DSB Task Force Report on

Cyber Defense Management

September 2016

(U) This page intentionally blank

REPORT OF THE DEFENSE SCIENCE BOARD

STUDY ON

Cyber Defense Management

September 2016

(U) Office of the Under Secretary of Defense
for Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140

(U) This report is a product of the Defense Science Board (DSB).

(U) The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense (DoD). The Defense Science Board Study on Cyber Defense completed its information-gathering in November 2015. The report was cleared for open publication by the DoD Office of Security Review on December 12, 2016.

(U) This report is unclassified and cleared for public release.

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301–3140

DEFENSE SCIENCE BOARD

September 7, 2016

MEMORANDUM FOR THE UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY & LOGISTICS

SUBJECT: Final Report of the Defense Science Board (DSB) Task Force on Cyber Defense Management

I am pleased to forward the final report of the DSB Task Force on Cyber Defense. This report offers important recommendations on how the Department of Defense can ensure that it is investing properly to provide cyber resilience to its systems.

The study investigated ways to inform future investment priorities, including methods to assess and provide DoD leadership with improved management insight into the level of cyber protection that both currently exists and is planned within DoD networks, sensor, weapon and support systems. The study provides approaches to assess system resilience, or surrogates informing system resilience, to different kinds and levels of cyber-attack. The study also discusses methods to understand relationships between DoD cyber investments and the resulting increased resilience to attack.

Finally, the study details a set of recommendations for the "next dollar spent" to maximize effects against cyber threats. These new areas of investment include collecting and analyzing attack data, increasing automated functions for cyber defense, and including cyber preparedness in force readiness reporting.

I fully endorse all of the recommendations contained in this report and urge their careful consideration and soonest adoption.

Dr. Craig Fields
Chairman

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301–3140

DEFENSE SCIENCE BOARD

August 31, 2016

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Final Report of the Defense Science Board Task Force on Cyber Defense Management

The final report of the Defense Science Board Task Force on Cyber Defense is attached. In accordance with its charter, the study investigated ways to inform future DoD investment priorities. Methods are discussed for providing DoD leadership with improved management insight into the current and future levels of cyber protection that exist within DoD and its networks, sensor, weapon and support systems. The study also developed approaches for assessing system resilience to different kinds and levels of cyber attack. The report also provides insight into methods for DoD to understand the relationships between its cyber investments and the amount of increased cyber reliance it experiences. Finally, recommendations are provided for prioritizing investments and where the "next dollar spent" by DoD can provide maximum effects against cyber threats.

The highly publicized commercial and governmental cyber breaches have driven a dramatic increase in general awareness and concern for cyber threats, system vulnerabilities, and the potential for damage from losing personal information stored within a system. This awareness has resulted in increased demand for more secure products and services. Within DoD, the standup of the United States Cyber Command (USCYBERCOM) has given focus to DoD's efforts to improve cyber security. Though these signs are encouraging, and billions of dollars per year have been spent on cyber security, the Task Force believes most DoD systems are still not adequately protected against cyber threats. The increased awareness and understanding of the issue offers a window of opportunity to make major strides over the next several years to improve the cyber security posture of DoD.

A major finding of the study is that successful organizations collect and analyze attack data. It is important for DoD to track their cyber hygiene efforts and also perform consistent analysis on their system's performance against cyber attacks. These metrics should be shared with the DoD leadership to help build awareness from the top-down. Engaging senior leadership in understanding DoD's cyber performance will accelerate short-term performance and long-term improvements. Also, engaging the senior leadership will provide them with a better understanding of whether cyber investments are impacting cyber performance.

The task force found that DoD still manually collects the majority of their compliance metrics. Manual collection of compliance metrics can cause significant cyber vulnerabilities in addition to inefficient operations Automating many cyber hygiene and cyber security functions can provide reliable, timely, and comprehensive reporting on important cyber security metrics. Modern, well run IT enterprises employ highly automated cyber management processes to both keep the security features updated as quickly as possible and to drive down the expense of running the system. Automating these processes also allow the IT workforce to focus on the most sophisticated cyber attacks.

