



SECRETARY OF THE NAVY CYBERSECURITY READINESS REVIEW



MARCH 2019

THIS PAGE INTENTIONALLY BLANK

4 March 2019

From: The Honorable Michael J. Bayer
Mr. John M.B. O'Connor
Mr. Ronald S. Moultrie
Mr. William H. Swanson

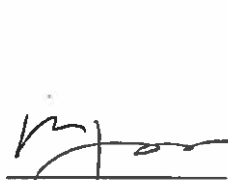
To: Secretary of the Navy

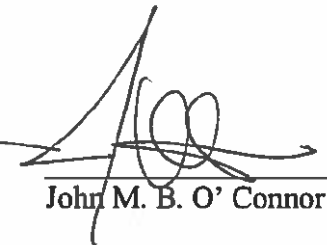
Mr. Secretary:

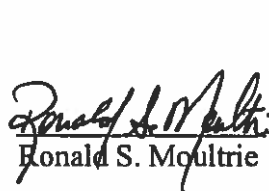
This report is in response to your request to conduct an independent Cybersecurity Readiness Review following the loss of significant amounts of Department of the Navy data. Attached are the findings of that review along with specific recommendations for your consideration as you determine the way ahead for the nation's Navy.

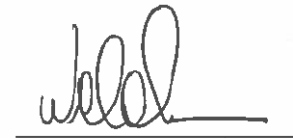
The review examined cybersecurity at the governance layer and identified five critical pillars key to cybersecurity readiness: culture, people, structure, processes, and resources. The team interviewed dozens of senior military leaders as well as Chief Executive Officers, Chief Operating Officers, Chief Information Officers, and Chief Information Security Officers from several *Fortune* 500 companies with deep experience in implementing successful cybersecurity measures following significant incidents of their own. We identified best-practices in both government and private sector organizations who are demonstrating success in contending with cyber threats.

The review team thanks you for the access granted to us and extends our sincere appreciation to the many senior leaders who shared their candid views of the cybersecurity challenges. The team would also like to thank the numerous industry partners who shared their individual journeys to achieving greater cybersecurity. Finally, none of this would be possible without the tremendous support of the staff assigned to the team. Their expertise and commitment was invaluable in producing this report. They represent the passion and talent that will be required to implement the recommendations in this report to ensure the nation has the Navy it needs.


Michael J. Bayer
Chairman


John M. B. O'Connor


Ronald S. Moultrie


William H. Swanson

THIS PAGE INTENTIONALLY BLANK

“If you’re asking me if I think we’re at war, I think I’d say yes” ...We’re at war right now in cyberspace. We’ve been at war for maybe a decade. They’re pouring oil over the castle walls every day.”¹

--Gen Robert Neller, Commandant, USMC, 21 Feb 2019

¹ Seffers, 2019, Kinetic Weapons Remain a Priority as Cyber War Rages, 1

Table of Contents

Forward	1
Scope and Methodology	2
Chapter 1: Introduction	4
Economic Security, National Security, and Cybersecurity	4
The Eroded Military Advantage	5
The Department Today	6
DIB Observations and Vulnerabilities	8
What Follows	9
Chapter 2: Culture	10
The Role of Culture as a Governance Tool to Achieve Cybersecurity	10
Culture Best Practices	10
State of Today’s Naval Service Culture	12
Culture Recommendations	14
Chapter 3: People	17
The Role of People as a Governance Tool to Achieve Cybersecurity Resiliency	17
People Best Practices	17
State of Today’s Naval Service People	18
People Recommendations	23
Chapter 4: Structure	26
Role of Structure as a Governance Tool to Achieve Cybersecurity Resiliency	26
Structure Best Practices	26
State of Today’s Naval Service Structure	27
Structure Recommendations	31
Chapter 5: Process	33
The Role of Process as a Governance Tool to Achieve Cybersecurity Resiliency	33
Process Best Practices	33
State of Today’s Naval Service Process	37
Process Recommendations	44

Chapter 6: Resources	49
Resources Best Practices	49
State of Today’s Naval Service Resources	52
Resources Recommendations	54
Final Thoughts	57
Appendix A	58
SUBJECT: Cybersecurity Review Tasking Memo	58
Appendix B	60
List of External Organizations Consulted	60
Appendix C	62
List of DoD Personnel Consulted	62
Appendix D	63
Cybersecurity Readiness Review Team	63
Appendix E	64
Acronym List	64
Bibliography	66

Forward

This report is the product of many minds, each of whom brought a unique perspective to its construction. Typically, this sort of effort is like others; there is a thesis asserted, discovery is conducted, findings are developed and finally, recommendations are created. However, as we did our work, we came to realize there were several big ideas necessary to wrap one's head around for the challenges of cybersecurity and for its solutions to make sense.

In prior eras, for good or ill, navies shifted their definition from wood to steel to wing, or from sail to steam and beyond. This time technology, not the naval service, or its opponents, have imposed a definition of what navies must be for the rest of the 21st Century. Nothing the Navy or Marine Corps does, or will do, can exist without it. It is the keystone of capability and survival. Navies must become information enterprises who happen to operate on, over, under, and from the sea; a vast difference from a 355 ship mindset. Today, knowing and living what business the Department of the Navy is in, is essential.

The current global struggle, like the old, is without domain boundaries or a terminus in time. Therefore, outcomes must be assessed over decades of moves and counter-moves, of investment and counter-investment, and not as a one round fight. This struggle for global influence and domination is enabled by sovereign wealth capacity. Everything the DON does has to be about the wise application of scarce resources towards capability, and the effect those capabilities have on imposing costs on its rivals.

In time, this era's opponent will overmatch our nation in manpower, industrial capacity, intellectual capital, and eventually financial resources. We, not they, stand to become the near-peer. Given this relative erosion of US dominance over time, every differentiating idea or intellectual product gained or lost is material. More importantly, in the years to follow, it will have compounding effects in advantage or disadvantage. That reality demands every bit of relevant intellectual property (IP) must be defended, but the relevant IP to be protected must expand beyond what we now protect, to that which our rivals want.

This is just not another challenge to be resourced. The failure to protect Navy and Marine Corps information systems and IP is an existential threat to their existence. To the extent the DON assesses its performance in this realm, it judges itself against and ahead of the private sector and its sister services. We do not believe either to be true. The DON should be assessing itself against the best of the private sector and its global rivals.

We find the DON preparing to win some future kinetic battle, while it is losing the current global, counter-force, counter-value, cyber war. Knowing and acting on that new reality is essential for the DON.

The Secretary of the Navy was correct to question if the current cybersecurity governance structure was optimally focused, organized, and resourced. We find it is not. What follows are best practices and solutions that can put the DON on the right path. Getting this right and underway can only be done by those who govern the Navy and Marine Corps.

Scope and Methodology

Scope

On October 12, 2018, the Secretary of the Navy (SECNAV) directed a comprehensive cybersecurity review following several significant compromises of classified and sensitive information.² The task was to examine the Department of the Navy (DON) current cyberspace governance structures to assess if they are optimally focused, organized, and resourced to prevent or mitigate future incidents. The team was specifically directed to examine the DON cybersecurity posture as well as the organizational and industrial environments in which previous events occurred. Finally, the review team was charged with investigating end-to-end cybersecurity processes to assess the alignment of authority, accountability, and responsibility within the DON.

To fully understand the current cybersecurity posture, this review examined the shift of national defense strategy, to include past and present information strategies, cyber strategies, cyber policies, and guidance across all elements of the government that has occurred since the 2017 National Security Strategy and 2018 National Defense Strategy's acknowledged return to global peer rivalry.

The DON handles and uses information in a manner consistent with its importance in today's security environment. Cyber operations, intelligence support, Command and Control (C2), organizational structure, integration of cybersecurity in warfare systems, and evolution of the fiscal environment all influence how the DON handles data. As such, the review specifically examined the workforce, culture, structure, processes, and resources with respect to authority, accountability, risk management, and budgetary tradeoffs within the Department. The review examined the career paths for cybersecurity professionals, manning trends, training architectures, assimilation of advanced technologies, and threat information exchange. These elements were evaluated and assessed for their cumulative effect on the DON's ability to secure data, use information in warfare, and evolve with the pace of technological advancement as a core element of strategy among an environment of great power competition and incidents that occur below the threshold of kinetic activity.

The review also included an examination of supporting Defense Industrial Base (DIB) cybersecurity practices and their ability to secure DON critical information. The review looked at control measures, capabilities, and resources available to secure DON information as well as mandated requirements for the DIB when doing business with government.

The review examined the evolution of the importance of technology-enabled-information and the derivative importance of cybersecurity on naval and marine operations, the Department's understanding of that impact, and how the reemergence of great power competition has altered the definition of success.

² Spencer, 2018, Cybersecurity Review

Finally, the review was not an investigation of the specific facts and circumstances surrounding recent incidents of data loss. Rather, it was a review of those key elements available to DON's governance enterprise for subsequent action - culture, people, structure, process, and resources. This is essential to understanding how those charged with governance can best move the DON away from reactive practices that have left information vulnerable to attack or theft, underestimated the scope and scale of vulnerability, overlooked the long-term impact of compromised systems, and the compounding effect of neglected Navy and Marine Corps critical infrastructure, from the consequences of accepting too much risk in unsecured warfare and essential supporting combat systems, and from underestimating the potential of malicious insider activity.

Methodology

The work commenced with a comprehensive review of the nature and aspirations of the threat, the totality of recent cybersecurity incidents, and the known-unknown incidents. The review then examined the both the National Security Strategy (NSS) and the National Cyber Strategy (NCS) as the guidance provided to the Department of Defense (DoD), and in turn to the DON, regarding how, and by what means, the cyber threat should be addressed. After a thorough review of the current security environment and the strategic guidance to the DoD, the Review sought a better understanding of the factors that drove DON decisions and actions of the past that resulted in the DON's current cybersecurity readiness and posture. Research was conducted into current and past policies and practices governing cybersecurity. The team interviewed current senior military officers and civilians from across the DoD and DON.

The review examined the best cybersecurity practices being employed within the government to include how they identified breaches, shared information, and trained their workforces, structured for success, maintained threat situation awareness, prioritized resources, and communicated the importance of cybersecurity throughout their organizations. The review also examined best practices within the private sector. Chief Executive Officers (CEOs), Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), Chief Risk Officers (CROs), and various subject matter experts were interviewed to obtain insight into how they anticipated threats, the actions they took when confronted with similar situations, and the strategies employed in the aftermath of significant cyber events. Particular attention was paid to organizations and environments where information security is vital to their operations, and their success has been dependent upon effective cybersecurity governance, strategies, policies, and execution.

The review conducted 85 interviews and 31 site visits, examining various aspects of cybersecurity (Appendices B, and C).

Chapter 1: Introduction

Economic Security, National Security, and Cybersecurity

America once won wars with overwhelming manpower, then later won with superior industrial might, and with the Cold War, won with better technology. Against today's adversaries who now possess these once uniquely American national capabilities at peer or near-peer levels, these capabilities are no longer guarantors of American success. Further, in the current struggle for global influence and dominance, US economic strength has been materially eroded by years of tolerated, massive commercial Intellectual Property (IP) theft. Those economics matter to the Navy and Marine Corps. Cicero noted centuries ago, the sinews of war are nourished by a strong treasury.

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. Over the longer term, as Cicero noted, relative military capability is a correlate to relative economic power. The erosion of US economic strength resulting from the national losses of IP will, in the future, further weaken US military capability as our competitors will be capable of funding their growth at a relatively faster rate. The interconnectedness between economic strength and military power makes every advantage gained or lost through IP exfiltration, exponentially consequential over time. It is this war before the war, and its consequential impact on outcomes to be, that is the existential threat to national security.

This cyber war has been ongoing for some time. The threat is long past the emergent or developing stage. While its "guns" go unheard, it is as real, and with as or more devastating consequences. This war is manifested in ways few appreciate, fewer understand, and even fewer know what to do about it. The DON and the nation have been slow to awake to the reality that we are in a multi-decade struggle for influence that is having a direct impact on our national destiny. There are many bad actors, but China and Russia in particular have focused their efforts in strategic ways and are executing at scale to achieve their objectives, while the US remains relatively flat-footed, and is too often incapable of defending itself. Meanwhile, both China and Russia are executing well developed cyber-enabled regional and global "grey zone" unconventional strategies against the US and its allies.

These are not "unknown, unknowns," China has been very explicit in stating their goal of becoming the world's dominate superpower through a comprehensive set of strategies including their commitment to acquiring critical US and allied IP through acquisitions, foreign business restrictions, and cyber enabled theft. By some estimates, economic espionage is costing the US \$400B annually and has cost approximately \$1.2 trillion since 2015.³ However, the review assesses these numbers to be a fraction of the actual thefts. China has effectively used stolen IP to grow its gross national product (GNP) and has derived an incalculable near and long-term military advantage from it, thereby altering the calculus of global power. At present, China's GNP has grown to roughly two-thirds of America's, trending to their economy equaling the US

³ The National Bureau of Asian Research, 2017, IP Commission Report

by the middle of the next decade. By mid-century, China's economy is projected to be 50 percent larger than the US economy.

Russia has been employing cyberwarfare against their adversaries for more than a decade. Russia seeks to influence and restore their global power through cyber activities that undermine support within targeted democratic governments and institutions. They have employed cyber-attacks against other countries' financial institutions, communication networks, election commissions, and social media networks. Their strategy also includes using cyber tools to directly impact the outcome of regional conflicts, and to intimidate former Soviet Union states by tampering with or controlling those states' critical infrastructure.⁴

China and Russia carefully meter their cyber warfare against the US so as to not trigger a national response. As but one example, their conduct of gray zone operations is carefully conducted at or below the US threshold of triggering a kinetic response. This enables them to achieve superiority "left of phase 0" and achieve their goals without incurring a kinetic consequence.

These complex and dynamic cybersecurity challenges have been years in the making and can be traced to a national miscalculation of the shifting intentions and capabilities of our competitors. Although our systems were known to be vulnerable, there has been a long-standing belief that the open systems in this country would be relatively untargeted for the near future. This belief severely underestimated both the growth of technology that enabled cyber-crime, espionage, and malicious activities, and the shift in our rivals' intentions and aspirations from benign to malicious. In combination, this enabled competitor states to gain significant advantage by exploiting our openness while building closed and well defended systems of their own.

If the current trend continues unimpeded, the US will soon lose its status as the dominant global economic power. That loss of relative economic power foreshadows the Navy and Marine Corps becoming relegated to being a near-peer. As a near peer, every asymmetric advantage becomes magnified and more valuable in a future fight, and every advantage lost the more intolerable. Alarming, near peer status may have already been reached if one truly considers the disruptability of the critical enabling infrastructure necessary to mobilize the nation and actually get forces to and sustained in a true peer-on-peer fight.

These facts, juxtaposed against significant information losses the DON has experienced in the past few years, contribute directly, and significantly, to a loss of naval advantage on land, in the air, and on and below the seas.

The Eroded Military Advantage

The growing decline in economic advantage via the exploitation of our open economic system has similarly been accompanied by an erosion of the US military advantage via the theft of critical information on weapon systems, advanced technologies, and unique capabilities and

⁴ Windrem, 2016, Timeline: Ten Years of Russian Cyber Attacks on Other Nations, (NBC News, 2016), 2

systemic and individual human vulnerabilities. The systems the US relies upon to mobilize, deploy, and sustain forces have been extensively targeted by potential adversaries, and compromised to such extent that their reliability is questionable. Supervisory Control and Data Acquisition (SCADA) systems, strategic and tactical communications, and logistics systems are of uncertain utility given the well-recognized vulnerabilities inherent and threat created in those systems.

The DON's dependency upon the DIB presents another large and lucrative source of exploitation for those looking to diminish US military advantage. Key DIB companies, primes, and their suppliers, have been breached and their IP stolen and exploited. These critical supply chains have been compromised in ways and to an extent yet to be fully understood.

Long-term, US future military advantage is being diminished by years of IP exfiltration from the DoD, DON, and DIB, all with little to no adverse consequences to the thieves. Long-term military advantage is also being further eroded as the indigenous innovation capabilities of China begin to grow at an exponential rate. Such innovation was formerly viewed as a nearly unique US advantage, but their rapidly expanding innovation capabilities are remarkable. In sum, the Review found that the national security enterprise, which has well observed, but not altered, these patterns with an effective response, is not correctly organized or postured to deal with this long-term struggle.

The Department Today

Today the DON, like the DoD and its sister Services, is exquisitely organized, structured, equipped, and cultured for a previous era. After the Cold War, the dissolution of the Soviet Union and the fall of the Berlin Wall, the DoD and DON enjoyed nearly 25 years of operating in an environment where there was no peer challenging US national security dominance. In fact, until the terrorist attacks of 9/11, the country had decided it was at end of the line of history and large standing militaries were no longer relevant. The national focus was on harvesting a peace "dividend" by reducing the size of the military by more than half its Cold War size.

Following 9/11, the US military became laser focused on counterterrorism, to the detriment of other threats. Peer engagement capability continued to decline in attention and readiness. Yet, over those 25+ years of shrinking forces, the size and complexity of the institutional overhead at DoD and DON expanded remarkably. That expansion was able impose a myriad of people, rules, and processes that facilitated the ever-expanding bureaucracy. Lacking the traditional competitive pressures that serve to limit bureaucratic growth in other sectors, in defense there was no competitors to benchmark and expose the imposed drag. The consequential cultural shift to the minimization of risk to the enterprise, vice the traditional war time focus on minimization of risk to the forces, resulted in the pursuit of no risk, safe development of marginal capability or marginal process improvement, all at the cost of material breakthroughs.

That massive bureaucracy, too evolved to its own ends, is now confronted with a new reality; a competitively informed, peer driven threat and risk, all enabled by technology that is evolving beyond the bureaucracy's grasp. Its reaction to all this has been to assert that what it

needs for this fight is what it had previously decided was appropriate for the earlier world, but in slightly larger quantity.

In today's era, where the dependency on information technology (IT) is central to success in any future conflict, the DON's institutional reluctance to shift its focus from ship or platform centric, to information centric, in order to attend to the world of vulnerabilities presented by its adversaries' capabilities growth and sophistication is striking. The bureaucracy's inability to get ahead of the threat best sums the heart of the problem, which is why this Review calls for the enterprise's governance to reconfigure its culture to adapt to this new world.

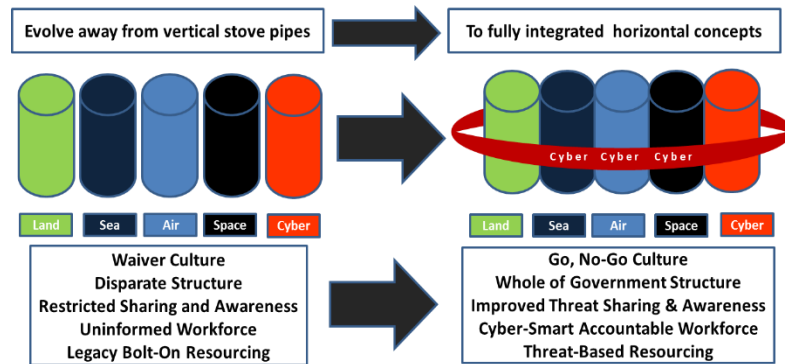


Figure 1: "Vertical Stovepipes." Cyber is currently regarded as a separate effort that does not affect the land, sea, air, and space domains. "Horizontal and Vertical Cyber Integration." Some elements of the cyber domain are distinct, other warfare domains include elements of the cyber domain.

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.

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. This systems approach must anticipate, defend, detect, isolate, mitigate, respond, and learn as a means to maintain network resiliency and preserve continuity.

This stovepipe approach is further disadvantaged by global technology evolving at a rate far faster than the DoD is capable of absorbing. In contrast, our global rivals, differently organized, have enterprises that have demonstrated the capability to adapt and incorporate these new technologies at a much faster rate than the DoD. Once, the DoD and the DON were viewed as leaders in the development, adoption, and protection of IT. Tragically, this is no longer the case. The decades of disinvestment in US national systems have also created additional vulnerabilities, contributing to a downward spiral in capabilities.

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

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.⁵ The military and the civilian infrastructure that supports the warfighting capability are equally vulnerable.

