMB, the GAO, the DoDIG, the DSB, the DOT&E, other agency inspector generals, RAND Corporation, and numerous others—a cyberattack by an advanced cyber nation states could inflict significant mission impact to the DoD and its supporting infrastructure. This conclusion can be drawn from at least 100 different reports of cybersecurity assessments over the last eight years—a sophisticated cyberattack could inflict significant impact to DoD missions, with possibly substantial losses of life, equipment, and supporting infrastructure (Coates, 2019). Current risk mitigation strategies are not tightly connected to mission assurance imperatives in the face of a growing hostile cyber environment. In 2017, a RAND study found that "cybersecurity risk management does not adequately capture the impact to operational missions nor is it designed in" (Snyder et al., 2017, p. ix). Snyder et al. (2017) went on to say that the policies governing cybersecurity are better suited for simple, stable, and predictable environments leading to significant gaps in cybersecurity risk management. Without more critical thinking about ongoing risk management of an evolving cyber threat, future studies are likely to announce the same conclusion—the DoD is vulnerable to crippling cyberattacks by cyber peers that could impose significant loss of life, equipment, and ability to execute missions.

2. **What are the metrics and have they been effective?**

The answer is still no. Extensive DoD cyber activities are not achieving measurable outcomes of secure and resilient systems. Most DoD metrics measure activity instead of outcomes of systems of system security and resilience. While there are numerous metrics that could be cited, the authors believe the following three metrics best sum up DoD cybersecurity effectiveness: (1) comments on cyber survivability from DOT&E open source annual reports to Congress; (2) the SECNAV *Cybersecurity Readiness Review* of cybersecurity risk with who has the largest Dark Web footprint of stolen sensitive data; and, (3) the number of open cybersecurity recommendations for remediation as reported by the DoD Inspector General (IG).

DOT&E Comments From Cyber Tests on Effectiveness

DOT&E has conducted over a hundred operationally realistic cyber-threat tests over the last eight years. Only a few programs during that time achieved cybersecurity survivability objectives. In the last two DOT&E open source annual reports to Congress, successful ratings included: one instance of "demonstrated a robust cyber network defense to protect against an operationally realistic cyber threat opposing force" (Behler, 2018, p. 130), two instances of "survivable in a cyber-contested environment" (Behler, 2019, pp. 49, 53), and one instance of "secure against a cyber threat having limited to moderate capabilities" (Behler, 2019, p. 15). In this and previous DOT&E open source annual reports to Congress, the more frequent ratings are

- "not survivable in a cyber-contested environment" (Behler, 2019, p. 21),
- "vulnerabilities identified during earlier testing periods still had not been remedied" (Behler, 2019, p. 23),
- "the system remains vulnerable to cyber-attack" (Behler, 2019, p. 94),
- "has cybersecurity vulnerabilities that can be exploited" (Behler, 2019, pp. 103, 105), and/or
- "cybersecurity testing identified deficiencies" (Behler, 2019, p. 144).

Please note the above instances with page references are for different systems traceable through page references. The issue is less about cybersecurity execution by a specific program and more about an ongoing trend of DoD system effectiveness against realistic cyber threats.

DoD Protection of Sensitive Information

The lack of achieving outcomes is best demonstrated by the loss of classified and controlled unclassified information (Nakashima & Sonne, 2018). A recent *Wall Street Journal* article described the armed forces under constant cyber siege by relentless foreign actors (Lubold, & Volz, 2019). The loss of sensitive information has a significant effect on the Department of Defense (DoD) for lethality and technological superiority (Mattis, 2018). Estimates on the value of losses of intellectual property from the United States are up to $600 billion (Mattis, 2018). According to the White House, "The United States cannot afford to have sensitive government information or systems inadequately secured by contractors. Federal contractors provide important services to the United States Government and must properly secure the systems through which they provide those services" (Trump, 2018, p. 7). The DoD implemented DFARS 252.204-7012 to require contractors to protect unclassified sensitive DoD information, defined as Covered Defense Information (CDI), on their networks. SECNAV (2019) concluded that "competitors and potential adversaries have exploited DON information systems, penetrated its defenses, and stolen massive amounts of national security IP. This has lessened our capabilities and lethality, while strengthening their offensive and defensive capabilities" (p. 4). The emerging DoD vision sees a shared responsibility developing between the DoD and its contractors on the protection of sensitive information regardless of its location (DoD, 2018a, 2018b).