DIB Observations and Vulnerabilities

The industrial base necessary to support the DON warfighting enterprise must be a critical partner in this global struggle. However, this includes a significant number of necessary key industrial and utility commons ecosystems that are no longer centered or owned in the US, such as advanced composite materials or national telecommunications infrastructures. There are also those traditional companies thought of as the DIB that are US owned or domiciled, which are supported by a supply chain that includes sub-contractors that are not US owned or domiciled. For years, global competitors, and adversaries, have targeted and breached these critical contractor systems with impunity. These enterprises, regardless of their relationship with the Department, are under cyber siege, not because they are important to the DON, they are under siege because of their vital importance to our global rivals. The Department has relied on long standing security constructs based on information sharing and self-reporting to inform it of its supplier's vulnerabilities and breaches. That after the fact system has demonstrably failed.

Despite our adversaries' clear statements of intent, the DON did not anticipate this attack vector. As the DIB is not viewed as a partner by the DON, the DIB was not adequately informed of the cyber threat. We believe there is ample evidence that the industrial base is not composed of individuals who want to see their hard-earned IP stolen by anyone. They are as motivated as any member in uniform to protect what is theirs. Understanding this common natural interest, and informing them of threats early and often, will serve to unleash their creativity in forming defenses and getting ahead of the problem. Further, animated by their financial interest in their IP, once informed, they are more likely to anticipate and develop their own protective measures.

Because of the scarcity of resources available, and the limitations of the available art and science of detection, the DoD and DON have only a limited understanding of the actual totality of losses that are occurring. Only a very small subset of incidents are "known" and of those known, an even a smaller set are fully investigated. This has led to lengthy timelines and processes for discovering, reporting, and assessing information losses. That knowledge is often hyper classified and difficult to share, sometimes leading to an alarming lack of understanding and appreciation of the threat. Finally, in an age where it is impossible to protect everything, identifying what information must be absolutely protected is vital and not being adequately accomplished.

⁵ Dark Owl, The Dark Owl Index US Government Edition: Ranking US Government Agencies Using Darknet Intelligence

What Follows

This review took a systems approach and examined best practices within the government and the private sector. It assessed the current cybersecurity situation across the DON and makes specific recommendations for the leaders at the governance level regarding culture, people, structure, processes, and resources. These are levers that can only be adjusted by those at the governance level, the leaders at the very top of an organization. In the DON that is the Secretary, the Chief of Naval Operations (CNO), and the Commandant of the Marine Corps (CMC). All these pillars are critical for success and are interrelated. They are also those that have the most significant and sustaining impact when meaningful change is required. Most importantly, they enable the necessary changes that must occur within lower organizational levels. These executive levers can drive lasting change in information resiliency, cybersecurity, readiness, lethality, and survivability.

The review found CEOs of the best enterprises understand that they are being targeted every day in cyberspace. They take an enterprise approach towards cybersecurity and are personally engaged and consistently communicate expectations. They select leaders that understand the threat and set priorities and incentives that reflect the centrality of information to the success of their operations. They hold everyone accountable for cybersecurity and therefore demand education, training, and constant testing of their workforce at every level. They establish clear and enforceable standards and set the priorities for what information must be protected. They have strong, empowered CIOs that are accountable and report directly to them. They establish organizational structures and processes that optimize alignment of responsibility, authority, and accountability. They maintain good situational awareness of their organizations' cyber-health and require and use dashboards and scorecards to predict and monitor performance. They mandate the use of simulations and threat modeling to train their personnel and prepare for "0" day events. The most successful CEOs factor cybersecurity into every decision they make.

What follows is what was found in their best practices, the current state of the DON, and how those crucial best practices can be applied to the Navy and Marine Corps and their supporting enterprise.

Chapter 2: Culture

The Role of Culture as a Governance Tool to Achieve Cybersecurity

Organizational culture is the underlying beliefs, assumptions, values, and ways of interacting that contribute to the unique social and psychological environment of an organization.⁶ Beginning with the Chief Executive and then down, leaders are key to the creation, maintenance, and communication of organizational culture.

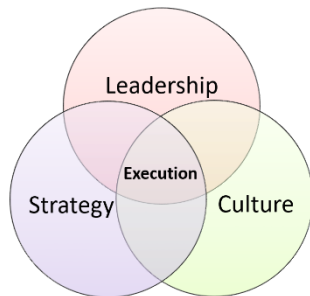


Figure 2: Successful execution within an organization occurs when Leadership, Strategy, and Culture align.

Experienced executives understand a strong culture always trumps strategy. However, when combined, a strong culture and thoughtful strategy become the key ingredients to execute efficiently and effectively as well as make and sustain meaningful change. Although burdened with an oversized institutional bureaucracy, the naval service enjoys a strong historical culture characterized by its core values of honor, courage, and commitment. Further, it has a clear mission to maintain an enduring maritime competitive advantage for the United States of America. For centuries, Sailors, Marines, and civilians have never let this mission fail, always committed to the service of something greater than their own self-interest. This same commitment needs to inform how the cybersecurity mission is viewed and executed across the Navy and Marine Corps enterprise. To preserve a lethal maritime force cybersecurity must be deemed an all-hands on deck evolution of individual cyber hygiene, effective configuration management practices, constant and complete system updates, and prompt mitigation of network vulnerabilities to long term design, test, evaluation, procurement, fielding, and operation of warfighting systems.

Culture Best Practices

The best corporate and government organizations have embraced the new information-centric environment wherein data, IT systems, structures, and processes are essential to their success and existence. Private sector commercial and financial institutions now view their information systems and capability as being their core business asset, a massive shift from their traditional self-view as a banking or insurance enterprise. Industry refers to this as “digital transformation” and they have forcibly and quickly incorporated this reality into their corporate strategies. Corporate leaders ensure every member of their organization understands precisely what business they are in and what that means for their role in the organization. They verify that individual and group behaviors are accordingly aligned to achieve measurable outcomes. Focused senior leadership engagement and consistent reinforcement of expectations establishes and maintains a culture that values relentless technology modernization and vigilant data protection on par with their revenue generation. Evidence of this shift is manifested in actions and words throughout their companies from bank tellers to directors of the board. Internal processes and investment decisions reflect this shift with technology risk evaluation being closely aligned to the company’s existing enterprise risk management framework (RMF). With

⁶ The Business Dictionary, 2019

the centrality of information clearly set in the culture from the top down, the cyber threat is then viewed as real and existential to the life and livelihood of the enterprise. Those realities, inculcated into culture, drive risk behaviors and resource allocation decisions across the enterprise.

The best CEOs are deeply informed, engaged, and holding their organization accountable for information resilience and cybersecurity. A key part of each day is anticipating and getting ahead of the competition by knowing the next moves in technology, or the next competitive threat or opportunity. To maintain network resiliency and preserve business continuity, corporate leaders have taken a system of systems approach and focused on “defend, detect, isolate, mitigate, respond, and learn” as a means to improve the cyclic response to a cyber-event. In order to effectively execute this approach, senior management is required to fully understand the technical aspects of information operations, cybersecurity, and most importantly the operational impact if their information or network is compromised. Leaders establish and enforce strict compliance standards to connect and operate on their network. Their employees are held personally accountable for data protection, and the consequences of non-compliance are real and understood by everyone. The best CEOs constantly communicate, advocate and measure understanding of cybersecurity throughout the enterprise. They review daily system performance dashboards, demand their systems and people are constantly tested, and annually conduct surveys to gauge employee understanding of the corporate strategy and values to improve and reinforce their messaging.

In the best organizations, information resilience and cybersecurity are well understood and driven down to every level. Leaders continuously discuss the issue at every internal and external forum and have created governance boards and audit mechanisms to oversee and evaluate progress. Employees aspire beyond mere compliance, to ultimately understand the operational importance of their behavior. This understanding enables employees to embrace the impact of cybersecurity, feel safe to speak up or act when they see something that does not look right, and in doing so, their initiative is firmly backed up at every level. In industry, the system of meritocracy (what the company values and rewards) is easily understood and employees’ compensation and professional development opportunities are tightly aligned with it. Senior leaders have absolute authority to stop or halt any practice in the business if it poses or is perceived to impose a cyber-risk. We were hard pressed to find the same in the DON.

Lastly, it is well known in industry “if you can’t measure it, you can’t improve it.”⁷ Transformation in the best organizations is observable and measurable, not just in meeting Power Point or talking points presented in various public speaking engagements. Companies set cybersecurity as a strategic objective and develop an execution plan with qualitative and quantitative metrics to demonstrate progress and highlight areas in need of additional attention. Those metrics are key to making information resiliency part of the cultural DNA of the enterprise.

⁷ Drucker, 2010, The Effective Executive

State of Today's Naval Service Culture

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. The DON culture continues to value investment in physical warfighting platforms over resilient information system capabilities.

Recognizing the need to institute a cybersecurity culture within the DON is not a new concept, however the “getting it done” has been the problem. For over five years, senior leadership acknowledged that risks in the cyber domain were growing significantly given increased adversary sophistication and the military’s growing dependency on information to fight and win. For example, in 2014, the Navy established Task Force Cyber Awakening (TFCA) in response to an important adversary breach of the unclassified network. In addition to identifying the organizational and resourcing changes needed to combat the threat, TFCA was to develop a robust strategic engagement plan to increase cybersecurity awareness and establish cybersecurity as “Commander’s Business.”⁸ Then, in 2015, the Secretary of Defense (SECDEF) and the Chairman of the Joint Chiefs of Staff (CJCS) established the DoD Cybersecurity Culture and Compliance Initiative (DC3I) to “raise the level of individual human performance in cybersecurity.”⁹ DC3I established five operational excellence principles: integrity, level of knowledge, procedural compliance, formality and backup, and a questioning attitude – each deemed fundamental to the DoD cyber enterprise. To build a strong cybersecurity culture they targeted specific populations within the DoD – leaders, providers, cyber warriors, and users. The SECDEF and CJCS further directed quarterly updates be made to the Deputy Secretary of Defense (DEPSECDEF) and the Vice Chairman of the Joint Chiefs of Staff (VCJCS).

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. Many leaders do not comprehend the full scope of the threat, which contributes to a disparity in relative emphasis. The workforce is generally uneducated in cybersecurity, largely complacent, and fails to fully embrace “a risk to one is a risk to all.” As a result, cybersecurity is undervalued, and often used as a bill-payer within programs of record. The lack of mechanisms to adequately measure or even estimate the cost or value of items at risk inhibit the ability to articulate justification for investments in this area. For example, given competing priorities, an operational commander may view a cyber-vulnerability as a high mission risk while the resource sponsor or system commander may view it as a medium programmatic risk. In either case, cybersecurity continues to be seen largely seen as an “IT issue” or “someone else’s problem.”

In addition, by his choice, the Under Secretary of the Navy (UNSECNAV) is currently triple-hatted as the Under Secretary, Chief Management Officer (CMO), and the Department’s CIO. He is supported by two Deputy DON CIOs, the Navy’s Deputy CNO for Information Warfare (OPNAV N2N6) and the Marine Corps’ Director of C4. The Deputy DON CIOs are

⁸ Deputy Chief of Naval Operations for Information Dominance, 2014, Task Force Cyber Awakening Memorandum

⁹ Pentagon, 2015, Department of Defense Cybersecurity Culture and Compliance Initiative

themselves multi-hatted, responsible for overseeing the daily execution of the DON CIO function and other Service responsibilities. This creates inconsistent communication from the top-down and inconsistent messaging laterally. Commands and personnel remain protective of their traditional structure and budgetary status quo.

There is also a lack of accountability across the enterprise for cyber readiness. There are no real consequences for failure and few rewards for success. For example, the workforce continues to accept known vulnerable, non-compliant systems which pose an unknown risk to the mission. As an example, the Navy Secretariat only began this year to install the 2015-created Windows 10 operating system. Consistent with what the DON discovered in the 2017 Strategic Readiness Review (SRR), a critical look at how declining readiness in the surface fleet contributed to the loss of 17 Sailors, the Navy has embraced a culture of “normalization to deviation” in cybersecurity.¹⁰ Specifically, the Navy has waived known material readiness standards mandated by the DoD RMF and knowingly continues to field high risk vulnerability systems. For example, there are currently a number of high risk systems connected to the Navy network that have received five or more formal waivers to continue operating due to a lack of resources or scheduled modernization occurring in the distant future. For these systems, the “waived” state has become the de-facto standard. These waivers inject unknown risk to the enterprise and reinforce the narrative that cybersecurity is not a priority. The SRR also found that waiving standards not only creates unsafe operating conditions, it creates a readiness deficit which ultimately must be paid in order to sustain operations. Similarly, the Navy is creating a “tech deficit” by not fully funding needed systems and capabilities to established standards. Charged with oversight of securing the Navy Cyber Platform, the Navy Cybersecurity Executive Committee (EXCOM), is briefed routinely on warfighting systems designated as high risk and operating on the network without an approved Authority-To-Operate (ATO) certification. None the less, at risk systems are allowed to remain connected to the network and no one is singularly held responsible for non-compliance. This is a very sharp contrast to best practices in corporate and government organizations.

The DON has also been slow to respond to the growing cyber talent gap at all levels. This gap continues to trend in the wrong direction and leaves the Department ill-prepared to meet today’s most sophisticated threats. Additionally, the majority of the workforce views cybersecurity as a nuisance that unnecessarily complicates their mission and for which they have little to no direct responsibility. The leadership does not grasp that cybersecurity cuts across the DON and is not a vertical issue remedied with “bolt on” solutions. Cybersecurity must be viewed horizontally and integrated across the DON, distinctly different from the common refrain we heard throughout the DON: “we have people for that.” Of particular concern, key individuals in the DON and DoD we met with consider resources allocated for cybersecurity to be bill payers within the broader budgeting process and are willing to trade them for other competing priorities.

DON culture must reflect the existentiality of the cyber threat and be characterized by a sense of urgency in demanding cybersecurity excellence at all levels, characterized by uncompromised integrity, increased knowledge, procedural compliance, formality, and backup, and an ever-questioning attitude. DON leadership must reinforce a culture of trust throughout the organization and celebrate acts of self-reporting that will enable learning. This requires a

¹⁰ US Navy, 2018, Strategic Readiness Review

better understanding of the operating environment and the proper tools and education to make better risk decisions at every level. Accountability, through robust auditing and certification, is essential across all DON information and cyber platforms (IT, Operational Technology (OT), Weapon Systems, and Data). The DON must develop a culture that understands that data protection must be considered in every evolution, similar to the Navy's safety program. Sailor, Marine, and civilian behaviors must embody the importance of protecting DON data throughout the enterprise from requirements, to resourcing, to acquisition to operations.

The lack of clarity of thinking evidenced in the several attempts to reorganize the CIO, the unwillingness to create leader dashboards or issue standing orders to not "fly" or "sail" networks that are "unsafe," are but three proofs of the inability of the leadership to effectively react to competitor's harm. From that, the ability of the leadership to get ahead of the competitor's harm is nearly impossible. The totality of the resulting losses, the competitors gain and the damage to the future naval enterprise and the nation, are beyond measure.

In summary, the DON cybersecurity culture can be characterized by distrust, a lack of knowledge or accountability, a willingness to accept unknown risks to mission, a lack of unity of effort, and an inability to fully leverage lessons learned at scale. For example, the implementation of the Navy's CYBERSAFE program has been significantly strained due to ambiguity surrounding who possessed the requisite technical authority, where the resources would come from to pay for it, and the impact it would have on delivering the capability on time. The workforce fears the potential impact that establishing requirements and resourcing cybersecurity solutions will have on their equities and the bureaucratic status quo. This can be observed across the enterprise from Systems Command (SYSCOM) control of technical authority, to resource sponsor investment prioritization. While there are pockets of excellence throughout the DON that understand and embrace a mindset of "a risk to one is a risk to all", the majority of the workforce has a complacent or distrustful attitude towards cybersecurity. Senior leaders will occasionally articulate cybersecurity as a significant risk to mission, but then routinely fall short of translating this sentiment into specific actions across the naval enterprise. The disparity between stated priorities and directed action creates ambiguity, which in turn distances the DON from implementing a unified, cost efficient and operationally effective cybersecurity strategy.

This diagnosis has a common thread of causation - the absence of sustained focus and attention from the top down. The lack of mobilization to action in the face of a deluge of IP thefts the past two years in a service that understands the call to all hands to task, is remarkable. This powerful cultural force that is Navy and Marine Corps now must inculcate the criticality of information resilience and cyber in every aspect of life and execution of their maritime security mission.

Culture Recommendations

To succeed in the coming decades of global rivalry, the DON must develop a culture that fully recognizes and embraces the importance of information and cybersecurity and resiliency across all mission areas and all personnel in order to enable success in future battles.

Select key leaders and promulgate actionable long- term cybersecurity and resiliency plan

The SECNAV, CNO and Commandant must select leaders who understand the problem and inculcate the proper cybersecurity culture—the top sets the culture. Key subordinate leader position selection criteria must also be established to further focus on cyber awareness. There is a significant “say-do” gap due to a lack of leadership and a clear cybersecurity implementation plan. It is unclear what the organization expects at each level to achieve cost efficient and operationally effective cybersecurity outcomes:

- Direct the establishment of a cybersecurity competency as a selection criterion for key leadership positions to ensure future leaders believe and understand in its relative importance
- Direct cybersecurity risk be articulated in all strategy and policy documents to increase overall awareness
- Direct the development of a comprehensive, actionable long-term cybersecurity strategic plan akin to shipbuilding or aviation

Improve and measure cybersecurity culture

The SECNAV, CNO and Commandant must embrace the existentiality of cybersecurity risk and direct their senior leadership to communicate its importance, drive necessary change, and instill and maintain a culture of continuous focus and improvement. They must assure the workforce always values cyber and understands its importance in DON’s strategic priorities:

- Direct the Chief of Navy Information to develop and execute a communications plan for the senior leaders to inform all levels of the DON on the shift of the business of the DON from ship and MEU centric to information centric
- Direct the conduct enterprise-wide surveys to continually assess personal comprehension of DON strategy and values as it relates to cybersecurity and resiliency

Improve awareness of the cyber threat

There is a critical ignorance and understanding of the evolving cyber threat. The magnitude of the consequences of failure is also unclear to most individuals. The enterprise needs to be shocked into action through real threat briefings and reinforced by instituting an “Every Sailor a Cyber Sentry” mindset, similar to the “Loose Lips Sink Ships” and “Every Marine a Rifleman” slogans. The DON needs cybersecurity to be on the forefront of every action and as reflexive as saluting a senior or as responsible as Nemo Resideo: “No Man Left Behind.” To accomplish this, leadership will need a persistent commitment of words and actions.

- Direct the regular development and conveyance of appropriate relevant cyber and information threats and breach consequences tailored to individual ranks and specialties at the scale of the operational threat briefs to the fleet during the cold war

- Direct creation of a sustained, robust cybersecurity information campaign to increase awareness, share threat information, highlight importance of cybersecurity to warfighting success, and re-inforce expectations across the workforce (MIL, CIV, CTR/DIB)
- Establish a campaign with the focus of “Every Sailor & Marine a Cyber Sentry” as a core tenant of naval service
- Re-write the education platform at all levels to include cybersecurity education starting from the entry-level on up in the DON

Establish clear expectations for individual and organizational collaboration

The DON/DIB needs to work together to mitigate evolving cyber threats. The DON should take immediate steps to lower the barriers to communication in order to enhance information sharing and collaboration.

- Routinely participate in DIB association meetings to ensure members understand priorities, policies and desired outcomes
- Establish forum for DIB CEOs, CIOs, and CISOs to meet regularly with DON counterparts to share information and drive continuous improvement
- Establish formal process to improve information sharing of threat data and cybersecurity best practices, to enable the DIB to anticipate, innovate, and assist in securing the entire cyber platform

Improve and measure accountability to produce cybersecurity outcomes

Finally, DON must create a culture built on a foundation of accountability, from the top down, where leaders establish measurable objectives and drive organizations to achieve them. The protection of DON information in the cyber battlefield needs to be embraced in the same way one would protect the water tight integrity of a ship. These cultural attributes must be achieved with a sense of urgency and criticality. Without a cultural shift, all other efforts will fall short of achieving the security and mission assurance required for success in future conflicts.

- Institutionalize culture of “cybersecurity & resiliency first” in the DON, similar to “safety first” or “safety of flight”
- Raise the level of priority for cybersecurity capability development and execution; holding individuals personally accountable for achieving mandated standards
- Align system of meritocracy to communicate value of adherence to cybersecurity policies and standards

Ultimately, our information and cyber culture must move beyond a system of compliance to one characterized by individual and institutional initiative. DON goals must shift beyond the minimum thresholds of acceptance to an outcome-based model, focused on performance. By doing so, DON’s culture will be characterized by behaviors that allow for greater agility across the entire cybersecurity production chain. In this new environment, actions must result in resilient systems that permit the naval service to continue the fight and win.

Chapter 3: People

The Role of People as a Governance Tool to Achieve Cybersecurity Resiliency

In the very best information and data-dependent organizations, people are seen as the greatest asset, as well as the greatest liability. As an asset, people are the innovation and decision engines for the organization and the capable hands that ultimately accomplish desired outcomes. As a liability, every hour of every day, individuals of all roles and specialties make dozens of decisions and take hundreds of actions that may enable or fall prey to cyber threats. Tougher training and better recruiting will reduce vulnerability to the threat. However, regardless of the amount of training and education, even the best workforce will always remain vulnerable.

People Best Practices

Cultivation of the Workforce

Best-in-class organizations carefully manage this seemingly contradictory point that people are their greatest asset and their greatest liability. Their personnel are thoroughly indoctrinated, trained, continuously educated, and evaluated. While their personnel are trusted, they are also continually tested and monitored to ensure they are maintaining established security standards. With this in place, top performing organizations are then able to optimize the alignment of people with desired objectives and empower them to out-perform the competition. Although there will always be some inherent cybersecurity risks with personnel, good training and instruction on proper cybersecurity hygiene, periodic evaluations, and appropriate monitoring can reduce these risks.

Non-Cyber Workforce

Training and education is an ongoing process that should build and reinforce the capabilities of all employees. As the essential means of execution, personnel must always be ready and fully capable of achieving company objectives. Leadership in top performing enterprises understand that the threat posed by internal compromise is real. However, people can only be held accountable if they have the knowledge and tools to make informed decisions. Leadership spends time and effort ensuring that relevant and adequate training is provided to every employee.

Best-in-class organizations also use a combination of aggressive self-stressing and the “principle of least privilege” through use of Zero-Trust-Models. The self-stressing such as red team phishing helps to reinforce standards by demonstrating to people how threats manifest. It also lets individuals see the right way to protect themselves and the organization. The Zero-Trust-Model, paired with advanced algorithms through automation, further helps put an organization’s business rules into technical practice and enforcement, thereby relying less on methods that require manned intervention.

Cyber Professional:

Cyber professionals are highly valued in the commercial sector. Their high compensation levels reflect the extremely competitive market challenge for their recruitment. Commercial companies go to great lengths to provide retention incentives to new recruits and to retain their existing talent. Best-in-class companies understand it is more cost-effective to retain good talent than to prospect and train new talent. The use of cutting-edge recruiting tools that specifically target those that possess these skills, and a proactive approach to retain them, is a major step in addressing frequent turnover in key areas. With no imposed “up-and-out” requirement, the private sector has the flexibility of appropriately incentivizing their cyber professional workforce to stay in their position.

An advantage to retaining a qualified, well incentivized cyber professional workforce is familiarity with the networks these professionals must monitor and maintain. As frontline defenders (i.e. local defenders) their longevity provides greater understanding of their network’s steady state and can quickly detect anomalies to defend against.

State of Today’s Naval Service People

Cultivation of the Workforce

With more than a million users on DON networks, there is no shortage of opportunities for opponents to exploit the workforce. As the greatest potential source of cybersecurity vulnerabilities, their level of knowledge, training, and daily actions will either contribute to safe operations or present opportunities for adversaries to exploit. Technical solutions can be developed and deployed, but technical solutions alone are not sufficient to meet the threat imposed by the large overall DON population that uses the networks. Other vulnerabilities and challenges are specific to the cyber-specialist workforce and are very different than those of the non-cyber-specialist workforce. In either case it is paramount that the DON cultivate both workforces in a manner that achieves desired outcomes.

The framework of the analysis that follows is closely tied to the idea that cultivating the workforce requires an Identify-Recruit-Train-Sustain-Retain model:



Figure 3: Identify, Recruit, Train, Sustain, Retain model. CSRR 2019. The Review developed this model to illustrate key issues for the cyber and non-cyber workforce.

- **Identify:** Identify the jobs, roles, functions, and skills required to achieve mission success. Know what you have and what you need to achieve your desired outcome. Proactively manage the mission, functions, and tasks within an organization; specifically, functions of the workforce.
- **Recruit:** Find, entice, and hire individuals that possess the skills or aptitude. The effort put into finding qualified and willing bodies is only the first step. Further steps

- must consider what the organization offers relative to others to bring in talent and how the organization compares to peers in regard to workplace satisfaction.
- **Train:** Teach individuals the concepts to perform the functions within the organization and how to be an asset. Implement entry-level professional education. Ensure training is relevant and updated to keep pace with the changing environment.
 - **Sustain:** Reinforce training, update information provided to individuals above the baseline offered in initial training. Reinforce and enhance training and education efforts to ensure they keep pace with the changing environment. Provide continuing professional education and growth opportunities. Motivate the individuals through incentive for performance.
 - **Retain:** Incentivize workforce to maintain competitive employment opportunities. The cost of retaining personnel is less than the cost to train new people. This includes compensation and benefits, but also includes job satisfaction.

Non-Cyber Workforce

The non-cyber workforce represents the vast majority of the DON. Any activity that does not involve the direct management or support of IT systems, to include control systems, falls into this category. Examples include logistics, engineering (non-cyber), operations (non-cyber) and administration. While these activities do not fall under the cyber workforce category, the performance of their individual jobs involve access to information and systems that are very much the focus of the threat. Understanding how to safely manage their access to, and their manipulation of information is a major challenge facing the DON.

The DON, at all levels, does not have a comprehensive, integrated process to prepare the workforce for the evolving threat. Without a process that validates the effectiveness of training, such as the “Cybersecurity Awareness Challenge,” the DON has no definitive indication of the true state of workforce awareness about cyber threats and the actions they should take when confronted with them. Audits, red-teaming, and lessons learned are common processes to assess the status of other heavily process-oriented organizations within the DON. Yet in cybersecurity, compliance is often achieved by a question asked, followed by an answer, and then a check in the block. A well understood phrase within the DON is ‘expect what you inspect.’ Cybersecurity throughout the force should be no exception.

Train

Cybersecurity training in the DON is insufficient to counter the prevailing nation-state and insider threat. The general workforce is usually the target or inadvertently the cause of most cyber breaches and incidents.¹¹ Phishing attacks, poor cyber hygiene, and failure to update and patch software are the root cause of the vast majority of cyber incidents. Annual cybersecurity training for the entire workforce is far too basic and one-size-fits-all. Most dangerously, it underemphasizes the realities of the cyber threat. The workforce is led to believe that cybersecurity is simply a matter of routine compliance, which enables seeing security practices such as password protection and email vigilance as needlessly burdensome. This was validated

¹¹ Cybersecurity Insiders, 2018, Insider Threat 2018 Report

through numerous interviews that cited cybersecurity as “a problem for the cyber-specialists” whereas the reality is that non-cyber specialists are the preferred target of exploitation.

Sustain and Enhance

The vast majority of compromises to systems are through non-cyber workforce personnel. The education of these individuals should be designed to increase awareness of vulnerabilities to reduce risk. While the people that operate and maintain DON systems require intense formal education, the workforce at large needs a better understanding of the risks that cyber poses to successful mission accomplishment. The annual cybersecurity training, currently required by DoD, is insufficient in providing that training to the overall workforce. It is slow to change and does not sufficiently relate the threat to the individual in ways that are understandable and relevant to their jobs and the missions they are performing. Evaluating training effectiveness by simply clicking through electronic training that is virtually identical to the previous year does not increase user level knowledge or reduce risk.

Retain

Leaders have always been promoted and retained based on common knowledge skills such as readiness, damage control, and safety. Naval personnel do not rise through the ranks unless they can demonstrate an ability to meet readiness standards, defend the ship, and maintain safety standards. These functions, the fabric of naval missions, are key attributes of successful leaders. Today’s great power competition, information-centric, highly-networked cyber environment makes cybersecurity a critical and required common knowledge skill for leaders and the workforce. However, cybersecurity knowledge and the ability to protect information is not a key attribute in the selection or retention of today’s leaders. This must change.

Cybersecurity must now be recognized as an essential element of the common knowledge skill sets leaders must possess. Given the technological nature of cybersecurity, the DON needs to consider this common skill requirement as a factor for promoting or retaining personnel. Without a better understanding of cybersecurity DON leaders will be handicapped in their ability to develop and execute strategy. This knowledge must go well beyond simply understanding the existence of risk. Relying solely upon cyber professionals defies the reality that the Navy and Marine Corps cannot defend itself or advance in this domain with only the specialists possessing the knowledge.

Cyber Professional Workforce

The Navy has a well-established cadre of cyber professionals. Civilian, enlisted and officer communities support the mission requirements in the cyber domain. In the DON, unlike the private sector, individuals are required to move and be promoted on a defined schedule (up or out). Many of these professionals have expressed interest in remaining in service but are not interested in leaving the technical positions that brought them into this career field and are equally not interested in staying in an organization that doesn’t recognize, reward, and promote based upon their technical skills and contributions. This presents a very real dilemma for them and for DON retention of these cyber professionals. Furthermore, given the private sector’s

expanding need for highly trained cyber professionals, the lack of incentives is an attrition accelerant, and is severely degrading the DON's ability to attract and retain top cyber talent.

Identify

The DON needs to refine the category of personnel that comprise the cyber workforce to cover, not only traditional network and IT positions, but also those that are essential to supporting cybersecurity within acquisition, program management, intelligence, legal and law enforcement. These areas have been dramatically impacted by the evolution of the cyber challenge and require specially trained individuals to facilitate those missions.

The most impacted of the cyber-specialist workforce are government civilians. The civilian workforce includes a small number of very highly skilled employees that are essential for analytical support on cybersecurity issues related to foreign intelligence (both technical and operational), counterintelligence, policy, and data analytics. These employees are required to have education and backgrounds in multiple disciplines such as computer science, engineering (e.g. computer, electrical, software, mechanical, industrial, civil), intelligence, targeting, network operations, and more. There currently is no comprehensive process by which to identify, recruit, develop, and assign these personnel with the specific talent necessary for these specialty positions. There is also no process by which to develop and cultivate the currently-assigned employees with additional training or a career progression track to follow based on increased experience. The lack of sufficient numbers of these very critical personnel is a significant DON vulnerability.

Recruit

It is well known that the hiring process for federal employees is a challenge in itself for attracting talent.¹² The hiring process is even more antiquated for the acquisition of specialized skills such as cybersecurity. This skillset is one that is in high demand in the private sector, with very attractive incentives. For the DON, without a more deliberate strategy and targeted means by which to identify and enumerate positions that must be held by personnel with proven cybersecurity skills, it is difficult to link these required positions with attractive incentive packages that could be presented to potential employees when they apply for the job. To recruit new talent, it is necessary to offer competitive compensation to civilian employees. While pay may be constrained by the federal government through the Office of Personnel Management, there are many programs and incentives that can offset pay disparity, including telework, modified work schedules, and defined retirement benefits. The cyber excepted service is a good concept, but the initiative needs to be validated to ensure it is being effectively employed and expanded.

Train

Developing unique cyber skills that the DON requires demands a robust training program for cyber professionals. The military workforce has training programs for enlisted information technicians and the Marine Corps recently established Military Occupational Specialty (MOS)

¹² Partnership for Public Service, 2015, Cyber In-Service Security II: Closing the Federal Talent Gap

1700 Cyberspace Operations Occupational Field to address the absence of cyber-designated workers. However, the DON lacks an adequate training pipeline to satisfy all the requirements for scarce cybersecurity skills in the civilian workforce.¹³ In fact, with an expectation that the nation will require an increase of as many as 1.5 million additional trained professionals needed by 2020, development of a training program is critical, but has yet to be developed within the DON.¹⁴

Despite those training programs within the DON for military personnel, there remains a lack of adequate training specifically for the local defenders. The IT personnel charged with maintaining the networks and communication systems are provided in-depth cybersecurity training only when assigned to specific billets. In the event of an incident there may not be an individual that possesses adequate knowledge to react to or support incident response.

The cybersecurity workforce has challenges in identifying positions and skillsets for the civilian workforce. The DON has many talented professionals in this area, but the management of those individuals is poorly executed. There is no consolidated organization that focuses on civilian workforce development and training for cybersecurity. DON efforts to maintain a cybersecurity educated, well-trained workforce is inadequate. Beyond computer-based training, maintaining standards requires a reinforcement of lessons via other means.

Unit-level drills, exercises, and persistent self-stressing are either non-existent, not routine, or not tough enough in many DON organizations. Unit-level drills for cyber-specialists at some core organizations are developed and formalized by the Information Forces Type Commander. Others are only in pilot-stages and are underdeveloped. Unit-level training at non-cyber units is mostly nonexistent. Finally, there is a lack of maturity for advanced levels of training across the DON, which should also include a full understanding of all end points and architectures for local defenders.

Sustain and Enhance

The DON's challenge for personnel is balancing traditional career paths while evolving specific expertise in an ever-changing environment. The traditional naval career is often a balance of sea and shore duty. However, the bulk of cyber billets exist ashore. When individuals are required to complete sea tours or tours outside of their specialty, their time away from cyber-related tours puts them at a disadvantage for keeping pace with rapidly evolving cybersecurity advances and their skills atrophy. Conversely, if these Sailors forgo sea duty and disassociated tours in favor of shore-based cyber-related tours, they are placing themselves in jeopardy of not being promoted due to reward system that values balanced sea-shore rotations.

Further complicating the matter, is that the sea-tour requirements diminish opportunities for challenging national mission assignments, where their skills are needed and can be further developed. As long as military cyber professionals are held to the same sea-rotation requirements as the rest of the workforce, with limited opportunity to work on afloat networks, their personal cyber skills will atrophy. Additionally, Fleet Cyber Command (FCC), who is

¹³ The Cornell Institute of Public Affairs, 2017, Attracting and Retaining Talent in the Field of Cybersecurity

¹⁴ Commission on Enhancing National Cybersecurity, 2016, Report on Securing and Growing the Digital Economy

responsible for providing cyber-trained professionals for national missions will be challenged to answer the call to fill empty billets.

Despite persistent challenges with assignment rotation, sustainment of the cyber professional workforce has similar challenges to the non-cyber workforce; albeit at a more technological level. The ability to evaluate the effectiveness of their training is equally important. Command Readiness Team Training Scenarios and the DON's Information Warfare Development Command (IWDC), which creates tactics, techniques and procedures for scenario-based training has not been leveraged to evaluate network local defenders' training to detect, identify, and protect against threats.¹⁵

Retain

The private sector is just as hungry as the DON for personnel skilled in cyber. Private sector competition does not only seek talent from college graduates and other companies. The DON talent pool is highly sought after for recruitment by the commercial sector. This demand makes retention of qualified Sailors and the civilian workforce a vital part of the personnel strategy. Cyber Excepted Service is a new program that may prove beneficial when fully implemented. If military personnel are separating from service, this program potentially allows the retention of these skills by shifting service into the federal service and retaining the skills in DON.

People Recommendations

Improve military and civilian cybersecurity career paths

There is a need to build a career path tailored to develop expertise in specific cyber skill sets. While sea-time may be a part of this tailored development, any rotation should deliberately build on expertise in the cybersecurity specialty. Sea-tours are important for cyber professionals, but the tours should be focused on a geographic area commensurate with the member's cyber expertise, building depth of knowledge through the entirety of their career. The Navy must acknowledge this reality and build the geographic cyber depth necessary to support the DON's, and the nation's strategic political, military, and economic goals.

- CNO and CMC, reexamine the requirement that cyber professional personnel are forced to promote or be forced out
- DCNO IW, explore career and assignment changes that will enable the DON's cyber force to meet the mission objectives being levied by national authorities
- SECNAV, direct CIO to improve the identification and career progression of civilian workforce through the establishment of a designated and organized civilian workforce supporting cybersecurity within the DON

¹⁵ Nascent in its development, the IWDC is Only two years old. The Review did not assess IWDC's ability to develop methods to evaluate the effectiveness of cybersecurity training for the Cyber Professional workforce, but compared with sister Warfare Development Commands, it is not unreasonable to look within the lines of the IWDC or Information Warfare Training Group (IWTG) to develop sustainment mechanisms for the Cyber Professional workforce.

Improve cybersecurity training for DON's workforce

If the DON expects to achieve unmitigated resiliency in the technologically-advanced systems that make the force so formidable, it must acknowledge the requirement to train its personnel to protect the information and systems over which data flows. The development of education programs that inculcate cybersecurity in DON's culture and training programs must be accelerated to ensure the workforce maintains pace with emerging threats and the technologies that help defend against those threats.

- SECNAV, create a training pipeline of cyber core competencies based on educational background and work experience, as well as a means to highlight cross-training and promote the workforce into key positions to retain talent
- CNO and CMC, develop processes to establish and maintain an integrated education process to prepare the workforce for an evolving threat
- CNO and CMC, create processes that better articulate the requirement for trained and qualified Local Defenders who can consistently and effectively counter the threat

Sustain DON's cybersecurity capability

Sustainment of the DON's capabilities in cybersecurity must be validated through constant, effective monitoring. This reinforces and enhances training and education efforts to ensure they keep pace with the changing environment. Once a common baseline is reached, effectiveness monitoring will help provide a demand signal for increasing professional education and growth opportunities and additional training. Such sustainment efforts can also inform the Information Warfare Development Command's efforts to develop designated cybersecurity experts who can develop sustainment programs consistent with technological advancements and evolving threats.

- SECNAV, order comprehensive testing, assessments, audits, and investigations¹⁶.
- CIO, initiate processes for aggressive self-stressing (maximize National Security Agency (NSA) certified red teams and private sector best practices)
- CNO and CMC, improve the level of cybersecurity knowledge, including an understanding of cyber hygiene, in non-cybersecurity workforce through improved basic training and unit-level self-stressing
- DON CIO, institute standardized manual and automatic testing and probing (Red-Teaming) of DON systems, platforms, and installations to sensitize personnel and relevant organizations to potential vulnerabilities
- DCNO IW, leverage IWDC's mission to develop evaluation of higher-level training through scenario and warfare expert designations for the Cybersecurity Professional workforce. Higher level training should include a full understanding of networks to be protected

¹⁶ Office of the Secretary of Defense, 2018, National Defense Strategy 16

Retain DON's professional cyber workforce

Given the high demand for cyber professionals, the DON is competing poorly against the commercial sector for the best talent. There are incentives, such as bonuses for military personnel that attempt to address the pay disparity with the commercial sector, but further efforts should be explored to ensure highly valuable and competitive skills are obtained and retained in the workforce.

- SECNAV, mandate a change to the current bonus structure and tailor it to career progression in a manner that retains sufficient cyber professionals
- CNO and CMC, fully leverage existing human capital programs to incentivize and retain talent
- CNO and CMC, maximize the use of Cyber Excepted Service for transitioning military and current general schedule civilians as a means to retain talented personnel within the DON

Chapter 4: Structure

Role of Structure as a Governance Tool to Achieve Cybersecurity Resiliency

Organizational structures are ideally created to enable the optimal flow of information and resources in a manner that supports strategic intent. Through structure, an organization's mission, vision, and goals are communicated and priorities established. Additionally, the best corporate structures incorporate internal systems of checks and balances, such as the separation of responsibilities for prevention and acceptance of risk to enterprise, from the pursuit of profit responsibilities.

In order to be successful, a cybersecurity program requires dedicated engagement throughout the enterprise, from the senior management team down to, and including, all employees. The "tone at the top" is key, but this tone, or sense of awareness and urgency, must be driven throughout the entire organization. A properly organized enterprise structure can facilitate this and will also provide for the effective creation, implementation and oversight of cybersecurity policies and directives. An effective organization will also enable the identification and mitigation of risks, and the active reduction of breaches and the severity of losses from them.