DFARS 252.204-7012 is now applied to all new contracts and requires contractors to protect CDI on their networks. Concerning effectiveness of these activities, the metric that the SECNAV used in his *Cybersecurity Readiness Assessment* is applicable.

> While there are many ways to measure cybersecurity risk, one indicator of vulnerability is how much data about an organization is available on the Dark Web. When compared to Fortune 500 companies, the US government has the largest collective Dark Web footprint. Of the 59 government agencies, the DON led the government with the largest Dark Web footprint. (SECNAV, 2019, p. 8)

Of particular concern should be the ability for entities to detect if they are breeched. Nine of the 129 security requirements in the National Institute of Standards and Technology (NIST) concern the ability to perform audit of unusual activity on the network. In the redacted DoJ, Office of Inspector General report, *Audit of the Federal Bureau of Investigation's Cyber Victim Notification Process,* dated March 2019, "the FBI had 721 Special Agents dedicated to cyber investigations, including cyber victim notifications" (p. 1). Over the period from November 2014 to December 2017, "Cyber Guardian had 16,409 cyber incidents and 20,803 victim notifications" (DoJ, 2019, p. 12). Of special note was another revealing comment: "According to FBI personnel, victims of cyber intrusions are typically identified by the FBI or its partner agencies in the course of their investigative activities. As a result, many cyber victims, most of which are companies or organizations, are unaware that they are victims of an intrusion until the FBI notifies them" (DoJ, 2019, p. 1).

Open DoD Cybersecurity Recommendations for Remediation

The DoD tends to be a leader in the federal government and not to be forced to remediate open cybersecurity recommendations. A DoD Inspector General (IG) redacted report (DoDIG, 2019) states that "recently issued cybersecurity reports indicate that the DoD still faces challenges in managing cybersecurity risk to its network. Additionally, as of September 30, 2018, there were 266 open cybersecurity-related recommendations, dating as far back as 2008" (p. 6). As noted in our previous paper, "FISMA requires that each Federal agency conduct an annual independent evaluation to determine the effectiveness of the agency's information security program and practices" (DoD IG, 2019, p. 1). Prior independent assessment of DoD cybersecurity maturity, using the Cybersecurity Framework categories of identify, protect, detect, respond, and recover, tended to rank the DoD at the lowest levels of maturity of any federal agency (OMB, 2017). The DoD IG (2019) found that

> the DoD needs to continue focusing on managing cybersecurity activities in four of the five NIST Cybersecurity Framework functions—Identify, Protect, Detect, and Respond, primarily in the Framework categories of governance, asset management, information protection processes and procedures, identity management and access control, security continuous monitoring, detection processes, and communications. (p. 6)

3. Is the DoD headed in the right direction?

The answer is still partly. The DoD has shown a willingness to create policy and strategy. Senior leadership has been willing to examine itself in very critical ways. Several senior leaders have shown extraordinary vigilance by instituting major initiatives in cybersecurity reform including the Acting Secretary of Defense; the Secretary of the Navy; Director, Operational Test and Evaluation; Assistant Secretary of the Navy for Research, Development, and Acquisition; and Director, Defense Contracting Management Agency. Numerous operational commands are taking positive steps as well with self-reporting and taking corrective action.

> 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. [emphasis added] (Behler, 2019, p. 231)

Additionally, there have been isolated pockets of excellence within the DoD. The Army's Warfighter Information Network-Tactical (WIN-T) Increment 2 Program Office did an exceptional job of becoming a cybersecurity leader and innovator of cybersecurity acquisition and operations best practices. The Army's WIN-T Increment 2 Program Office set a high bar. The DoD's ability to assure senior leadership of mission assurance, in spite of a cyber peer threat, can be much higher once acquisition programs "demonstrate they have a robust cyber network defense to protect against an operationally realistic cyber threat opposing force" (Behler, 2018, p. 130).

A group with potential to do more for cybersecurity is the DoD Acquisition Workforce. However, SECNAV (2019) aptly noted that

> Cybersecurity is largely viewed as an IT issue and is not integrated across all operations and activities of the organization. The current approach is characterized by vertical stovepipes of responsibility which ignore the reality that information and cybersecurity require a horizontal, systems approach across all aspects of the organization's activities and operations. This horizontal approach is extremely important for without it, the DoN cannot achieve cybersecurity. (p. 7)

The DoD acquisition workforce would be well-served if it approached cybersecurity as a dilemma instead of a problem. To make matters worse, many in the acquisition community have either deflected or not fully embraced their role in cybersecurity and the need to adapt to the persistent threat. It's vitally important to elevate the acquisition community's knowledge of cybersecurity risk management through better implementation of systems security engineering, the ability to adapt to advancing threats, and integration with cyber operations. The acquisition workforce needs to transition from a "compliance construct" for cybersecurity to one of cybersecurity for operational "mission assurance." More systems might achieve in operational test adversarial assessments and fulfill operational commanders' mission assurance needs if there was a transition of approach, culture, and workforce attitudes.

The cyber threat is evolving and changing as Snyder et al. (2017) indicated:

> Capabilities of potential adversaries are growing, and the changing technologies introduce new vulnerabilities over time. This evolution means that static solutions for cybersecurity management are unlikely to be effective; cybersecurity solutions need to be adaptive. Creating defensive barriers in the form of security overlays that respond to discovered vulnerabilities is by nature insufficient to protect against future, unknown threat vectors [emphasis added]. (p. 7)

Actors with the ability to exploit the DoD's systems are growing at a staggering rate:

> 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 cyberattacks [emphasis added] across both

> critical mission systems and the multitude of supporting systems and networks that enable these missions. (Behler, 2019, p. 229)

To keep pace with the threat, the DoD acquisition workforce needs to step up their game.

4. What industry best practices should the DoD adopt and why?

There are numerous. Industry best practices have concentrated their efforts on resilience, trustworthiness and continual testing. Intel, Google, Microsoft, Netflix, major financial institutions, and other cybersecurity leaders have taken an enterprise approach to cybersecurity. Their approaches include active engagement of cybersecurity by senior leadership and robust workforce cybersecurity involvement. As stated by SECNAV (2019),

> The enterprise approach is not just about the systems and management; it also includes robust involvement by the workforce. Many companies simply fire personnel, from the C-Suite to the line level, who fail to follow established cybersecurity policy and processes. They also have very active CEO and CIO/CISO-led Cybersecurity committees and working groups that meet on a regular basis which include business unit, technology, risk management, and executive leadership. (p. 34)

Best in class cybersecurity companies have transitioned their security posture traditional security activities to emerging security concepts. Their best practices include rapid adoption of transformational emerging security technologies (such as for access management); extensive monitoring of network and system health, especially for configuration management and access management; and extensive and continual testing (extensive developmental testing, internal adversarial testing, bug bounties, etc.).

An example of an industry best practice is the “zero-trust model.” This model was a core element of the Army’s WIN-T Increment 2 security posture. SECNAV (2019) described the zero-trust architecture as follows:

> With a Zero-Trust model, successful companies have addressed both careless behaviors and malicious intent by granting trust only to those who have securely proven their identity. Having done so, their subsequent access to resources is limited to the least amount of access required. Successful Zero-Trust designs include processes that ensure all resources are accessed securely, adopt a least-privileged strategy strictly enforcing access control, and continuously monitor the enterprise ecosystem. Everyone and everything is constantly validated, with zero exemptions. (p. 36)

The more mature cybersecurity companies have a wider focus than just system protection to that of dynamic performance evaluation. The September 2016 DoD Defense Science Board report on cyber defense management recommended

> 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)

These companies have adopted a security posture of adaptability and innovative thinking in response to impending cyber threats.

Will this type of thinking eventually become pervasive in the DoD? There are isolated pockets of excellence in the DoD exhibiting the required change of approach, culture, and workforce attitudes to execute these best practices. Such a transition just needs to occur across a much wider swath of the acquisition workforce and their DoD contractors in order to respond to impending cyber threats.

Assumptions

As with any research study, assumptions generally help characterize the research constraints as well as the prevailing environmental domain. While strikingly provocative, the following (and persistent) 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 (i.e., 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.
- Politics can trump engineering. Systems security engineering is constrained in pursuing a preferred solution set due to required integration with legacy components and systems, lack of control over interfacing systems, and a preference for functionality over security.
- If user behavior is monitored and proper user behaviors can be enforced, the chance to reduce a significant attack surface is increased. Significant benefits for good user disciple: cost of implementing an effective security posture is reduced, and probability of successful detection and recovery increased. Money is a poor substitute for discipline (especially enforced user security behaviors).