In a 2017 Open Society Foundation report found that structural dysfunction was the most significant obstacle undermining the effectiveness of the U.S. security sector.¹⁷ This finding is parallel to current challenges found with governance structure within the naval service.

Structure Best Practices

Governance-led, CIO/CISO-supported, outcome-driven

"Today, every company is becoming a technology company...Southwest Airlines is a technology company, McDonald's is a technology company and so on. In this transition, every department and every function of these companies has demands that go straight to the CIO."¹⁸

With regards to corporate structures, successful industry leaders have assigned their CIO and/or CISO to report directly to senior executive leadership and have empowered them with absolute oversight authority to enact new, stricter guidelines for cybersecurity; including authority to direct changes in cybersecurity posture throughout the corporation. In some cases, the CIO owns the networks and systems and the CISO is responsible for the cybersecurity oversight and compliance. Corporate Boards of Directors are also increasingly including a risk committee, which meets regularly with the CIO and CISO. One of the financial services companies the Review visited indicated that risk management strategy and its linkage with technology came directly from the CIO and the Global Operating Committee. Some of the best practices identified were:

¹⁷ Open Society Foundation, 2017, Untangling the Web: A Blueprint for Reforming American Security Sector Assistance

¹⁸ Ibid

- The organization positioned themselves as information centric institutions regardless of their line of service.
- In 65% of identified leading organizations the CIO reports directly to the CEO¹⁹.
- CIOs meet with CEOs on a frequent, often weekly, basis for anywhere from 30 to 90 minutes.
- CIOs and CISOs are empowered with robust authorities across business lines
- Cybersecurity is integrated horizontally and ingrained across the corporate architecture.
- CIO's, Chief Risk Officers (CROs), and Chief Financial Officers (CFOs) have a symbiotic relationship with a goal of balancing fiscal efficiency and corporate network security.²⁰
- CIOs did not run the networks they governed

State of Today's Naval Service Structure

DON's structure does not enable effective top-down governance

Over the last two centuries, the DON evolved as an organization with a governance structure designed for conventional operations. A relatively recent addition to that structure is the DON's IT and the modern warfare systems that use them. Despite the traditional forces and their platforms that now absolute depend on them, the cybersecurity of these systems and their supporting supply chain has generally been shoehorned in as an afterthought into those preexisting organizational structures.

Within the DON, there is a lack of understanding of the impact that cyber breaches actually have on the ability to conduct assigned missions. This stands in contrast to the private sector where nearly 80 percent of directors and general counsels in publicly traded U.S. companies feel that they now have "a good understanding of the cyber risks within their company."²¹

DON structure does not provide effective CIO/CISO authorities

DON CIO responsibilities are fairly well defined, but what is still lacking is clear willingness to enforce compliance with current technical standards. The CIO currently does not have authority to set strict "Go/No-Go" criteria, to which DON components must adhere in order to ensure unity of effort in addressing continuous threat vectors against DON's multiple disparate but integrated networks. There is no DON CISO. The CISO role is delegated to the N2N6G and the USMC C4 who both have many other duties. DON CIO's duties include²²:

- Senior IM/IT/IRM official and carries out the IM/IT/IRM responsibilities and duties set forth in Titles 10, 40, and 44 of the United States Code
- DON senior Cybersecurity official

¹⁹ Forbes, 2017, The Ascent of the CIO

²⁰ Burges, 2015, Data Security Requires a Symbiotic Relationship Between the CIO, CFO, and CISO

²¹ Diligent, 2017, Cybersecurity, Corporate Governance and Your Board of Directors

²² DON CIO website, 2018, About the DON CIO

- DON senior Electromagnetic Spectrum official
- DON senior Privacy Act official
- DON senior Civil Liberties official
- DON senior Records Management official
- DON senior Freedom of Information Act official
- Oversees Don IT capital planning and investment management
- Oversees DON compliance for protecting DON information and systems
- Oversees the process of developing and maintaining the DON enterprise architecture and assesses compliance with DoD and Federal standards
- Ensures compliance with Section 508 of the Rehabilitation Act
- Promotes the effective and efficient design and operation of all major IRM processes, including improvement to DON work process

Although there have been multiple recommendations and attempts at improving cybersecurity responsibilities and accountability in the recent years, the current stove piped structure has remained. This is not conducive to efficient process improvement or a proper system of checks and balances to ensure that procurements fully comply with all current cybersecurity standards. In the DON’s most recent reorganization, the role of CIO has been performed by the UNSECNAV, in addition to his role as CMO and all other responsibilities he is tasked with. The Undersecretary has all the power to he needs to play a critical role for cybersecurity in the DON as he acts with full authority of the Secretary in the general management of the Department and supervision of offices, organizations, and functions as assigned by the Secretary.

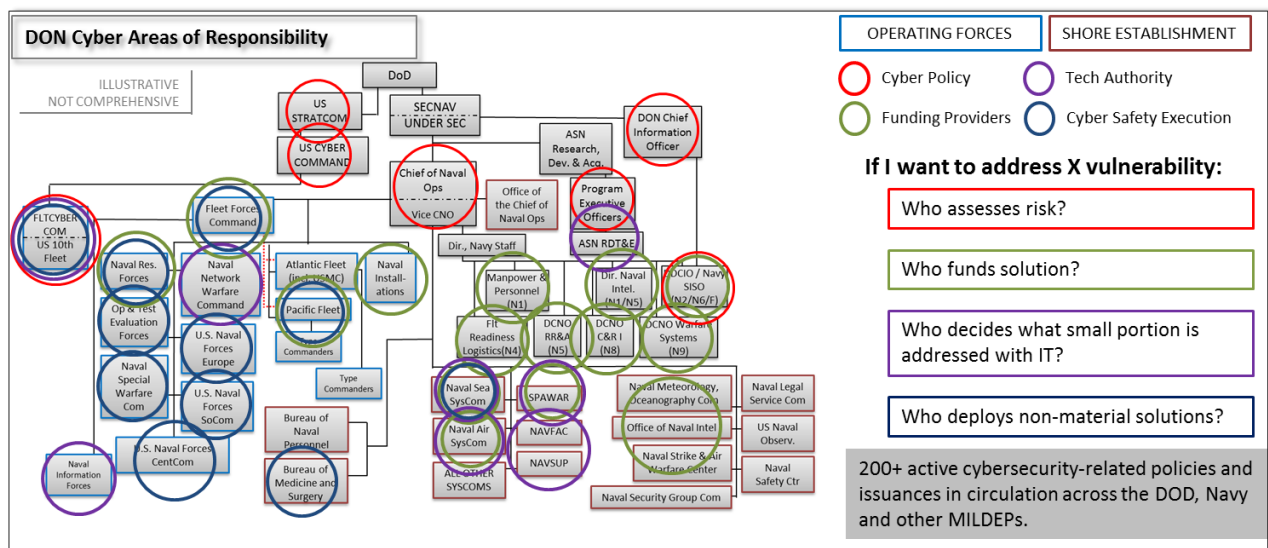


Figure 4: Shows who the informed leader is that oversees policy, funding, technical authority, and cyber execution across the DON. DON cybersecurity oversight and financial considerations briefing, 2017, Stewart

A key observation of the Review is that the authority, responsibility, and decision-making power for information risk management has been confused by its distribution within the DON, resulting in fragmented, or uncertain response to the expanding threat. Also, many of the policy and funding decisions do not reflect the current risk profile.

- The rates of incidents and vulnerability reporting highlight the ineffectiveness of current organizational structures, authorities, and responsibilities
- DON's decentralized cybersecurity governance structure has multiple parties able to block initiatives and no effective escalation methodology, making it difficult to modernize or maintain information systems configuration control across the enterprise
- The DON cybersecurity governance structure is characterized by an almost exclusive focus on compliance metrics based on a snapshot in time, which inhibit the ability to anticipate and/or adapt to current and future threat environments
- DON resource sponsors and program managers' acquisitions structures are not conducive to implementing evolving cybersecurity risks mitigation within systems lifecycles
- Horizontal flow across the DON, other Services and Agencies, programs of record and their supporting defense contractors of threat and vulnerability information sharing is hindered due to vertically stove piped organizational structures
- Updating of guidance's too often requires wholesale modifications of major policies and doctrine making them frequently outdated, inhibiting the ability to keep pace with or anticipate evolving threats
- DON has multiple uncoordinated modernization efforts underway in different domain areas, this lack of a unified effort presents areas of vulnerability where systems that are not optimized and properly configured come in contact with critical mission systems as a result of US Joint Staff Interoperability Requirements²³

Structure inhibits USN-USMC DDCIO from achieving unity of effort

The responsibility of executing the CIO role has been delegated to a Vice Admiral (three-Star) who is the N2N6 (below the CNO and Vice Chief of Naval Operations (VCNO)) and within the USMC, a BGen (one-star) who is Director, C4 (below the Commandant and the Deputy Commandant for Information (DCI)).²⁴ However, as previously noted these two seniors lack the necessary authority to hold their subordinate enterprises accountable for compliance.

A 2011 memorandum from the UNSECNAV designating N2N6 and HQMC C4 as DDCIOs does not specifically enumerate their cybersecurity responsibilities nor does it designate a DON CISO.²⁵ It is also important to note that both the N2N6 and HQMC C4 offices have many other significant responsibilities, among them running the very networks they are responsible for governing. This arrangement makes it cumbersome for the DDCIOs to mandate a unified cybersecurity message across the USN and USMC. These network, system and data ownership authorities and responsibilities are not optimally aligned horizontally across the enterprise, and lack unity of effort which inhibits best practices.

The service Secretaries have recently raised concerns that new weapon systems are not being designed to be interoperable among Service Branches.²⁶ This is representative of how the

²³ Joint Staff, 2018, Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms. Interoperability is the ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together.

²⁴ Department of the Navy CIO, 2018, Organizational Structure

²⁵ Department of the Navy CIO, 2011, Organizational Structure

²⁶ USNI News, 2019, Say New Weapon Systems Must be More Interoperable Among Branches, <https://news.usni.org/2019/02/08/41001>

lack of synchronized cross-service cybersecurity authorities ensures that next generation systems will continue to be burdened with supporting fielded legacy systems and subsystems. There are multiple examples where various programs and subsystems have forced a major system to continue the use of these legacy systems, thereby exposing all other systems integrated alongside them to greater risk.

These sorts of issues can only be addressed by the highest levels of each service.

The DON is not unique in these matters

In August 2017, the Government Affairs Accountability Office found that only 4 of the 24 Federal Agencies had clearly defined CIO incremental development certification policies and processes in place that contained descriptions of the role of the CIO.²⁷ In August 2018, a follow-on GAO report found that none of the 24 agencies selected in their research had policies that fully addressed the role of their CIO, as called for by current law and guidance.²⁸ Additionally, officials from 21 of the 24 agencies in the GAO's review reported that bureaucratic challenges and inefficient governance processes hindered their ability to implement incremental development.²⁹

Changes to the NDAA

In order to address these problems, the US Congress has amended the 2018 National Defense Authorization Act (NDAA) to add language empowering the DoD and Service CIOs' roles. This new language ensures that DoD IT acquisitions have been reviewed for technical standards compliance. Of note:

Section 909 of the 2019 NDAA states:

“(3)(A) The Secretary of a military department or head of a Defense Agency may not develop or procure information technology (as defined in section 11101 of title 40) that does not fully comply with such standards as the Chief Information Officer may establish.”

Additionally,

“(B) The Chief Information Officer shall implement and enforce a process for-
“(i) developing, adopting, or publishing standards for information technology, networking, or cyber capabilities to which any military department or defense agency would need to adhere in order to run such capabilities on defense networks; and

²⁷ Government Accounting Office, 2017, Agencies Need to Improve Certification of Incremental Development

²⁸ Government Accounting Office, 2018, Agencies Need to Improve Certification of Incremental Development

²⁹ Ibid

“(ii) certifying on a regular and ongoing basis that any capabilities being developed or procured meets such standards as have been published by the Department at the time of certification

Despite the NDAA mandate above, the changes to date in the DON organizational structure have not yet produced the authorities and accountability intended by the law. DON governance structures remain characterized by stovepipe organizations and commands with competing priority, authorities, and responsibilities. Additionally, the DON has yet designated a single, dedicated, fulltime, and empowered authority who is both responsible and accountability for management across the entire naval enterprise.

Structure Recommendations

Improve top-down governance

SECNAV should reassess the decision to combine the CIO and CMO secretariat functions into the UNSECNAV position as well as the dispersal of much of its authorities and accountabilities into the uniformed military service deputies. The SECNAV should establish a full-time dedicated DON CIO with proper authorities, responsibilities and accountability who operates above the assistant secretaries and whom reports directly to SECNAV. This is in line with corporate best practice and the May 2019 Executive Order which directed the CIO position should report directly to the Agency head.³⁰

SECNAV should task the DON CIO with reviewing all DON IT systems acquisition programs to identify gaps in technical standards compliance as well as to determine if there are mitigation plans in place for programs operating in the absence of acceptable standards. This oversight should also include acquisition programs for national security systems used for tactical and strategic communications as the vendors providing the DON with this technology have been heavily targeted by foreign CNO activities.³¹

Beyond elevating the CIO to a SECNAV direct report:

- SECNAV, assign DON CIO all responsibility for cybersecurity/IT policy and technical standards as well as the authority to set modernization deadlines and standards
- SECNAV, establish a CISO that reports directly to SECNAV, whose responsibilities do not conflict with the CIO
- SECNAV, grant the DON CIO approval authority over the procurement of IT systems to ensure compliance with all current cybersecurity standards.

³⁰ Office of the President of the United States, 2018, Enhancing the Effectiveness of Agency Chief Information Officers

³¹ The term “national security system” means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function or use of which: involves intelligence activities, cryptologic activities related to national security or involves command and control of military forces or involves equipment that is an integral part of a weapon or weapons system or is critical to the direct fulfillment of military or intelligence missions (with the exception of routine administrative of business systems) or stores, processes or communicates classified information.

- DON CIO, collaborate with interagency organization to incorporate greater numbers of systems engineers for the forensic analysis of computer network exploitation events to better inform the DON of the impact of data loss
- DON CIO, direct the incorporation of cybersecurity threat and vulnerability information throughout the acquisition life cycle of weapons systems

Chapter 5: Process

The Role of Process as a Governance Tool to Achieve Cybersecurity Resiliency



Figure 5: Process should be defined, host improvements, be adoptable, and sustainable. CSRR, 2019

Top-performing organizations employ a dynamic array of processes that underpin their information and cyber operations, which serve as top-down force and effectiveness multipliers while balancing peak efficiency adherence with rules, policies, and regulations. Their processes also enable the organization to constantly learn and adapt to changes in the environment or competitive threats, ensure accountability, and inform decisions at all levels.

The best private sector processes for cybersecurity are forged from formal examples such as LEAN or Six Sigma. Whatever process is used, serves to achieve desired outcomes in a streamlined manner that takes advantage of agile capabilities which deliver consistent situational awareness, counters persistent threats, and minimizes risk.

Process Best Practices

Processes industry employs to achieve cybersecurity resiliency

The Review learned that best-in-class organizations have invested in authoritative processes that produce desired outcomes to secure data and maintain the integrity of their networks. Common among them are processes that are fully funded and deployed enterprise-wide:

- Governance-led enterprise approach to cybersecurity—achieving enterprise-wide standardization
- Visible cybersecurity health and monitoring of effectiveness—dashboards displaying current status of Platform Information Technology (PIT)-control systems³² and scorecards accumulating details of how the company is performing in cybersecurity
- Prevalent information sharing across all business sectors—achieving awareness of the latest cyber threats and the best way to counter them
- Implementation of Privileged Access Management (PAM)—achieved through a zero-trust model that determines appropriate levels of access to the network
- Prioritization of critical information—achieving common agreement about the “crown jewels” that must be protected, because everything cannot be protected
- Reduction of exploitable vulnerabilities—achieving assertive configuration management by eliminating archaic systems and investing in standardized modern systems

³² Committee on National Security Systems, 2015, Glossary. Platform Information Technology (PIT)-control systems include combat and weapons systems; navigation systems; propulsion systems; and hull, mechanical, and electrical systems to include systems, infrastructures, or software contractually operated on behalf of the U.S. Navy.

Comprehensive, well-defined, enterprise-wide cybersecurity governance plan

The enterprise approach to cybersecurity, practiced by the best companies, includes processes that assure cybersecurity is built in from inception and proactively updated. The challenge is different for DIB companies that build in cybersecurity based on resource sponsor requirements. The best companies CIOs and CISOs keep CEOs aware of enterprise-wide cybersecurity issues through weekly briefings. Those briefings help enable the CEO to manage risk and assure accountability. 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.

Additionally, PIT-control systems, generally managed by the CISO, and OT that direct what happens in physical plants or processes is closely aligned with and managed to meet company security standards.³³ There is no separation of standards between IT and OT. Finance and industry best practices assure that every application on their networks is either compatible with existing cybersecurity capabilities or is deployed with a capability that meets enterprise standards. The best companies have painfully learned that exceptions to this rule generally have resulted in lost revenue and are therefore not tolerated.³⁴ They protect their data and systems by first identifying critical information that must be protected within their enterprises and their key supply chain providers, then aggressively protect those “crown jewels.” Best-in-class companies also determine who should have access to that information strictly on a need to know basis. Finally, best-in-class companies invest in their people in multiple ways, including formal and informal training followed by testing with phishing and other exercises to assess the workforce’s ability to recognize and counter cyber threats.

Constant visibility of cybersecurity health and monitoring of effectiveness

Knowing and understanding the health of their PIT-control systems and the data hosted within is a key concern for industry. A variety of processes are used to achieve this knowledge. All companies the Review visited have dashboards within the “C suite” which allows hourly and daily monitoring of their networks, including endpoints, servers, and the Internet of Things (IoT). Their relevant, data-rich dashboards provide an instantaneous view on the status of their networks. Their network operators have the authority to take immediate action against cyber actors, including blocking, quarantining, monitoring, or, with more aggressive capabilities, execute response actions as needed. Their scorecards are another tool that help best-in-class companies make informed decisions about how to improve monitoring and better invest in cybersecurity capabilities.

Highly skilled cybersecurity operators use very technical displays to view logs, metadata, system speed/bandwidth usage, and other technical information. Their displays paint a common

³³ Governance Insights Center, 2018, How Your Board Can Better Oversee Cyber Risk, 4

³⁴ Almost every company interviewed holds strongly to the belief that poor cybersecurity practices causes them to lose their competitive edge over national and international competitors. They are also held to regulatory finance commission rules, that if not followed, can result in exuberant fines.

view such that every senior executive can appreciate, including the reality of the common persistent threats and the company's ability to withstand those threats. Others display in very clear terms, the overall status of their networks and data that enables anticipatory actions. The best of these data rooms look very similar to an air or surface common operating picture. However, for successful companies it does not stop there.

To assure their practice of using dashboards achieves desired outcomes, companies' CIOs, CISOs and Chief Risk Officers (CRO) develop scorecards to constantly assess the validity and usefulness of the data they monitor, and they regularly present these to the CEO and appropriate leadership. These scorecards are also used to assess the effectiveness of testing the workforce regarding phishing, outage, recovery, and other exercises. Scorecards are later used to help inform cybersecurity investment levels that preserve or enhance capabilities, workforce, and cost-benefit outcomes. Additionally, the information they gain about the effectiveness of their cybersecurity efforts against threats to their PIT-control systems are shared with other companies trying to counter the same or different threats.

Prevalent information sharing across all business sectors

Information sharing is prevalent as a best practice among companies that achieve effective cybersecurity. The sharing begins in house to help baseline the workforce to the cyber threat. Although companies aggressively protect proprietary information, they realize that sharing cyber threat information with other companies increases their own chances of success against cyber actors. Some of this is done CIO/CISO to CIO/CISO through their threat intelligence contract providers and others through their trade and professional associations. Of interest, some of the companies have access to cyber threat briefings (at lower levels of detail or clearance) from the same government organizations the DON relies such as the Department of Homeland Security (DHS) and the Federal Bureau of Investigations (FBI). This agency information sharing includes both passive and active briefings with company CIOs and CISOs, which are done over privileged network access (passive) or face-to-face briefings (active). Common among all successful companies is the CEOs' direct interest and continuous involvement about what the CIO, CRO, and CISO discover.

Implementation of Privileged Access Management (PAM)

Best-in-class organizations have strong processes for determining appropriate levels of access to the network. These processes begin with System Administrators who have the greatest potential to cause unintentional, or intentional, problems on the network. System Administrators are the most tightly regulated because they have permissions with access to extremely sensitive data. Their access is task- and time-bound and may require a "two-person to execute" rule. As to the rest of the users, many companies have adopted a Zero-Trust model which, in spite of all the in place back ground checks, training and financial self- interest, assumes no one can be trusted. This is especially important because most companies and individuals the Review met with identify the insider threat as the most persistent and challenging to counter, once the other state of the art controls are in place. The insider threat can be intentional and malicious or unintentional and careless. What drives this approach is the potential of immense destructive

consequences to these companies due to carelessness—the companies do not rely on their cultural norms to create error free employees

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. Additionally, technical validation, such as aggressive red teaming and spear phishing exercises, add an additional layer to validate a company's processes by testing not only employees' but also all senior executives' adherence to company policy about opening potentially malicious email—this is treated as a serious insider threat act, not a forgivable “careless mistake”. Additionally, many companies do not allow use of personal email or social networking accounts to pass through corporate firewalls. These progressive technologies are not always developed by the companies that employ them. Successful companies aggressively seek to employ the next better commercially-developed technologies that are resident in PIT-control systems and/or those that can be purchased as a capability upgrade.

Prioritization of critical information

Best-in-class companies assertively define and prioritize protection of the “crown jewels” (*those proprietary capabilities and others that give companies a competitive edge*) because they realize they do not have the resources to protect everything. This is not a singular decision, but one that is based on the CIO's and CISO's assessment of vulnerability and risk based on threat information briefings and importance of proprietary capabilities that must not be allowed to fall in competitor hands. Protection of these capabilities can be costly, but the CEO's assessment and final decision to “swarm” all protective capabilities around the “crown jewels” is often based in a determination that the benefit of protection far outweighs the cost. The processes to protect this information and capabilities involve consistent assessment of their importance to revenue and is closely tied to consistent monitoring through dashboards and assessing overall protection efforts through scorecards. CIOs and CISOs keep CEOs and Board Membership aware of the status of protection of these “crown jewels,” without fail.

Reduction of exploitable vulnerabilities

Best-in-class companies consistently investment in configuration management to reduce their vulnerability to cyber actors. This investment includes processes to eliminate barriers, such as outdated policy, vertical stovepipes of system ownership, and the lack of sufficient resources for progressive technology implementation. Aggressive and dispassionate configuration management has helped reduce a vast number of disparate systems to a manageable few that are required to use the same basic operating systems enabling simultaneous updates and patches through limited, if not single, action. Other actions, such as multifactor authentication and tighter security on remote access to company servers and services, help reduce man-in-the-middle attacks and other vulnerabilities associated with remote access.

Several organizations the Review visited went beyond best-in-class to cutting edge progressive technologies that reduce their network vulnerabilities and counter cyber threats. One such company invested \$600 million to improve their cyber platform in its entirety scrapping their entire proprietary IT and OT platforms and replaced them with state-of-the-art systems based in shared infrastructure to enable software sharing using Platform as a Service (PaaS)/Container as a Service (CaaS) for software applications. These systems are easily upgradable to the latest security controls; can receive patching across the entire enterprise instantly; and can monitor workforce access through data analytics supported by Artificial Intelligence (AI) and Machine Learning.

State of Today's Naval Service Process

DON processes do not achieve cybersecurity resiliency requirements

The naval service, by its very nature, is a process-oriented organization. The US Naval Nuclear Propulsion Program, Naval Air Training Operation Procedures and Standardization, and the Navy Occupational Safety and Health Program have some of the most recognizable rigid processes. With the introduction of DoD's RMF instruction, which directs a structured cybersecurity risk process and the Cybersecurity Safety Program (CYBERSAFE), which is intended to set technical standards to achieve resiliency in mission critical warfare systems, the DON also pursues rigid processes for cybersecurity. Yet, the September 2018 National Cybersecurity Strategy recognizes shortfalls in DoD-wide cybersecurity processes and has directed change:

"The Administration will integrate supply chain risk management into agency procurement and risk management processes in accordance with federal requirements that are consistent with industry best practices...This includes ensuring better information sharing to improve awareness and reduce duplicative supply chain activities...This effort will be synchronized... These standards and practices should be outcome-oriented rather than point-in-time company specifications."³⁵

Despite being one of the world's most expansive and capable process-oriented organizations, the DON's well-known rigid and codified processes, while making some progress to improve cybersecurity, remain widely deficient. Simply put, the DON processes too often have been ineffective in staying ahead of the threat. Some key examples include:

- Navy secretariat installing four-year-old Windows 10 in February 2019
- USS Gerald R. Ford being commissioned and delivered with Windows XP
- LCS and DDG-1000 class ships being developed with excepted IT networks
- CYBERSMART buildings constructed without cybersecurity built-in
- Legacy warfare systems kept in service with no plan to update or add cybersecurity

³⁵ White House, 2018, National Security Strategy, 2

- The Navy’s own network, Navy/Marine Corps Intranet (NMCI), continues to operate under an Interim Authority-to-Operate (IATO) status with no view in sight for full ATO

The DON’s approach has been to establish numerous, stand-alone cybersecurity processes that often result in stovepipes that are focusing on adherence to compliance-based rather than outcome-based processes. Compounding the challenge is a lack of common metrics and poor articulation of the threat that combine to compromise unified prioritization of risk-to-threat based resourcing decisions by the DON and the DIB. Without processes that can provide a clear understanding and appreciation of the risk, it is difficult to properly resource cybersecurity capabilities that can help protect against threats to the various cyber-based enclaves and thereby achieve cybersecurity resiliency within the DON. The ever-growing sophistication of external persistent threat vectors against networks, supply chains or from intentional or unintentional insider threats, drive a requirement for modernized policies, practices, and processes which enable an unimpeded threat sharing processes. The lack of common standards and processes makes accountability difficult, in fact, it is rarely achieved. For the ongoing, undeclared, cyber war. Current DON cybersecurity processes and authorities lack the clarity and agility necessary to achieve desired outcomes across the entire operating environment and win.

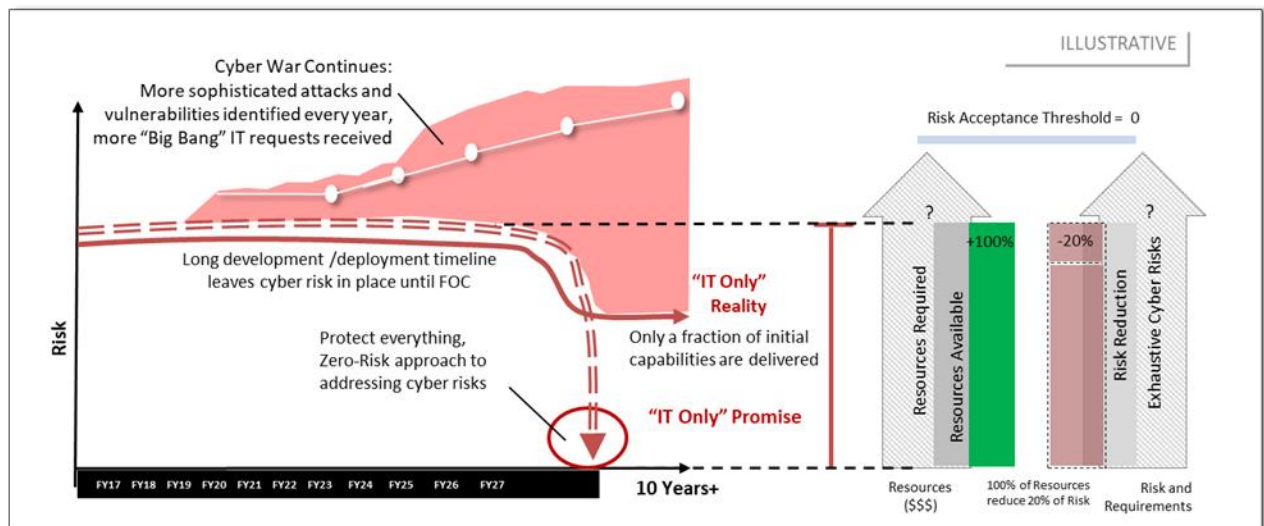


Figure 6: Key observations in the current state of the DON: Lack of a cyber-Common Operational Picture across the DON; Inability to communicate cyber risks and requirement in UNCLASS investment / resourcing processes; lack of a consistent means to identify, prioritize and resource short term, medium-term, and long-term cyber risk mitigation projects. Stewart, DON DUSN (M), 2017, (Cybersecurity Overview and Financial Considerations)

Ineffective top-down governance

The DON’s governance processes for cybersecurity are rife with compliance-oriented systems, non-standardized risk metrics, inhibited and prohibited threat sharing policies and practices, lack of accountability for not achieving standards, and obsolete processes to determine who should have access to networks. While current DON processes posture the organization to be successful in 20th Century ship centric “blue water” conflicts, they are highly ineffective in

21st Century information-dependent, highly-networked cyber centric conflicts. The Review documented numerous discrepancies and inefficiencies that are sub-optimizing DON's current cybersecurity effectiveness and are challenging the organization's goal to maximize its lethality.

These deficiencies and discrepancies are largely a result of inconsistent, top-down governance. A lack of overarching CIO or CISO strategy, guidance, and oversight are quantifiable obstacles to establishing effective processes and cybersecurity. As but one of many examples, the CYBERSAFE program, which the Navy is using to develop its hygiene standards, while the Marine Corps is leveraging RMF to establish its standards. This separation of effort constrains agility when the services will be stressed by actual amphibious and seaborne air combat operations.

In contrast to the best of the private sector where resourcing decisions for information resilience and cyber defense are top down driven the DON employs a massive committee-based trading mechanism. The Cybersecurity EXCOM is co-chaired by the VCNO and the Executive Director, Assistant Secretary of the Navy, Research, Development, and Acquisition (ASN (RD&A)). It is a 3-star forum that includes every N-Code director, including OPNAV N2N6 in their role as DDCIO, on the Navy staff and the CMC DC I as the DDCIO on the Marine Corps staff. The committee meets biannually for the primary purpose of making Programming Objective Memorandum (POM) recommendations for cybersecurity investments.³⁶ In theory, the EXCOM, with an authoritative process for informing POM funding is what the DON needs in the current-day cyber threat environment. In practice, however, the EXCOM does not have the requisite cyber situational awareness and authority to direct POM investments for cybersecurity.³⁷ Additionally, the EXCOM does not have the agility, nor does it meet frequently enough, to make timely and relevant decisions. Many of the Flag and General Officers the Review met with indicated that the EXCOM has little to no authority and therefore is ineffective.

Additionally, other ongoing organized efforts to assess or counter cyber threats, such as the Supply Chain Risk Management Working Group (SCRMWG) and Naval Critical Programs and Technology Committee (NCPTC) are not required to provide their findings to the EXCOM. Lack of formal coordination between these efforts, and identified authority overall, compromises development of a common, effective database for the most critical programs and technologies that must be protected. In contrast to the best of the private sector, there is no process for the DON to assess the effectiveness of assuring cybersecurity is built into new technologies or reviewing the effectiveness for sustainability of cybersecurity for deployed programs. DON milestone and gate reviews are instead used for this purpose. There is a cybersecurity Key Performance Parameter (KPP) required for Joint Capabilities Integration and Development System (JCIDS) documents, but language is standardized to meet compliance requirements with no real follow-up. For Planning, Programming, Budgeting, and Execution (PPBE) cycle Gate Reviews, cybersecurity assessment is only required in gates 1-3.

³⁶ DCNO for Cybersecurity OPNAV N2N6G, 2018, Navy Cyber Resiliency Investments. The EXCOM Purpose Statement Includes: 1) Review the Navy's cybersecurity risk posture across the entire cyber platform; 2) Determine strategic programmatic changes required to reduce risk; 3) Ensure required programmatic actions are executed, and review the effects of investment

³⁷ The EXCOM has successfully advocated for \$3.1B for cybersecurity investments since 2014 supporting efforts such as Task Force Cyber Awakening, Engineering Enclave Boundary Defense, NC3, and others. The issue here is that the EXCOM can only make recommendations. Resource Sponsors are the final authority for how much, if any resources they will allocate for cybersecurity capabilities.

Poor situational awareness

In contrast to the best of the private sector, there is no common cyber operational picture akin to the Air and Surface Common Operational Picture (COP) used in tactical platforms and Maritime Operations Centers (MOC). The Review was struck by the lack of performance indicators for a leadership that grew up operating big machines with dials and gauges for everything. For cyber there are none. As such, the DON processes deprive leadership of the true status of cybersecurity performance. What substitutes are glib comparatives (“we are better than the Army or the Air Force”) which reinforce the false confidence in the current cybersecurity posture. Furthermore, the lack of cyber dashboards or scorecards deprive leadership of situational awareness necessary to make informed risk investment decisions.

DON has no uniform or effective cybersecurity metrics to quantify the threat, influence resourcing, or operational planning. There is no overarching means to assess DON’s risk to mission, lives, or future planning based on ongoing compromises. In best-of-class enterprises this would be unacceptable. Proper assessment tools would enable the DON to be more proactive against cyber threats, provide better balance of resources, and ultimately maximize naval power. Without consistent situational awareness improvement and comprehensive assessment, overall processes will stagnate, a forward-leaning ability to counter cyber threats will not exist, and resource allocation will continue to be imbalanced. Without such process tools, it is impossible for the SECNAV, CNO, and CMTD, to properly fulfill their roles as executive agents for cybersecurity. For their DON CIO and CRO to clearly articulate the nature of the existential cyber threat they too must have full situational awareness and the tools to consistently achieve it. Furthermore, the CRO should be able to assess the risk posture by establishing a Risk Board to drive accountability throughout the enterprise.

Inefficient information sharing

Processes for sharing information and protecting sensitive but unclassified and critical information have failed and continue to fail. For the current cyber war, DON threat information sharing, and forensic investigation assessment processes only advantage our opponents. The DON’s relevant industry associations argue that small and medium-sized enterprises could better address the threats if only they were given better threat understanding.³⁸ However, threat and best practice information sharing processes operate in a vertical manner and are not producing desired outcomes. Many companies consider information sharing processes to be too restrictive and over-compartmentalized; largely due to under resourced investigations that are unable to provide the source, nature, and classification of incidents at the pace dictated by the ongoing cyber war.

The Defense Cyber Crime Center (DC3) conducts forensics on classified and unclassified logs, but the time it takes for breached companies to deliver the logs and the lack of manpower, once logs are received, often renders essential threat information nearly irrelevant by the time it is shared. The Naval Criminal Investigative Service (NCIS) conducts investigations and operations; forensics; and threat warning and analysis, but cooperation from vendors is not always forthcoming. National Cyber Investigative Joint Task Force (NCIJTF) facilitates threat

³⁸ The NDIA Cybersecurity for Advanced Manufacturing Joint Working Group, 2017, Cybersecurity for Manufacturing Networks

sharing, but prioritization of much of their efforts is based on membership (see appendix B). Navy and Marine Corps Intelligence provides technical and operational intelligence analysis for the purpose of alerting SECNAV, OPNAV, acquisitions, and law enforcement of foreign cyber threats, but DON's intelligence organizations are not adequately resourced to provide the needed level of support. The Damage Assessment Management Office (DAMO) which provides an assessment of the nature or impact of data losses must also wait for forensics to be completed and also suffers from a shortage of personnel to provide timely assessment. Even if there were an ability to accelerate these processes, there still exists the inability to accurately assess the fully burdened cost of cyber—cost to develop a program, cost to scrap it if it becomes too risky to deploy, and cost of research and development to replace it.

The processes for reporting cyber incidents, conducting forensics analysis, and sharing information are well-founded in basic intelligence cycle processes, but do not provide the expected outcomes in the volumes and manner to support timely proactive action against the threats from a rapidly evolving global peer. This is most notable against the insider threat because cybersecurity resources allocated to mitigate the insider threat are not commensurate with the immediacy of the threat. Reporting through the DIBNet web-based External Certification Authority (ECA) program makes it relatively easy for participants to gain awareness about breaches.³⁹ However, even with a 72-hour requirement to report an incident companies are often slow to report because, in addition to various other reasons, they want to avoid embarrassment to their company. Depending on the size of logs and available personnel, forensics analysis can take months to years before NCIJTF can facilitate sharing of threat information and DAMO can provide an assessment on the impact of data loss.

Inability to identify and prioritize critical programs and technologies

Similarly, but not entirely applicable to identifying and prioritizing the “crown jewels” for industry, the DON must identify and prioritize information needed to ensure lethality, sustainability, and what is needed to grow, strengthen, and enhance the enterprise. However, the process for identifying the criticality of PIT-control systems and subsequently vital cybersecurity threat information against them, including the impact of their compromise is wanting. Additionally, there are no means to identify or interdict components that are compromised in the supply chain allowing leaders to agree on a “GO/NO-GO” decision about continued development.

The goal of the CYBERSAFE program, in terms of new programs, is to assure, through the JCIDS process, that cybersecurity is built-in to warfare programs from inception. For programs in sustainment, SYSCOMs employ the Systems Engineering Technical Requirements (SETR) process to retrofit systems that were built without cybersecurity or require cybersecurity upgrades to meet the CYBERSAFE technical standards. However, in practice the CYBERSAFE program and SETR process is unevenly executed by resource sponsors, requirements officers, and program managers that are not sufficiently trained or understand the authorities to adapt what they are delivering as needed. Further complicating the issues is that the Navy and Marine Corps apply different standards to address processes for security control, program grading, audit, certification, and software chain risk management. Although the CYBERSAFE program was

³⁹ Defense Information Systems Agency, 2016, Information Assurance Support Environment

revamped in 2018 to help align cybersecurity technical standards, the absence of specific conditions based top-down governance does not inspire horizontal integration across the DON.

Using different standards is challenging. As an example, Marine air and ground units deploy on Navy ships and without the same cybersecurity standards, cyber vulnerabilities will persist and continue to create exploitable seams; including a higher probability that new technologies will be compromised before delivery. Additionally, manual, and automatic Red-Team testing and probing of DON systems, platforms, or installations are not based on evolving threat realities or common standards. This in turn disrupts a unified process to immediately identify and remove high-risk technologies from the supply chain or deployed line and replace them with trusted, properly vetted capabilities. Different standards also compromise program managers' ability to be kept apprised of co-development challenges of software and hardware capabilities. This includes processes to mitigate vulnerabilities from newly adopted technologies, such as 5G, rendering new software and hardware capabilities slow to develop and ineffective by the time they are delivered.

With no codified process to identify and prioritize DON's critical programs and technologies that meet modern cybersecurity standards, cybersecurity readiness will be questionable throughout the lifecycle of all DON PIT-control systems. These are all outcomes that have to be driven by the UNSECNAV who has the authority and responsibility for IT standards and resourcing in his role as DON CIO. However, by allowing the Navy and Marine Corps Deputy DON CIOs to build their programs independently, the outcome is a set of vertical stovepipes rather than horizontal implementation of capabilities that would otherwise achieve unified approaches to the most critical programs and technologies.

Too many widely exploitable vulnerabilities

The 2018 Mandiant Special Report assesses that industry organizations continue to struggle with reducing their network vulnerabilities.⁴⁰ The DON is no exception and has traditionally regarded access to unclassified systems as a privilege afforded to every member. Over time, much sensitive but unclassified data has been accumulated on unclassified networks and the wide access puts that information at a greater risk.

In addition to enterprise networks such as NMCI, OCONUS Navy Enterprise Network (ONE-NET), Consolidated Afloat Networks and Enterprise Services (CANES), Marine Corps Network (MCN), the DON operates nearly 50 excepted networks that do not enjoy the same configuration management standards as the enterprise networks. Configuration management is difficult to achieve because the DON is littered with archaic systems that cannot support modern cybersecurity standards, have cybersecurity bolted-on in a manner that compromises full function of the system, or simply have no cybersecurity at all. The DON is also slow to incorporate modern, more secure capabilities such as access to cloud services. These inconsistencies expand the DON's network vulnerabilities and have the potential to introduce greater risks across the enterprise.