Research Methodology

The researchers treated the cybersecurity skills captured in the NICE KSAs as the basis of the required critical learning behaviors. The researchers wondered what if they were treated as static, and not part of continuous process of learning and reinforcement (e.g., Monitor, Encourage, Reinforce, and Reward [MERR]). What if the acquisition workforce did not learn or retain the critical behaviors? These questions set the stage for what could be seen as more deterministic outcomes since

- Without a strong bridge in the form of metrics between what students learned in class (Level II) and what they applied in the workplace (Level III), it is more difficult to connect the two, and
- Without the evidence, organizations would be hard-pressed to confirm the resources they allocated to Level II learning gains actual paid off in the workplace.

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., MERR) to assure their Level III achievements (Kirkpatrick & Kirkpatrick, 2016, p. 56). Without them, a key feedback mechanism would be missing, and accountability opportunities would be lost. However, the more important aspect surrounds 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 Learning Level II and Learning Level III? The achievement of these Learning Level III critical behaviors represents the litmus test. Through a suitable dose of feedback (i.e., MERR), Learning Level III critical behaviors and Level IV results are more achievable later.

The Forgetting Curve

Closely tied to any learning is the unforgettable “forgetting curve,” originated by Herman Ebbinhaus (Murre, 2015). He characterized it in a simple formula:

$R = e^{(-t/s)}$, where R = Recall; e = Euler’s constant (2.71); t = time passed; and s = strength of memory.

He proved that about 80% of what we learn we forget in 30 days if there is no reinforcement (i.e., “forgetting curve”), and it still holds true today. Why is that important for cybersecurity? Aside from remembering and applying the nine framing assumptions originally described in this study, and in the context of an ever-evolving functional discipline that is more a dilemma than a problem, dismissing it would be a dangerous proposition. MERR is no antidote, but it certainly keeps the affected individuals’ consciousness on high alert, and rightfully so.

Cybersecurity Workshop Structure

To build greater cybersecurity knowledge and raise awareness for acquisition professionals, DAU conducted various workshops for diverse audiences. Figure 1 depicts the focus of these workshops and the variability between technical execution and technical oversight.

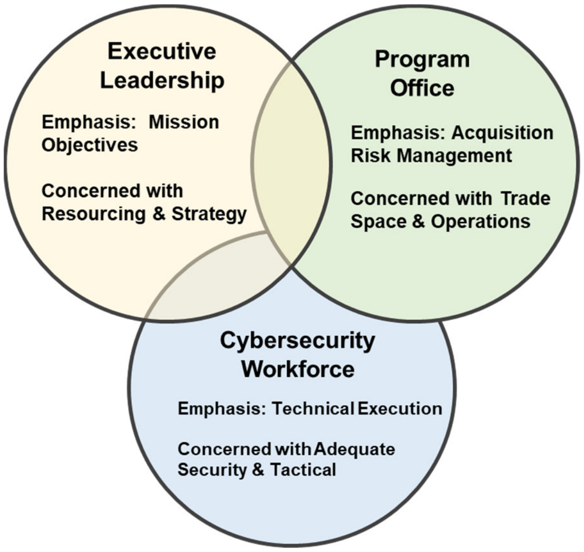
Executive Leadership
Emphasis: Mission Objectives
Concerned with Resourcing & Strategy
Program Office
Emphasis: Acquisition Risk Management
Concerned with Trade Space & Operations
Cybersecurity Workforce
Emphasis: Technical Execution
Concerned with Adequate Security & Tactical

Figure 1. Customer Composition in Workshops

The critical questions for these workshops have been: Will DAU's cybersecurity workshop enable the individual to develop a competence (either a tactic, technique, protocol, or procedure) or behavior that will enable an organizational outcome? Will the organization make a commitment in monitoring, encouraging, reinforcing, and rewarding to achieve learning gains in the workplace? Possibly the most successful of our cybersecurity workshops has been a series of three workshops over multiple days. Figure 2 covers the essence of the three workshops—NIST Systems Security Engineering, Threat-Based Engineering, and Active Cyber Defense. These workshops were designed to help the participants understand security principles, cyber threat and their tactics, and integration of acquisition with cyber operations. The compilation of these workshops addresses the horizontal issues brought up by SECNAV (2019). The SECNAV (2019) well understood that cybersecurity requires "a horizontal, systems approach across all aspects of the organization's activities and operations" (p. 7).