⁴⁰ Mandiant, 2018, M-Trends, 22

High-risk unsecure DIB

The Review was struck with how an enterprise that instantly goes to general quarters in a hull breach, has moved so lethargically with the flood of breaches of significant sensitive data. Despite forward-leaning efforts by the DIB Executive Steering Committee (ESC), the DIB continues to hemorrhage critical data. The processes employed by this multi-organization committee resulted in an ASN (RD&A) undersigned memorandum that directs program managers to change Contract Data Requirements Lists (CDRL) for new and existing contracts to reinforce DIB compliance⁴¹ and associated security controls.^{42 43} The memorandum demands aggressive timelines for Covered Defense Contractors (CDC) to meet standards. Yet, despite the ongoing cyber war, the timelines have not been enforced, additional auditing requirements for security controls have not been instituted, permissions for naval law enforcement to scan partner networks have not been granted, and the theft of IP from the DIB relentlessly continues. DoD CIO issued a similar memorandum that provided guidance for CDRLs that reinforces the requirement for companies to make their System Security Plans (SSP) available and adds a requirement for top-tier companies to track the cybersecurity compliance of their subordinate companies.⁴⁴ Yet, there is no accountability for these requirements.⁴⁵ These failures to reform can only be remedied with aggressive action by Secretary and his Chiefs.

Antiquated cybersecurity for the naval critical infrastructure

It is not beyond imagination that someday a naval combatant would fail to sail because the supply system vectored the wrong grade of lube oil for the LM2500 engines; upon reaching its rendezvous point, a tanker was not available to refuel a hungry bomber because the tanker was maliciously directed elsewhere; or all electricity and backup systems to a satellite control station failed during a complex Ballistic Missile Defense or Tomahawk missile strike. Processes to prioritize investment in naval critical infrastructure are ineffective, there is no common agreement about prioritized Task Critical Asset (TCA) and Mission Relevant Terrain-Cyber (MRT-C) lists that forces action; the condition of TCA and MRC-T has not driven appropriate funding for repair and upgrade to current-day cybersecurity standards; cybersecurity requirements for new programs of record are not observed throughout naval or JCIDS processes from cradle to grave; and CYBERSAFE technical standards and requirements have not been fully exercised to assure integrity of naval critical infrastructure, including cyber smart buildings. Simply put, processes to assure integrity for the DON owned critical infrastructure have not been effective, placing logistics, power, communication, maintenance, and other services at high risk.

The naval critical infrastructure, essential to the DONs warfighting success, is also at great risk. However, the DON must look beyond traditional categorization and redefine critical infrastructure from the perspective of an opponents that seeks vulnerabilities to delay or disrupt our ability to deploy or sustain through out every phase of a peer on peer war. This is well

⁴¹ DFARS Clause 252.204-7012, 2015

⁴² National Institute of Standards and Technology, 2015, NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

⁴³ Geurts, 2018 Implementation of Enhanced Security Controls on Select Defense Industrial Base Partner Networks

⁴⁴ DoD CIO, 2018, Cybersecurity Memorandum

⁴⁵ Chief of Naval Operations, 2018, Defense Industrial Base Incident Reporting Requirements. This Navy Message directed that upon notification of a cybersecurity incident from DC3, DAMO shall report the incident via OPREP 3 reporting format. The first of these reports was successfully issued in 22 February 2019.

beyond the infrastructure that is Government-Owned/Government-Operated (GO/GO); GO/Contractor Operated (GO/CO); CO/GO; and CO/CO such as piers and repair docks that supply power, deliver supplies, and conduct repairs and upgrades with heavy cranes for combatants, or forward air refueling bases that supply airborne tankers with fuel for fighter and bomber aircraft; and SCADA grids that supply primary and redundant power to MOCs. Whatever form the ownership takes, the DON must apply and enforce cybersecurity resiliency standards.⁴⁶

Cybersecurity processes and capabilities on track should be celebrated and accelerated

In some areas the DON has demonstrated an ability to move in the right direction to improve cybersecurity in PIT-control systems while still delivering uninterrupted lethality. Leveraging industry best practices, the Deputy CIO Navy has gone full speed ahead to deploy the Compile-to-Combat in 24 Hours (C2C24) capability throughout the Fleet.⁴⁷ C2C24 has been developed in accordance with the CYBERSAFE program technical standards. Moreover, it embraces the use of commercial cloud to assure the availability of data in any operating environment; including employment of Security Development Operations (SecDevOps) and other progressive technical standards. C2C24 moves away from a hardware-based architecture in favor of data as a service through agile software capabilities which can be delivered securely (uncompromised) and reside on existing already-approved hardware. The expectation is that if C2C24 can work on the lowest common denominator of the Fleet with respect to bandwidth availability, it can work anywhere throughout the fleet.⁴⁸ C2C24 deployment is an excellent example of the DON leveraging commercial capabilities and assuring that cybersecurity is built in from inception and extended to associated systems. C2C24 must be established as a program of record and funded immediately.

Process Recommendations

Effective DON top-down governance can achieve cybersecurity resiliency

Cyber, like other warfare areas, must have processes that are characterized by relevant speed, anticipation, awareness, well-established metrics, agile cyber threat sharing, and comprehensive standards with enforced accountability and intolerance for failure due to carelessness. Overall, the processes should ideally lead the threat, and if attacked, have the resiliency to ensure that the naval force can get to or remain in the fight.

Beyond requirements of strategy and policy, the current cyber environment drives a requirement for cybersecurity processes to dynamically inform war-gaming scenarios, fully contribute to net assessments, and authoritatively inform or alter programs and resourcing

⁴⁶ Chief of Naval Operations, 2015, Publication of the Chief of Naval Operations Shore Investment Guidance. Among other requirement, the message directs a) Strengthen the resilience of critical assets and their supporting infrastructure against physical and cyber threats. Owners and operators of critical assets will collaborate with installation leadership to take proactive steps to identify threats and manage risk and; b) CNIC and NAVFAC will review mission assurance and asset management processes to create a single measure of *facility criticality* capable of supporting investment prioritization for POM-18 deliberations.

⁴⁷ Deputy Chief of Naval Operations for Information Warfare (N2N6), 2018, Transforming Our End-to-End Information Environment: Compile to Combat in 24 Hours Implementation Framework. A successful pilot was tested in Spring 2018 in USS ESSEX (LHD 2) and USS STOCKDALE (DDG 106) using CANES as the supporting hardware architecture.

⁴⁸ CHIPS Magazine, 2018

allocation. Processes must serve to enable a culture that instills a narrative to animate the DON to seamlessly counter cyber threats. The processes must assure the workforce is properly trained, incentivized, and recognized for taking ownership of mission objectives and the DON recruits and retains a force which recognizes cybersecurity as a core element of warfighting, from SECNAV actual to the E1 who will join tomorrow. The processes must drive the Department to a structure that lends itself to unmitigated horizontal traceability, accountability, and proper authority. Finally, processes must inform resource investment to achieve prioritized and balanced capabilities to counter the assault on DON information and PIT-control systems while still retaining multi-pronged lethality.

The Department has taken some steps to modernize processes that attempt to outpace risk to the DIB and DON. New governance processes such as the Cybersecurity EXCOM, DIB-ESC, Cyber Resiliency Requirements Working Group (WG), and DoD Top Ten Cyber Risk WG are some examples of these efforts. Capability investments such as C2C24, Navy Cyber Mission Assurance Integration Platform (NCMAIP), and DIBnet/ECA point in the right direction to shore up DON's cybersecurity concerns. However, further change is required to give these efforts authority and horizontal impact in a manner that eliminates stovepipes and responsibly reduces redundancy while simultaneously streamlining processes to achieve an outcome-oriented mindset, and exercise authoritative accountability processes for meeting cybersecurity objectives.

Enforce top-down governance

DON must take advantage of industry best practices to improve its cybersecurity process. A single authority must be responsible for cybersecurity processes that align with overarching strategy and guidance. The DON must rapidly employ end-point protection and network intrusion products uniformly across the organization and everyone must be required to uniformly comply. To improve processes such as systems configuration management, prioritization balancing, and supply chain confidence, bodies such as the EXCOM must be given relevant knowledge and authorities. Given the high rank of the EXCOM membership, it would be appropriate to grant the body authority to direct resource allocation; determine prioritization of critical programs and technologies; and direct discontinuation of programs and technologies, as well as supply chain components that do not meet cybersecurity standards. Without such authorities, the EXCOM's effectiveness will remain in question.

Increase situational awareness

The DON must demand immediate improvement to cybersecurity situational awareness. Situational awareness of the security of warfare systems is analogous to situational awareness of the air, surface, and subsurface COP. Commanders must know if their systems are secure and must understand level of vulnerability and associated risk to the threat. Additionally, threat information must be shared across the DON and DIB to enable stake holders to shore up their cyber platforms to confront current and emerging threats.

- SECNAV, direct DON CIO to develop uniform cybersecurity metrics to inform a scorecard that quantifies the threat and influences resourcing or operational planning

- SECNAV, direct DON CIO to develop scorecards in a manner that can help decision makers determine return on investment (RoI) of cybersecurity capabilities
- SECNAV, institute a cybersecurity risk assessment process through which a CRO and associated Enterprise Risk Board can assess effectiveness and accountability
- DON CIO, direct ASN (RD&A) and DCNO IW to leverage industry, finance, technical, and other warfare areas to develop cybersecurity dashboards that show, at a minimum, status of cybersecurity to warfare systems, current threat, vulnerability, and risk to current threat, ongoing cyberattacks, and others
- DON CIO, direct DCNO IW to determine a method for displaying dashboard information where a central facility, such as FCC, Fleet Forces Command (FFC), and Commander, US Pacific Fleet (CPF) can observe the full picture
- DON CIO, direct ASN (RD&A) to develop a method whereby Program Managers can review and make decisions based on relevant dashboards and make “GO/NO-GO” decisions about continued development of programs & technologies in the DIB
- DON CIO direct ESH II and III commands to conduct disaster exercises to test DON processes under pressure

Improve information sharing

Ever-growing sophistication in persistent threat vectors against networks; supply chains; and intentional and unintentional insider threats, drive a requirement for modernized policies, practices, and processes that enable unimpeded threat sharing processes. The Finance Industry has demonstrated impressive success by robust horizontal sharing processes. The Secretary must work to ensure eliminate inhibitors of success such as restrictive law, the lack of manning, or the over-compartmentalization of information.

- SECNAV, coordinate with DoD to develop processes to ensure that incident reporting, forensics analysis, and information sharing provide the expected outcomes to support timely proactive action against threats
- SECNAV, direct DON CIO to Develop authoritative processes with proper accountability that break down stovepipes and over compartmentalization of threat information
- SECNAV, direct DON CIO to effectively rebalance cybersecurity resources from a compliance-based to a risk-based standard to assure that allocations are commensurate with the immediacy of the threat
- DON CIO, direct ECH II and III commands to develop scenario-based interactive training about the current insider threat that will motivate the workforce to take appropriate action against the threat

Identify and prioritize critical programs and technologies

The DIB builds capabilities in accordance with resource sponsor requirements and should provide program managers and developers with clarity about which programs must be protected. SYSCOM Technical Authorities must follow set cybersecurity technical standards in accordance with the CYBERSAFE program, to identify the criticality of various components that make up a

system. This is important because since there are not enough resources to protect everything, the DON must assure that the most critical capabilities are delivered uncompromised.

- SECNAV, direct DON CIO to develop overarching guidance to identify and prioritize critical programs and technologies
- SECNAV, ensure the “Supply Chain” is delivered uncompromised to guarantee mission readiness
- SECNAV, empower the Cybersecurity EXCOM with authority to direct and audit resources for cybersecurity to support protect critical programs and technologies
- SECNAV, direct that any high-risk technologies are immediately removed from the supply chain and replaced with trusted capabilities that have been vetted through established processes
- SECNAV, direct DON CIO to standardize Navy and Marine Corps processes for achieving technical standards for cybersecurity
- DON CIO, direct ASN (RD&A) to incorporate processes and requirements that assure Program Managers are kept apprised of co-development challenges of software and hardware capabilities
- DON CIO, ensure that the EXCOM be provide requisite data to make informed decisions on cybersecurity investments

Reduce exploitable vulnerabilities

Cybersecurity must be seen as an integral part of any acquisition in the DON. This means that resource sponsors must demand and track cybersecurity implementation throughout development and sustainment of programs.

- SECNAV, direct DON CIO to fully incorporate cybersecurity into new and existing programs
- SECNAV, direct DON CIO to reduce the use of non-enterprise networks, where practical
- SECNAV, direct DON CIO to establish configuration management across the DON enterprise
- SECNAV, direct DON CIO to accelerate development and standardization of remote access to cloud services
- SECNAV, direct DON CIO to determine cybersecurity “go/no-go” criteria for developing capabilities at all milestone and Gate Reviews
- SECNAV, establish automated PAM processes such as zero-trust-models to determine who should have access to sensitive data and who should hold administrative privileges
- SECNAV, direct DON CIO to establish processes to accelerate configuration management by eliminating archaic systems that cannot support modern cybersecurity standards; this includes perceived irreplaceable weapons and data systems
- SECNAV, direct DON CIO to develop processes to model impact of all exploitable IP and networks in war games and exercises

Secure the DIB

Despite forward-leaning efforts by the DIB-ESC, the DIB continues to hemorrhage critical data. CDCs must meet timelines and improve security control in accordance with the ASN (RD&A) cybersecurity and DoD memorandums.

- SECNAV, direct DON CIO to develop processes for DON DIB partners to receive meaningful monthly briefings that indicate level of risk against their programs and technologies
- SECNAV, direct DON CIO to develop processes to include DIB partners in discussions about prioritization guidance for critical programs and technologies that must be protected
- SECNAV, direct DON CIO to work with named associations (Aerospace Industries Association (AIA), National Defense Industrial Association (NDIA), Professional Services Corporation (PSC)) to develop processes for sub-prime contractors to improve defenses against the threat
- DON CIO, direct ESH II and III commands to develop processes to model impact of exploited programs and technologies in war games and exercises

Modernize cybersecurity for the naval critical infrastructure

Naval critical infrastructure is fundamental to the success of naval mobility, logistics, communications, and combat. Without assurances that capabilities which enable these fundamental naval missions will be available when required, every mission is at an unacceptable risk.

- SECNAV, empower the Cybersecurity EXCOM with authority to direct and audit resources for cybersecurity for protection of naval critical infrastructure
- SECNAV, direct DON CIO to institute assessment processes to assure that cybersecurity capabilities for all critical naval infrastructure is kept on line and up to date with approved and relevant standards
- SECNAV, require legacy critical naval infrastructure conform to modern and relevant cybersecurity standards.
- SECNAV, identify and defend the additional critical infrastructure our opponents will/might destroy or disrupt to interfere with the naval enterprise deploying or sustaining a long peer fight
- SECNAV, direct processes for gates 1-6 reviews and all JCIDS Milestone Reviews that assure cybersecurity standards are in place when new naval critical infrastructure is brought on line / determined fully mission capable

Chapter 6: Resources

Resources as a Governance Tool to Achieve Cybersecurity Resiliency

Resource allocations are the means by which leaders can achieve strategic objectives and message priority shifts. In an era where information and data are so critical, the foundational pillars of culture, people, structure, and processes must be properly resourced for successful mission accomplishment. Thus, resource allocation is the first among equals of the levers available to the Secretary to transform the naval enterprise to information centric.

Resources Best Practices

Fully-informed resource allocation

Best-in-class companies have risk registers that shape priorities and assign accountability, which in turn dictates resource allocation. This enables a clear understanding of the benefits from cybersecurity and amount of resources necessary for it.

A typical large, global company informs its resource requirements with an Enterprise Risk Management (ERM) process based on Committee of Supervisory Organization (COSO) principles. The ERM process involves a comprehensive compilation of risk events or scenarios, including the probability of occurrence, and the financial and operating impact of such occurrence. This model incorporates all forms of risk across the enterprise ranging from geopolitical to operating and financial. External elements including legal, regulatory, and compliance matters are also factored in, typically with binding minimum constraints.

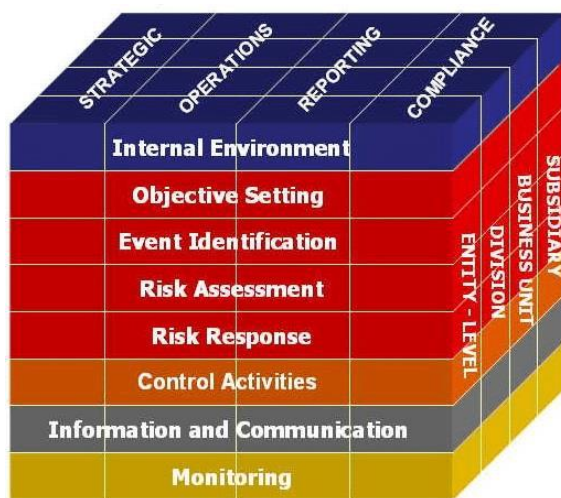


Figure 7: The COSO ERM process is frequently illustrated by the above cube

This often results in increased or reallocated resources to cybersecurity requirements in response to a greater awareness of the scope, scale, and impact of potential cyber damage. Most companies allocate and reallocate funds based on this kind of risk analysis.

In certain industries, such as financial services, it has become increasingly important to be cyber secure as both a regulatory requirement, and to build “trust” equity.

Benefits of cost is well understood

In 2015, a major software company estimated that \$3 trillion of US market value was destroyed by cybercrime.⁴⁹ These enormous losses changed the way industry looked at cybersecurity, and the level resources they were willing to commit to achieve it.

The magnitude of cyber spending in the best of the private sector is notable. A senior researcher at an investment bank detailed that “spending about 3% of company’s capex (capital expenditures) on IT and security is relatively low.”⁵⁰ According to a major research group, industry projected a 2019 forecast growth of 8.7% in cybersecurity spending, which will equate to \$124 billion.⁵¹ In contrast, DOD reported \$8.5 billion in cybersecurity funding in FY2019, a \$340 million (4.2%) increase above the FY2018 estimate.⁵²

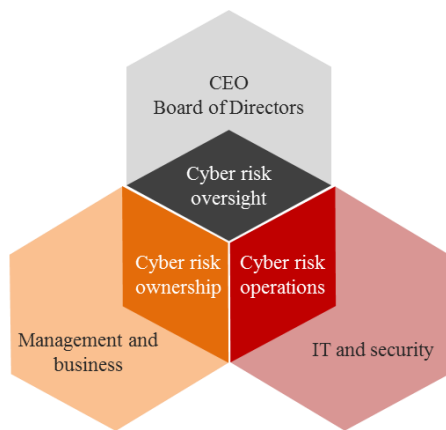


Figure 8: Functional Best Practice in Cyber Risk management. (Price Waterhouse)

The Exostar Cyber Security Questionnaire, which measures a company’s cybersecurity risk, is one of several methods that many companies are adopting to better understand cybersecurity risk within an organization and to improve their resource allocation. This enables an understanding that cybersecurity is not a dart board where the correct solution is found randomly with wasted resources, but in fact, is based upon deciding those priorities that need to be protected then considering their cost of defense vs the investment to develop those priorities or their value to the enterprise.

Careful balance of resources

The best organizations can quantify cyber-related consequences in terms of risks to capital, revenue, and operations. However, this is rarely done to an auditable level of precision, rather it is only enough to enable risk informed assessment. This understanding of the fully-burdened cost of the investment and costs from failure is also important to the ability of the workforce to identify all the risks to their operations from cyber threats. In these organizations, cybersecurity and other organizational operational functions are carefully balanced through risk informed assessments with embedded cyber outcomes, that dictate the prioritization and speed of deliverables.

Resources are prioritized according to risk and benefit

For private sector and non-government organizations, there is a very serious need to remain agile and not be burdened by unnecessary bureaucracy. The best organizations survive

⁴⁹ Markus, 2016, Complacency over cybercrime cost \$3 trillion in 2015

⁵⁰ Morgan, 2017, Cybersecurity Market Report

⁵¹ Aitken, 2018, Global Information Security Spending to Exceed \$124B in 2019

⁵² Office of Management and Budget, 2018, An American Budget

on the margins, and live or die by their effectiveness. Accordingly, they aggressively seek out and remove unnecessary organizational impediments, enabling the workforce to make the right decisions. They know their entire organization could die if they are the victim of a cyber-related incident, so they have in place lean and quick acting threat and vulnerability processes and an efficient and effective risk calculus.