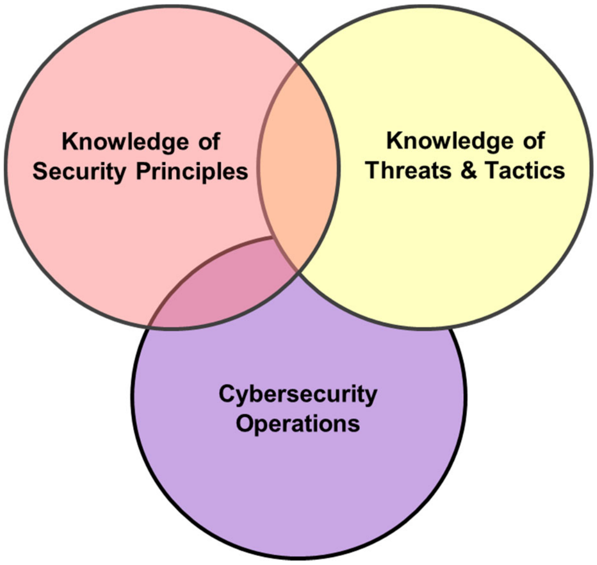
Knowledge of Security Principles
Knowledge of Threats & Tactics
Cybersecurity Operations

Figure 2. Types of Cybersecurity Workshops

The NIST Systems Security Engineering (SSE) uses the NIST 800-160 (Vol. 1 & 2) to cover the standards and constructs of system trustworthiness and system resilience. The NIST SSE workshop was designed to give the participants time to apply best practices outlined in NIST publications 800-160 (Vol. 1 & 2; Ross, McEvilley, & Oren, 2017; Ross et al., 2018). Three core behaviors are taught and practiced in the NIST SSE workshop:

- Construct a comprehensive and holistic system view while addressing stakeholder security and risk concerns;
- Apply input to analyses of alternatives and to 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.

NIST has done an exceptional job of understanding standards and techniques and developing a core process in each of the various volumes. For example, Ross et al. (2017) state,

> The ultimate objective is to address security issues from a stakeholder requirements and protection needs perspective and to use established engineering processes to ensure that such requirements and needs are addressed with the appropriate fidelity and rigor across the entire life cycle of the system. (p. viii)

For system security engineering trustworthiness, our desired outcome is to develop and demonstrate the evidence necessary to support assurance claims and to substantiate the determination that the system is sufficiently trustworthy. Ross et al. (2018) note that “the ultimate objective is to obtain trustworthy secure systems that are fully capable of supporting critical missions and business operations while protecting stakeholder assets, and to do so with a level of assurance that is consistent with the risk tolerance of those stakeholders” (p. ix). For system security resiliency, the desired outcome is focused on designing security risk management activities, producing related security risk management information, and advising the engineering team and key stakeholders on the security-relevant impact of threats and vulnerabilities to the mission/business supported by the system.

This is the pre-course email sent to the workshop participants:

> You will do a capstone case study as part of a team for either system trustworthiness or system resiliency. While we have case studies for you to work on—if you should desire to nominate a project that you are working on as either a trustworthiness or resiliency exercise—we will accommodate it. The only caveat is that the training is being executed in Unclassified spaces. We have done other DoD systems as exercises (either trustworthiness or resiliency) in previous SSE workshop sessions in unclassified spaces. Please talk to me on day 1 with your proposal. I suspect there is a high probability that we can figure out how to make it work.

The participants nominate a problem they have in their environment. The goal is to help participants understand how to implement the standards and techniques to achieve an outcome through a series of exercises and case studies. The capstone exercise validates whether their system is trustworthy and resilient.

In the NIST SSE workshops, participants raised the following issues that they felt have limited their ability to execute a particular security standard and/or resilience technique:

- Can I change the design/architecture?
- Can I change configuration?
- Ability to manage interfaces?
- Can I contain/isolate/segment trust relations?
- Can I implement new processes?
- Can I automate a process?
- How will I monitor & enforce user behavior?
- Can I trade off/restrict functionality?
- What capability will a newer technology provide (will my users be able to implement the technology)?