Another recurring theme from industry is that effective cybersecurity must be a continuous, multidimensional process and not dependent upon episodic events. Resource management for cybersecurity is not a “fire and forget” process.

All successful companies have common simple operating concepts, including:

- Know that cyber is an enterprise-wide business issue, not an IT issue
- Maintain risk oversight with access to cyber expertise
- Understand legal and regulatory requirements
- Have a cyber-strategy and plan
- Monitor the cyber program
- Ultimately, monitor cyber resilience⁵³

The largest reported and most impactful event in the financial industry was Equifax’s data breach. This breach came with an initial cost estimate of \$4 Billion.⁵⁴ The financial service industry has since seen that the reallocation of resources to physical hardware on the boundary is but one part of the solution. Major financial companies reacting or anticipating to cyber challenges are allocating resources across the organization and working as a team to address threats.

These include resourcing for the following:

- Allocate resources based upon value, not lowest cost
- Mandate visibility into all Supply Chain vulnerabilities
- Design every contract be cyber resilient
- Fund talent retention and recruitment
- Build a counter fraud program and ensure data integrity
- Implement an insider threat program
- Promote external partnerships/collaborations, even with competitors

⁵³ Price Waterhouse Cooper, 2018, How Your Board Can Better Oversee Cyber Risk

⁵⁴ Lim, 2017. Equifax's Massive Data Breach Has Cost the Company \$4 Billion So Far

State of Today's Naval Service Resources

Resources are not prioritized or balanced appropriately

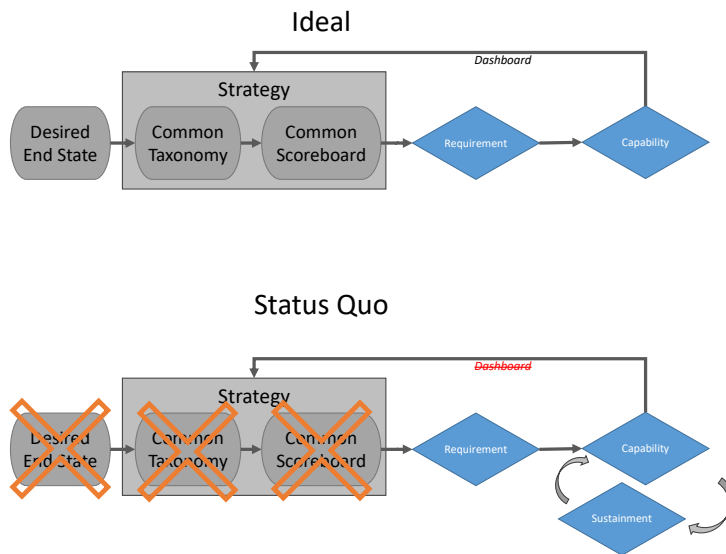


Figure 9: Resourcing Strategy Models

Regrettably, in stark contrast to industry best practice and executive branch guidance, the DON cyber resourcing (as to both financial and human resources) does not reflect its level of importance in magnitude or time shifts.

The Review was unable to estimate, with any confidence, the total cybersecurity resource posture of the DON, as there is no provision for explicit separation of cybersecurity expenditures in the current operating scheme. As such we are unable to suggest what the appropriate level of funding should be.

The ability to properly resource is limited by the inability to fully understanding the cost or benefit of the impact of cybersecurity expenditures across the DON enterprise. The prioritization and utilization of resources from program to program is also variable and often appear to be more of a function of the perspective of the individual program leadership, not a function of specific policy mandates.

Complicated processes make tracking money and expenses for cybersecurity difficult in all industries. But the process within the DoD/DON are orders more complex. Current DoD/DON governance of IT/Cyber is driven by a maze of "...multiple, often overlapping senior governance committees, functional oversight committees and processes, advisory boards, and corporate, which have proliferated over time, resulting in many inefficiencies and sub-optimal decision-making that is dramatically slower than our global competitors."⁵⁵ These decision making entities must

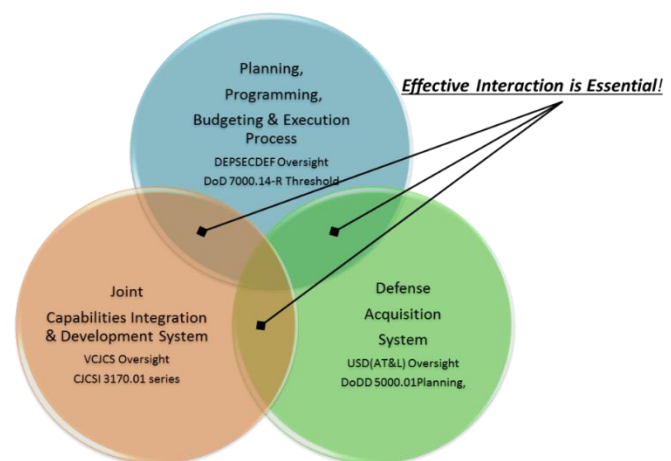


Figure 10: Interaction of the JCIDS, PPBE, and DAS process

⁵⁵ DoD, 2015, Department of Defense Information Resources Management Strategic Plan Version 1.0

“bolt-on” cybersecurity while adhering to congressionally mandated requirements, resourcing, and acquisition processes (Figure 11). Also, the lack of agility in the existing JCIDS, PBBE, and Acquisition processes coupled with constraints of existing policies and other DoD processes prevent the delivery of capability at pace with the threat.

Chief among these many entities is the Cybersecurity Executive Committee EXCOM, the governance body created in 2014 to validate cybersecurity funding and prioritization on a quarterly basis. Its goal is to move towards the “Ideal Model” from the “Status Quo Model,” however, it lacks the common taxonomy and risk scoring metrics necessary to effectively identify the level of required resources and prioritization.

The EXCOM also lacks sufficient authority to direct the expenditure of funds for cybersecurity. As an example, the EXCOM proposed the 2014 cyber resiliency strategic approach, however, it was funded for only 1/3 of the original resourcing request during the five-year plan beginning in PB17, which equated to 1/3 of the product or implementation.

These are two negative outcomes that can occur in the absence of a true enterprise-wide approach that would imbue the EXCOM with appropriate responsibility and authority. Without the proper responsibility, appropriate authorities, and feedback loop, the EXCOM will continue to be unable to fulfill its charter.

DON does not associate the cost of cybersecurity with expected benefit

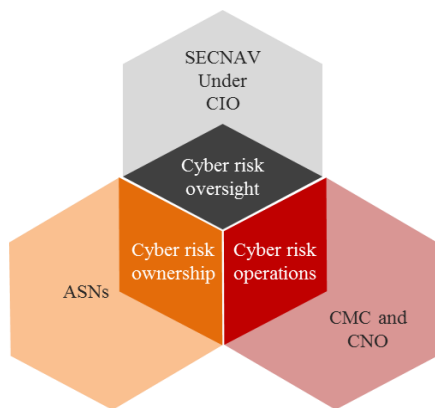


Figure 11: Current State of DON Functional Best Practice in Cyber Risk management

Cost, the investment to obtain a capability, is generally known. On the other hand, value, the more important metric, is the total benefit to be achieved to the warfighter from an improved capability, or the shift of advantage if ceded to an opponent. The inability to denominate those consequences makes it difficult to determine how much is too much to spend to protect a particular capability.

The value of IP being lost within the defense contracting companies and from DON data is enormous and of undetermined cost or value. Even when known, damage assessments typically are not portrayed as investment dollars lost or as a capability casualty. The additional question from

leadership that should flow after every breach is what will be the “cost” to purchase the capability necessary to neutralize the now shifted advantage, and the additional cost necessary to regain the lead in that capability area?

The prioritization of what should be protected must be related to the allocation of resources and to the risk of losing important data. The DON has always been challenged to accurately align resources to requirements. The DON is unable to effectively measure cybersecurity investment due to a lack of visibility in PPBE process. Individual line item

resource allocations are not properly tagged to the cyber security mission area and as such are not easily audited or linked to measurable outcomes.

Ineffective budgeting allocation of cybersecurity resources in acquisition

The acquisition community’s historical, and nearly exclusive focus on cost, schedule & performance, has failed to anticipate the emergence of “security” as a key performance parameter (KPP) in the face of aggressive penetrations by our adversaries, which has resulted in critical vulnerabilities not appropriately prioritized in the PPBE process. This has been aggravated by the inability of program managers to understand or adequately characterize and measure the marginal value of a cybersecurity investment dollar.

Additionally, within the DIB, the implementation of enhanced security controls on select partner networks is a starting point to ensure prime contractors doing business with the DON are adhering to basic cybersecurity practices. Also, the USD(I) MITRE report “Deliver Uncompromised,” has raised awareness, but once again has not sufficiently changed behavior, demonstrating that the DON “turning circle” remains considerably longer than our opponents.

The Review does not believe there will be a significant increase in resources for the DON in the near future. AI, quantum computing and other seemingly silver bullets being pursued by the Department’s research and development enterprises are likely years from being military reality. Therefore, the leadership’s focus on these science projects risks reducing resourcing and attention to immediate and material challenges at hand.

Resources Recommendations

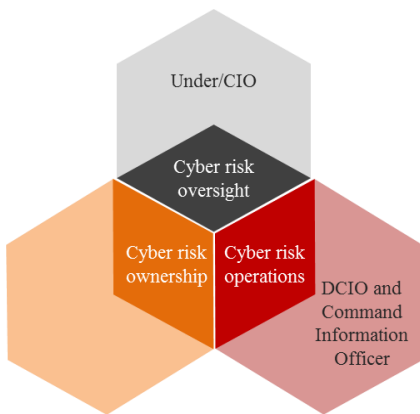


Figure 12: Desired State of DON Functional Best Practice in Cyber Risk management

Resource allocation for cyber must include both new investments and the reprioritization of current investments. This can only be done by a CIO that is fully empowered and whose sole position and purpose is to aggressively monitor, audit, investigate, adjust, and reallocate resources across the DON enterprise with impunity and no other distractions or programmatic responsibilities. Programmatic responsibility such as running networks or systems would position a CIO to be prioritized rather than driving prioritization.

To ensure maximum return on service or equipment/software from industry, defined enterprise standards must be adopted. Standardization of requirements includes horizontal allocation of resources across the DON and DIB. The connection of resources and requirements are imperative within the DON and essential when providing requirements external to the DON.

Senior leaders within industry are adamant that the DIB is as well provided with one set, not multiple requirements, from across the DoD and DON. Standardized requirements will enable industry to work more efficiently, driving cost down for the government.

Improve prioritization of resources

Resourcing everything means the protection of nothing. The DON must identify the “Crown Jewels” at all levels of classification, not just for the sensitive non-classified categories. The NCPTC provides the initial facilitator to identify the DON critical programs. This identification is not simply the program or technology that ensures lethality, but extends to controlling and sustaining processes, talent management, and removing inefficient and time-consuming business plans. However, the methodology currently employed is slow and has limited influence on priorities outside the DON.

- SECNAV, identify and direct the review all critical cyber programs, systems, technologies, and processes to ensure adequate attention and resourcing
- SECNAV, establish a more effective process that prioritizes cybersecurity resource commensurate with the current and projected threat against systems, mission, and forces
- Assistant Secretary RD&A, ensure cybersecurity is a priority in trade-off decisions among program life-cycle cost, schedule, and performance objectives

Improve balance of resources

Cybersecurity for DON networks and IT must have prominence within the resourcing decisions to ensure it is being appropriately budgeted.

- SECNAV, resource cybersecurity requirements in parallel with new programs and address funding requirements for programs currently in sustainment that have no, or inadequate cybersecurity
- DON CIO, remove vertical stovepipes and align resources for PIT-controlled systems in a horizontal manner that eliminates unnecessary redundancies and inconsistencies in prioritization when measured against the threat
- DON CIO, establish a framework to appropriately fund cybersecurity for infrastructure, data, and PIT-control systems
- DON CIO, chair the EXCOM governance structure to effectively balance resources for cybersecurity investment

Improve allocation of cybersecurity resources within cybersecurity budgets

The DON must ensure a common taxonomy of the cybersecurity budget is capturing accurate costs and is executed for its intended purpose. This includes a complete and common characterization across the DON which is shared with other services and understood by the DIB. No matter the situation, the assumption should be that the network is not secure enough if the adversary has penetrated a network that contains DON critical data.

- SECNAV, lead an effort to work with sister services to establish a standard acceptable to CAPE as to what qualifies/defines essential cybersecurity cost benefit metrics to better inform the allocation of resources

- SECNAV, mandate auditing of cybersecurity inflection points across the DON in order to provide metrics for better allocation of resources
- SECNAV, order a review to accurately determine the necessary increase of resources for entities and organizations that find breaches and conduct damage assessments, (Counterintelligence/Law Enforcement response, intelligence analytical apparatus, and red teams)

Associate cybersecurity as a cost with a benefit

Cybersecurity should be seen in more dimensions than just cost. This is especially important when enabling the DIB with requirements and metrics-based outcomes.

- SECNAV, direct an exploratory resource sponsor to provide a government controlled operational network to DIB N-tier small businesses, or provide grants to those who self-perform to cybersecurity standards
- SECNAV, direct ASN (RDA) with CIO coordination to create specific metrics and feedback loops to ensure industry is adhering to DON standards and requirements following DON assistance to N-tier companies
- SECNAV, direct ASN (RDT&E)/DAMO to develop processes to capture, track, and maintain an assessment of the fully burdened cost of cyber
- DON CIO, mandate that N-tier suppliers immediately adhere to the top 10 NSA cybersecurity recommendations and limited “Deliver Uncompromised” with performance incentives based upon Exostar type of security assessments
- SECNAV, immediately order the cessation of operation of non-compliant DON and DIB systems that store, transport or process “crown jewel” data until existing security controls are certified sufficient to achieve the established standard

Final Thoughts

All great leaders aspire to leave the organization entrusted to them better than when they took over. The truest legacy is leaving behind something of enduring quality within the institution and its people. As the leader of the Department of the Navy, your passion and deep affection for this great institution and its people are well known. Asking for the tough scrutiny of this report is a manifestation of your willingness to search for ways to make the Navy and Marine Corps even better.

Effective and enduring change best occurs when leaders strengthen others' capacity to learn, to reflect, and to extract meaning from their learning. This report frames what it takes to do just that. The challenges enumerated throughout this report are immense, but the Navy is a learning institution, its leaders and people are up to the task. With the leadership's complete focus, we believe what is now existentially threatening can be turned into decisive advantage.



Appendix A
THE SECRETARY OF THE NAVY
WASHINGTON DC 20350- 1000

October 12, 2018

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Cybersecurity Review Tasking Memo

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.

Complacency and an unwillingness to confront this challenge are not an option. We must examine, enhance, and where necessary create, cybersecurity policies, procedures, processes, and behaviors that deny adversaries access to our most important information. We must fully understand the root causes of these compromises, protect ourselves and reexamine how we train, organize, and operate in this environment.

To that end, I am directing a comprehensive cybersecurity review that will examine our cybersecurity posture focusing on the current organizational and industrial base environments in which several significant compromises of classified information have occurred. Our experts will examine the Navy's current cyberspace governance structures to assess if they are optimally focused, organized, and resourced to prevent serious breaches. It will further investigate our end-to-end cybersecurity processes to ensure alignment of authority, accountability, and responsibility with government and industry best practices. I have directed our experts to accomplish the following:

- Review the series of material breaches over the past 18 months to identify common failures and the Navy's post event actions.
- Review the appropriateness of the enterprise architecture's alignment of authority, responsibility, accountability, and resource allocation.
- Review the appropriateness of the Navy's organizational culture and that of its supporting contractors.
- Examine incentives and reward systems to ensure alignment with cybersecurity goals, objectives, training, and performance.
- Examine the Navy's end-to-end cybersecurity strategy, governance, policies, and procedures for the protection of Navy information.
- Develop fully implementable immediate-, mid-, and long-term recommendations to ensure that the Navy administers, maintains, and abides by best-in-class cybersecurity practices.

SUBJECT: Cybersecurity Review

Our team will be led by Michael J. Bayer and include William H. Swanson, John M. B. O'Connor, and Ronald S. Moultrie. They will be further assisted by Bryan G. Whitman and a team of senior civilian and military personnel with immense expertise in this field. This review will touch every element of our enterprise, and I am counting on you to give the team your full support and cooperation. Just as important, I know that many of you have invaluable experience and expertise in this domain and the team welcomes your insights and recommendations.

The team will ensure their work is informed by and complements the work of the Department of Defense Chief Information Officer. This team will complete their work and provide me with their findings and recommendations in early Fiscal Year 2019.



Richard V. Spencer

Distribution:

n:

USN

CNO

VCN

O

ASN(RD&A)

ASN(M&RA) OGC

ASN(FM&C)

ASN (EI&E)

DON/AA

DNS

DMCS

NCIS

CHINF

O OLA

CNR

JAG

NAVI

G

AUDGE

N OCH

Appendix B

List of External Organizations Consulted

Industry

Natl. Def. Industrial Assoc.