The fact that these types of questions are occurring in the workshop case studies is very encouraging. The next step is to follow up with the workshop participants to ensure the behaviors of construct, apply, and evaluate are underway at their workplaces. There's no guarantee that the learners will have enough opportunities to apply everything they learned in the workshop. What needs to happen in the workplace to combat the likely consequences of forgetting curve? Without a coach or mentor, how do they get to the point where they sustain the cognitive connection to the original learning behavior—and how do we measure it? The workplace has to establish surrogate scenarios that refresh and reinforce the critical learning behaviors—and what tools are the most appropriate.

Results and Findings

Individuals enter the workshops with a wide variance of cybersecurity experience and knowledge levels—novice to experienced practitioner. There seems to be several revelations that occur during a workshop that would likely increase the chance that a student will apply appropriate risk management and security engineering constructs and behaviors to their situation after the conclusion of a workshop. Students progress through the following stages: understanding cybersecurity is a severe security threat; acknowledging the cyber threat is not static, but evolving; accepting that their system/program needs to do something about evolving cyber threats; adapting their cybersecurity security posture if the cyber threat changes; committing to cybersecurity risk management as a continual, ongoing effort; and becoming an effective agent of change to achieve meaningful outcomes. Depending on the maturity of the student and their organization, individual progression can stop at any point in the cycle of progression. During these workshops, the following common themes surface:

- Workshop participants usually start the workshops looking for prescriptive answers. They hope to find a fix to their cybersecurity problem.
- The initial focus is frequently satisfying some external entity. The most common DoD focus is to satisfy an Authorizing Official (AO). More advanced programs will set a goal of succeeding against a capable adversarial assessment sponsored by a DoD Operational Test Agency (OTA). While both are worthy objectives, their real focus should be one of mission assurance.
- Often, they are not creating a solution set that can adapt if the threat should change. Most want to stop after finding a single possible solution, instead of creating a solution set.
- They want to make the threat static and then optimize to a static threat. Accepting an evolving threat is a significant strain on people and resources.
- They need to achieve a construct of self-assessment and continual testing—such that achievement of either an ATO/ATC or passing an OTA assessment—are just part of an ongoing process for cyber risk management to achieve mission assurance.

The core question simply stated became "What initial successes will likely occur as you consistently apply what you learned?" In the researchers' Part 1 of this study, we examined the Western Naval Audit Service in learning and applying critical cybersecurity behaviors from our workshops. This particular group was highly motivated and had committed leadership. Kirkpatrick calls it having required drivers (i.e., monitor, encourage, reinforce, and rewards) to assure their Level III achievements (Kirkpatrick & Kirkpatrick, 2016, p. 56). Since their initial series of cybersecurity workshops, this group offered to the SECNAV's office to bid for a cybersecurity audit. The SECNAV assigned Western Naval Audit Service a critical audit issue concerning fleet cybersecurity readiness. This audit is underway and should be back to the SECNAV's office for review before the end of 2019. To go from no cybersecurity audit experience to conducting a major fleet readiness cybersecurity audit review was a major commitment by this group and the start of objective measurable outcomes in the form of secure and resilient systems.

Across multiple workshops, we have seen statistically significant changes in attitudes towards the behaviors. The following qualitative comments across various workshops summarize the trend seen across the workshops.

- Participant 1—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 …
- Participant 2—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.
- Participant 3—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 …
- Participant 4—This workshop helped me better understand the requirements and how to convey that importance to our customers …
- Participant 5—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. …
- Participant 6—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 …
- Participant 7—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 …

From the above comments, the described student progression can be seen. These participants are starting to understand cybersecurity is a severe security threat, acknowledging the cyber threat is evolving, accepting their responsibility to do something, adapting their cybersecurity security posture, and committing to ongoing cybersecurity risk management. If these participants receive reinforcement from their organization, there is a significant probability for meaningful outcomes to occur. If we can start to have more of the acquisition workforce to exhibit the same types of attitudes – our operational forces might have a chance against when facing a cyber peer.

Conclusion

The number of cyber threat actors who have the ability to exploit the 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 inescapable and impending cybersecurity threats. Admittedly, the danger signs are very telling, and they're not good.