CEO, NDIA, Gen (ret) Hawk Carlisle
COS, NDIA, MG (ret) James Boozer
VP Divisions, NDIA Dave Chesebrough
CIO Northrup Grumman, Mike Papay
Leidos, Lt Gen (ret) William Bender
McGrath Analysis, Dr. Mike Mcgrath,
ANSER, Mrs. Kaye Ortiz,
Raytheon, Mrs. Holly Dunlap
Attorney RJO, Mr. Robert Metzger,
Dir, A&DGF, Mr. Ezra Hall
Draper Labs, Titako "Rocky" Takapu
CISO BAE, Jeffrey C. ("J.C.") Dodson,

Aerospace Industries Assoc (AIA)

COO, AIA LTG (ret) Bob Durbin
CIO, AIA Mr. Bob Lenny

Interagency

National Security Agency

Dep Dir, NSA/CSS, Mr. George Barnes
CSO, Mrs. Cindy Widick
Senior Advisor, Cybersecurity, Hon. Mr. Rob Joyce
CIO, Mr. Gregg Smithberger
Assoc. Dep Mission Manager, National Security Systems, Michael Lamont
CSO (Tech Director), Mr. John Lockwood
NSA External Relations, Howie Larrabee,
Cyber Executive, Dave Frederick

IC Task Force(s) [FBI-CPC]

NCSC, Bill Evanina
NCIS, Jay Doyle
DC3, Steve Shirley
White House, NSC, Josh Steinman
Task Force, Bob Giesler
Defense Science Board, Bill Schneider
DSS, Mr. Richard Naylor
DHS, Janet Manfra
Asst. Dir, FBI, Mr. Matt Gorham

Finance

Sullivan and Cromwell Lawyers-ISAC
1-800-Flowers
Encore Financial Partners
Belmont Savings Bank / BSB Bancorp Inc.
Investment banking Wells Fargo
CLS Group Brown Brothers Harriman
NY Stock Exchange / Intercontinental Exchange
Goldman Sachs
JP Morgan Chase
Black Rock

Tech Companies

Microsoft, Mr. Mark McIntyre
Microsoft Corporation
Amazon Web Services
Sony

Appendix C

List of DoD Personnel Consulted

Military

CNMF, Brig Gen Timothy Haugh
Deputy CDR, CNMF, Mrs. Terri Kondos
USCC, Deputy J5, Mr. Mike Clarke
JS J6, Lt Gen Bradford Shwedo
DOD CIO, Dana Deasy
ASN (EI&E), Mr. James Balocki
DISA, VADM Nancy Norton
O4 Panel
VADM (ret) Jan Tighe
USD (I) Mr. Joseph Kernan
Joint Staff J3, VADM Mike Gilday
Defense Innovation Unit, Mike Brown
OSD (CAPE), Robert Daigle
N2N6, VADM Matt Kohler
Dep N2N6, Mr. Mark Andress
Defense Science Board, Bill Schneider
DWO, Mrs. Margaret Palmieri
ASN (RD&A), Mr. James F. Geurts
DON CIO, Thomas Modley
DCI, LtGen Lori Reynolds
HQMCC4, BGen Lorna Mahlock
FCC/C10F, VADM TJ White
VCNO, ADM William Moran
USD (P), John Rood
USD INDPOL, Eric Chewning
USCC J3, MajGen Charles Moore
Dir Net Assessment, Mr. Jim Baker
DON IG, VADM Rick Snyder
NAVIFOR, VADM Brian Brown
Dep NAVIFOR, Mr. Matthew Swartz
CO, NCDOC, Captain Julia Slattery
OPNAV N8, VADM William Lescher
SPAWAR, RADM Christian Becker
OPNAV N1, VADM Robert Burke
OPNAV N4, VADM Dixon Smith

Appendix D

Cybersecurity Readiness Review Team

Principals

The Honorable Michael Bayer, Chairman
Mr. John M.B. O'Connor, Principal
Mr. Ronald S. Moultrie, Principal
Mr. William H. Swanson, Principal

Executive Director

Mr. Bryan G. Whitman

Team Members

Captain James W. Adkisson III, USN
Mr. William Bridgette
Lieutenant Commander Jacob Foster Davis, USN
Mr. Jaurette Dozier
YNC Brandon Gollehon, USN
Mr. Kevin Roberts
ITCM James Simon, USN
Mr. Alan Stocks
Special Agent Laukik Suthar

Appendix E

Acronym List

AI	Artificial Intelligence
AIA	Aerospace Industries Association
ASN (RD&A)	Assistant Secretary of the Navy for Research, Development, and Acquisition
ATO	Authority-To-Operate
C2	Command and Control
C2C24	Compile -to-Combat in 24 Hours
CANES	Consolidated Afloat Networks and Enterprise Services
CDC	Covered Defense Contractor
CDRL	Contract Data Requirements List
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CJCS	Chairman of the Joint Chiefs of Staff
CMO	Chief Management Officer
CNO	Chief of Naval Operations
CPF	Commander, Pacific Fleet
CYBERSAFE	Cybersecurity Safety Program
DC3	Defense Cyber Crimes Center
DCI	Deputy Commandant for Information
DCNO	Deputy Chief of Naval Operations
DEPSECDEF	Deputy Secretary of Defense
DIB	Defense Industrial Base
DIB-ESC	DIB Executive Steering Committee
DoD	Department of Defense
DON	Department of Navy
DON DAMO	DON Damage Assessment Management Office
EXCOM	Executive Committee
FCC/C10F	Fleet Cyber Command / Commander Tenth Fleet
FFC	Fleet Forces Command
GNP	Gross National Product
IA	Information Assurance
IoT	Internet of Things
IP	Intellectual Property
IT	Information Technology
JCIDS	Joint Capabilities Integration and Development System
MRT-C	Mission Relevant Terrain-Cyber

MCN	Marine Corps Network
MOC	Maritime Operations Center
MOS	Military Occupational Specialty
NCIJTF	National Cyber Investigative Joint Task Force
NCMAIP	Navy Cyber Mission Assurance Integration Platform
NCPC	Naval Critical Programs and Technology Committee
NDAA	National Defense Authorization Act
NDIA	National Defense Industrial Association
NMCI	Navy/Marine Corps Intranet
NSA	National Security Agency
ONE-NET	OCONUS Navy Enterprise Network
OPNAV	Office of the Chief of Naval Operations
OT	Operational Technology
PIT	Platform Information Technology
POM	Programming Objective Memorandum
PPBE	Planning, Programming, Budgeting, and Execution
PSC	Professional Services Corporation
RMF	Risk Management Framework
RoI	Return on Investment
SCADA	Supervisory Control and Data Acquisition
SCRMWG	Supply Chain Risk Management Working Group
SecDevOps	Security Development Operations
SECNAV	Secretary of Navy
SRR	Strategic Readiness Review
SSP	System Security Plans
SYSCOM	Systems Command
TCA	Task Critical Asset
TFCA	Task Force Cyber Awakening
USMC	United States Marine Corps
USN	United States Navy
VCJCS	Vice Chairman of the Joint Chiefs of Staff
VCNO	Vice Chief of Naval Operations

Bibliography

- Ackerman, Robert, K. 2015. "Marines Strive for Holistic Network Improvements." *SIGNAL AFCEA*. December 1. Accessed March 1, 2019. <https://www.afcea.org/content/Article-marines-strive-holistic-network-improvements>.
- Aerospace Industries Association. 2018. "National Aerospace Standard 9933: Critical Security Controls for Effective Capability in Cyber Defense." *Aerospace Industries Association*. December. Accessed January 28, 2019. <https://www.aia-aerospace.org/issue/cyber-security/>.
- Aitkin, Roger. 2018. "Global Information Security Spending to Exceed \$124B in 2019: Privacy Concerns Driving Demand." *Forbes*. August 19. Accessed December 9, 2018. <https://www.forbes.com/sites/rogeraitken/2018/08/19/global-information-security-spending-to-exceed-124b-in-2019-privacy-concerns-driving-demand/#4c060aa27112>.
- Bayer, Michael, and Gary Roughead. 2017. *Strategic Readiness Review*. Readiness, Washington DC: US Navy.
- Bruhn, Michael L. 2015. *Department of Defense Cybersecurity Culture and Compliance Initiative (DC3I)*. Memorandum, Washington DC: Pentagon.
- Burgess, Christopher. 2015. "Data Security Requires a Symbiotic Relationship Between the CFO, CIO and CISO." *Security Intelligence*. April 8. Accessed January 14, 2019. <https://securityintelligence.com/data-security-requires-a-symbiotic-relationship-between-the-cfo-cio-and-ciso/>.
- Chandler, Scott. 2017. "Rethinking Defense Acquisition: Zero-Base the Regulations." *War on the Rocks*. January 6. Accessed January 7, 2019. <https://warontherocks.com/2017/01/rethinking-defense-acquisition-zero-base-the-regulations/>.
- Chief of Naval Operations. 2019. *Defense Industrial Base Incident Reporting Requirements*. Navy Message, Washington DC: US Navy.
- Chief of Naval Operations. 2015. *Pulication of the Chief of Naval Operations Shore Investment Guidance*. Navy Message, Washington DC: Chief of Naval Operations.
- Coats, Daniel R. 2019. *National Intelligence Strategy*. Washington DC: Director National Intelligence.
- Coats, Daniel R. 2018. *Worldwide Threat Assessment of the U.S. Intelligence Community*. Statement for the Record, Washington DC: Director of National Intelligence.

- Commission on Enhancing National Cybersecurity. 2016. *Report on Securing and Growing the Digital Economy*. Accessed February 27, 2019. <https://www.nist.gov/document/cybersecurity-commission-report-final-postpdf>.
- Committee on National Security Systems. 2015. "Committee on National Security Systems Instruction No. 4009,." *CNSS Instruction 4009*. Washington DC: Pentagon, April 6.
- Cybersecurity Insiders. 2018. "Insider Threat 2018 Report." *CA Technologies*. Accessed February 2019, 2019. <https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf>.
- Dark Owl. 2017. "The Dark Owl Index US Government Edition: Ranking US Government Agencies Using Darknet Intelligence." *Dark Owl*. August 8. Accessed January 22, 2019. <https://www.darkowl.com/news/2017/owl-cybersecurity-announces-darknet-index-ranking-government-agencies-by-darknet-footprint>.
- Defense Information Systems Agency. 2016. *Information Assurance Support Environment*. Accessed December 14, 2018. <https://iase.disa.mil/Pages/index.aspx>.
- Defense Intelligence Agency. 2019. *DIA-02-1706-085 China Military Power: Modernizing a Force to Fight and Win*. Assessment, Anacostia: DIA.
- Department of Defense. 2015. *Department of Defense Information Resources Management Strategic Plan Version 1.0*. Plan, Washington DC: DoD.
- Department of the Navy CIO. 2018. *DON Office of the CIO (OCIO) Leadership Team*. May 9. Accessed January 25, 2019. <https://www.doncio.navy.mil/ContentView.aspx?ID=645>.
- Department of the Navy. 2017. "Department of the Navy Cyber Glossary: Terms and Definitions." Washington DC: Pentagon.
- . 2011. "Organizational Realignments and Designation as the DON DCIO (Navy) and the DON DCIO (Marine Corps)." *Department Of the Navy Chief information Officer*. May 11. Accessed January 26, 2019. <https://www.doncio.navy.mil/ContentView.aspx?ID=2225>.
- Deputy Chief of Naval Operations for Information Dominance. 2014. *Task Force Cyber Awakening*. Memorandum, Washington DC: Pentagon.
- Deputy Chief of Naval Operations for Information Warfare (N2N6). 2018. *Navy Cyber Resiliency Investments*. Washington DC: Chief of Naval Operations.
- Deputy Chief of Naval Operations for Information Warfare (N2N6). 2018. *Transforming our End-to-End Information Environment: Compile to Combat in 24 Hours Implementation Framework*. Naval Message, Washington DC: Chief of Naval Operations.

- DeSimone, Antonio, and Nicholas Horton. 2017. *Sony's Nightmare Before Christmas*. Corporate, Baltimore: John Hopkins Applied Physics Laboratory.
- Diligent. 2017. "Cybersecurity, Corporate Governance and Your Board of Directors." *Diligent*. May 4. Accessed January 08, 2019. <https://diligent.com/blog/cybersecurity-corporate-governance-board-directors>.
- Edleman, Eric, and Gary Roughead. 2018. *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy*. Assessment, Washington DC: United States Institute of Peace.
- Forbes. 2017. "The Ascent of the CIO." *Forbes Insights*. Accessed January 06, 2019. http://info.forbes.com/rs/790-SNV-353/images/VMWare_AscentCIO_Report_FINAL-WEB.pdf.
- Geurts, James F. 2018. "Implementation of Enhanced Security Controls on Select Defense Industrial Base Partner Networks." *Cybersecurity Policy Memorandum*. Washington DC: Pentagon, October 1.
- Governance Insights Center. 2018. "How Your Board can Better Oversee Cyber Risk." *PwC*. November. Accessed January 23, 2019. <https://www.pwc.com/us/en/services/governance-insights-center/library/risk-oversight-series/overseeing-cyber-risk.html>.
- HarperCollins Publishers Limited . 2019. *Collins English Dictionary*. January 25. Accessed January 25, 2019. <https://www.collinsdictionary.com/us/dictionary/english/process>.
2016. "IT Security Spending Trends." *Sans*. Accessed January 19, 2019. <https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697>, SANS.
- Kinney, Jeff. 2018. "DoD Rule Defines When LPTA May be Used." *Washington Exec*. January 15. Accessed December 6, 2018. <https://washingtonexec.com/2019/01/dod-rule-defines-when-lpta-may-be-used/>.
- Kornbacher, Devika, and Sarah Fortt. 2018. "Cyber-Governance: Legal Considerations for Cyber Disclosure and Preparedness." *Vinson&Elkins*. November 1. Accessed January 31, 2019. <https://www.velaw.com/Insights/Cyber-Governance--Legal-Considerations-for-Cyber-Disclosure-and-Preparedness/>.
- Levinsky, Peter. n.d. *Growththink*. Accessed February 6, 2019. <https://www.growththink.com/content/two-most-important-quotes-business>.
- Lim, Paul J. 2017. "Equifax's Massive Data Breach Has Cost the Company \$4Billion So Far." *Time*. September 12. Accessed January 19, 2019.

- <http://time.com/money/4936732/equifax-massive-data-breach-has-cost-the-company-4-billion-so-far/>.
- Lynch, Justin. 2018. "The Fifth Domain." *A New DoD Task Force Addresses the Growing Threats to Critical Technology*. November 2. Accessed November 26, 2018. <https://www.fifthdomain.com/dod/2018/11/02/a-new-dod-task-force-addresses-the-growing-threats-to-critical-technology/>.
- Mandiant. 2013. "APT 1: Exposing One of China's Cyber Espionage Units." *Mandiant*. February 11. Accessed 11 20, 2018. <https://www.fireeye.com/content/dam/fireeye-www/.../mandiant-apt1-report.pdf>.
- Mandiant. 2018. *M-Trends 2018*. Special, Milpitas: Fire Eye Inc.
- Markus, David. 2016. "Complacency over cybercrime cost \$3 trillion in 2015." *Smart Company*. January 2016. Accessed December 18, 2018. <https://www.smartcompany.com.au/technology/complacency-over-cybercrime-cost-3-trillion-in-2015/>.
- McLeary, Paul. 2018. "Pentagon Pushes Counterintel For Industry As China Hacks Away." *Breaking Defense*. June 21. Accessed November 26, 2018. <https://breakingdefense.com/2018/06/pentagon-pushes-counterintel-for-industry-as-china-hacks-away/>.
- Morgan, Steve. 2017. "2018 Cybersecurity Market Report." *Cybersecurity Ventures*. May 31. Accessed January 8, 2019. <https://cybersecurityventures.com/cybersecurity-market-report/>.
- National Institute of Standards and Technology. 2015. *Cyber Supply Chain Risk Management*. Accessed November 11, 2018. <https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management>.
- . 2019. *NIST Cybersecurity Framework General Resources*. December 10. Accessed January 23, 2019. <https://www.nist.gov/cyberframework/general-resources>.
- . 2013. *NIST Interagency Report 7298, Revision 2, Glossary of Key Information Security Terms*. May. Accessed November 17, 2018. <https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>.
- . 2015. *NIST SP 800-161: Supply Chain Risk management Practices for Federal Information Systems and Organizations*. April. Accessed November 11, 2018. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf>.

- National Institute of Standards and Technology. 2015. *NIST Special Publication 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. Gaithersburg: National Institute of Standards and Technology.
- National Institute of Standards and Technology. 2015. *NIST Special Publication 800-53*. Gaithersburg: National Institute of Standards and Technology.
- National Security Agency. 2018. *NSA's Top Ten Cybersecurity Mitigation Strategies*. Government, Fort Meade: March.
- Navy Live. 2018. "Enhancing Cyber Protection While Increasing Resiliency." *Navy Live*. 15 October. Accessed January 27, 2019. <http://navylive.dodlive.mil/2018/10/15/enhancing-cyber-protection-while-increasing-resiliency/>.
- Office of Management of the US Government. 2018. *An American Budget*. Fiscal, Washington DC: Office of Management and Budget.
- Office of the President of the United States. 2017. "Executive Order 13806: Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States." *Presidential Documents*. Washington DC: The White House, July 21.
- . 2018. "Executive Order Enhancing the Effectiveness of Agency Chief Information Officers." *Executive Orders*. May 15. Accessed January 7, 2019. <https://www.whitehouse.gov/presidential-actions/executive-order-enhancing-effectiveness-agency-chief-information-officers/>.
- . 2017. *National Security Strategy of the United States of America*. Washington D.C: The White House.
- Office of the Secretary of Defense. 2018. *Cybersecurity Reference and Resource Guide*. Washington DC: Office of Republication and Security Review.
- . 2017. *Defense Industrial Base (DIB) Cybersecurity (CS) Activities, Incorporating Change 1*. July 27. Accessed December 5, 2018. <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520513p.pdf>.
- . 2016. *DoD Cybersecurity Discipline Implementation Plan*. February. Accessed November 22, 2018. <http://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf>.
- Office of the Secretary of Defense. 2018. *National Cyber Strategy*. Strategy, Washington DC: Office of the Secretary of Defense.

- Office of the Secretary of Defense. 2014. *Risk Management Framework (RMF) for DoD Information Technology (IT)*. DoD Instruction, Washington DC: Office of the Secretary of Defense.
- Palo Alto Networks. 2018. *Cyberpedia*. Accessed February 6, 2019. <https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture>.
- Partnership for Public Service. 2015. "Cyber In-Service Security II: Closing the Federal Talent Gap." *CA*. Accessed February 27, 2019. http://ourpublicservice.org/wp-content/uploads/2018/09/Cyber_In-Security_II_.
- Pomerleau, Mark. 2018. *In Speech, Mattis Explains His Cyber Concerns*. January 19. Accessed February 17, 2019. <https://www.fifthdomain.com/dod/2018/01/19/mattis-dod-reorganizing-in-cyber/>.
- Price Waterhouse Cooper. 2018. *How Your Board can Better Oversee Cyber Risk*. Corporate, Price Waterhouse Cooper.
- Rose Jackson. 2017. "Untangling the Web: A Blueprint for Reforming American Security Sector Assistance." *Open Society Foundations*. January. Accessed January 08, 2018. <https://www.opensocietyfoundations.org/sites/default/files/untangling-the-web-20170109.pdf>.
- Seffers, George I. 2019. "Kinetic Weapons Remain a Priority as Cyber War Rages." *SIGNAL AFCEA*. February 15. Accessed February 21, 2019. <https://www.afcea.org/content/kinetic-weapons-remain-priority-cyber-war-rages>.
- Sinsel, Adam, LCDR. 2018. "DoD Needs a Joint Cyber Red Team." *U.S. Naval Institute*. December 1. Accessed December 6, 2018. <https://www.usni.org/magazines/proceedings/2018-12/dod-needs-joint-cyber-red-team>.
- Spencer, Richard V. 2018. *Cybersecurity Review*. Memorandum, Washington DC: Secretary of the Navy.
- Steinkopf, Tim. 2018. "Six Cyber Predictions for 2019." *SC Media*. December 12. Accessed January 29, 2019. <https://www.scmagazine.com/home/opinions/six-cybersecurity-predictions-for-2019/>.
- The Business Dictionary. 2019. *The Business Dictionary*. Accessed January 5, 2019. <http://www.businessdictionary.com/definition/culture.html>.
- The Cornell Institute of Public Affairs. 2017. *Attracting and Retaining Talent in the Field of Cybersecurity*. Accessed February 27, 2019. <https://ecommons.cornell.edu/bitstream/handle/1813/52178/CIPA%20Capstone%20Sp%202017%20Gov%27t%20Acct.%20Office%20Cybersecurity%20Report.pdf?sequence=2>.

The National Bureau of Asian Research. 2017. "IP Commission Report." *The IP Commission*. February 1. Accessed January 10, 2019. <http://www.ipcommission.org/>.

The NDIA Cybersecurity for Advanced Manufacturing Joint Working Group. 2017. *Cybersecurity for Manufacturing Networks*. White Paper, Rosslyn: National Defense Industrial Association.

Under Secretary Of the Navy. 2018. "Memorandum: Restructure of Secretariat Functions." Washington DC : Department of Navy, March 16.

US Government Accountability Office. 2018. *GAO-19-128: Weapon Systems Cybersecurity: DoD Just Beginning to Grapple with Scale of Vulnerabilities*. Assessment, Washington DC: GAO.

US Government Accountability Office. 2018. *GAO-19-54: DoD Should Clarify Criteria for using Lowest Price Technically Acceptable Process*. Assessment, Washington DC: GAO.

US Government Accounting Office. 2017. *Agencies Need to Improve Certification of Incremental Development*. Information Technology Reform, Washington DC: US Government Accounting Office.

US Government Accounting Office. 2018. *Implementation of Recommendations Is Needed to Strengthen Acquisitions, Operations, and Cybersecurity*. Information Technology Report, Washington DC: December.

US Joint Staff. 2018. "DoD Dictionary of Military and Associated Terms." Washington DC: Pentagon, November.

US Joint Staff. 2018. *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*. Washington DC: Joint Staff.

US Joint Staff. 2018. *Joint Publication 3-12 Cyberspace Operations*. Washington DC: Pentagon.

US Navy. 2018. "OPNAVINST 5239.1D." *U.S. Navy Cybersecurity Program*. Washington DC: Pentagon, July 18.

US Navy. 2018. *OPNAVINST 5239.4*. Navy Instruction, Washington DC: Pentagon.

US Navy. 2016. *SECNAVINST*. Navy Instruction, Washington DC: Pentagon.

Verizon. 2018. "Data Breach Investigations Report." *Verizon*. Accessed January 22, 2019. <https://enterprise.verizon.com/resources/reports/dbir/>.

Windrem, Robert. 2016. "Timeline: Ten Years of Russian Cyber Attacks on Other Nations." *NBC News*. December 18. Accessed November 24, 2018.

<https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111>.