In Part 2 of this research project, the authors reinforced how behaviors learned in workshops could be instituted in a participant's work environment. The researchers posit that the DoD will be hard-pressed to achieve the desired mission assurance objectives for security and resilience without recognizing that (1) cybersecurity risk management and security engineering critical learning behaviors require commitment at all levels—individual, team, and organizational; and (2) cybersecurity is a domain that must be viewed as a dilemma where there is no one-size-fits-all solution, nor can it be treated as a static problem. Cybersecurity threats will never wane in frequency or severity. Its asymmetric nature is too great. Without constant vigilance, the United States will lose the cybersecurity war.

Thankfully, the commitment from numerous senior DoD leaders is growing. Outside the DoD, there has been a willingness from numerous organizational leaders (e.g., the intelligence community, DOT&E, IG, audit service, chartered boards, think tanks, etc.) to take similar action. And programs like the WIN-T Increment 2 Program Office have demonstrated what it takes to achieve cybersecurity excellence at a given juncture. If the remaining acquisition workforce steps up to the cybersecurity learning challenge, the negative trends discussed at the beginning of the paper might just start to reverse course, resulting in a much more favorable heading.

References

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

Behler, R. (2019). *Director, Operational Test and Evaluation FY 2018 annual report.* Washington, DC: DoD. Retrieved from https://www.dote.osd.mil/pub/reports/FY2018/

Coates, D. (2019). *Worldwide threat assessment of the U.S. intelligence community*. Retrieved from Director, National Intelligence website: https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

Defense Federal Acquisition Regulation Supplement (DFARS), 48 C.F.R. 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (2016).

DoD. (2018a). *Fact sheet: 2018 DoD cyber strategy and cyber posture review.* Retrieved from https://media.defense.gov/2018/Sep/18/2002041659/-1/-1/1/Factsheet_for_Strategy_and_CPR_FINAL.pdf

DoD. (2018b). *Summary: Department of Defense cyber strategy 2018*. Washington, DC: Author. Retrieved from https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.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

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

DoD Inspector General. (2019). *Summary of reports issued regarding Department of Defense cybersecurity from July 1, 2017, through June 30, 2018.* Retrieved from https://media.defense.gov/2019/Jan/11/2002078551/-1/-1/1/DODIG-2019-044.PDF

DoJ. (2019). *Audit of the Federal Bureau of Investigation's cyber victim notification process.* Retrieved from https://oig.justice.gov/reports/2019/a1923.pdf

Geurtz, J. (2018). *Implementation of enhanced security controls on select defense industrial base partner networks.* Washington, DC: Assistant Secretary of the Navy for Research, Development, and Acquisition.

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

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

Lubold, G., & Volz, D. (2019). Navy ‘under cyber siege’ by Chinese hackers. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/navy-industry-partners-are-under-cyber-siege-review-asserts-11552415553

Mattis, J. (2018). *Establishment of the Protecting Critical Technology Task Force* [Memorandum]. Washington, DC: Secretary of Defense.

Murre, J. M. J., & Dros, J. (2015). Replication and analysis of Ebbinghaus’ Forgetting Curve. *PLoS One, 10*(7). Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4492928/

Nakashima, E., & Sonne, P. (2018). China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html?noredirect=on&utm_term=.8836302b51d5

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

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

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

Ross, R., Graubart, R., Bodeau, D., & McQuaid, R. (2018). *Systems security engineering: Cyber resiliency considerations for the engineering of trustworthy secure systems* [Draft, NIST Special Publication 800-160 Volume 2]. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf

Ross, R., McEvilley, M., & Oren, J. (2017). *Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems* [NIST Special Publication 800-160, Vol. 1]. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf

Secretary of the Navy (SECNAV). (2019). *Cybersecurity readiness review.* Retrieved from https://www.navy.mil/strategic/CyberSecurityReview.pdf

Snyder, D., Power, J., Bodine-Baron, E., Fox, B., Kendrick, L., & Powell, M. (2017). *Improving the cybersecurity of the U.S. Air Force military systems throughout their life cycles.* Retrieved from https://www.rand.org/pubs/research_reports/RR1007.html

Trump, D. J. (2018). *National cyber strategy of the United States of America*. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

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

www.acquisitionresearch.net