In support of automating network operations, once DoD has ensured that its network-based IT infrastructure's protection is automated, then it should allow its IT workforce to focus on protecting the mission critical systems. These systems include weapons, sensors, and command, control, communications, computer, intelligence, surveillance and reconnaissance (C4ISR) assets. In time of conflict, a cyber capable adversary will focus their efforts on disrupting DoD's front line mission systems. Including cyber readiness as a factor in the Defense Readiness Reporting System (DRRS) is an excellent method for initiating a focus on protecting mission critical systems as well as tracking DoD's efforts in cyber hygiene and automating network operations.

The report also provides insight into models to assist in determining the DoD systems and networks most at risk from cyber-attack and those that are relatively secure. The study's charter also asked for a model to help inform future DoD investments. A full model capable of achieving these two objectives is a very complex undertaking and requires substantiating data, which will be generated through the actions described in this report. While achieving both these objectives in full today is not possible, the report details current models that provide a short-term solution for modeling the cost effectiveness of a particular system in protecting against cyber attacks. These solutions can be pursued until a more capable model is developed.

Finally, the report discusses the role DoD has in influencing the commercial marketplace in terms of cyber security and cyber hygiene. An understandable reliance on commercial technologies by DoD has meant that its systems have the inherent vulnerabilities that the commercial market place has been willing to tolerate. DoD can help to reinforce the marketplace changes that are already occurring due to increased awareness of cyber security.

The study believes that all of the recommendations contained in this report are critical for ensuring the Department maintains its advantages in the cyber domain into the future.

Mr. Robert Nesbit
Study Co-Chair

Mr. Lou Von Thaer
Study Co-Chair

Table of Contents

List of Figures

List of Tables

Executive Summary

In October 2014, the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) requested that the Defense Science Board (DSB) investigate ways to improve the Department of Defense's overall management processes for providing cyber security in its systems and networks. The Board assembled a Task Force composed of national leaders in information technology (IT) and cyber security. The Task Force met from January 2015 through November 2015 to deliberate on cyber security for the Department of Defense (DoD).

The task force was asked to take on four specific tasks:

- Determine methods to assess and provide DoD leadership with improved management insight into the level of cyber protection that either currently exists or is planned
- Devise the means or methods to assess system resilience to different kinds and levels of cyber attack
- Investigate ways to inform future investments for DoD cyber defense
- Develop approaches to produce prioritized recommendations for spending the next dollar for maximum effect against cyber threats

The most recent DSB study related to cyber security was in 2013, more than three years ago.[1] Since these recommendations were published, many serious cyber attacks and breaches have resulted in information and financial losses as well as information system down time. However, there have been some encouraging signs as well.

The highly publicized government and commercial cyber breaches have driven a dramatic increase in general awareness and concern for cyber threats, system vulnerabilities, and the potential for damage from losing personal information stored within a system. This awareness has resulted in increased demand for more secure products and services. Recently, cyber security insurance rates have experienced an increase averaging more than 30 percent from the previous year.[2] This may reduce "papering over" the security problem.

Within DoD, the standup of United States Cyber Command (USCYBERCOM) has given focus to DoD's efforts to improve cyber security. Effective red teams have led to "Cyber Awakening" activities across the services, especially the Navy.[3] The Defense Advanced Research Projects Agency (DARPA) Cyber Grand Challenge has created a number of innovative approaches for automating cyber defenses.

These signs are encouraging, and in the United States billions of dollars per year have been spent on cyber security for government and commercial systems. Nevertheless, the Task Force believes most DoD systems are still not adequately protected against cyber threats. The increased awareness and understanding of the issue offers a window of opportunity to make major strides in the near term to improve the cyber security posture of DoD.

---

[1] Defense Science Board, *Task Force Report on Resilient Military Systems and the Advanced Cyber Threat*, January 2013.

[2] Cyber Insurance Premiums Rocket after High-Profile Attacks, Reuters.com, October 12, 2015, accessed at http://www.reuters.com/article/us-cybersecurity-insurance-insight-idUSKCN0S609M20151012

[3] The Navy launched their Task Force Cyber Awakening in 2014.

Over the past decade cyber security defense strategies and techniques have matured substantially. The following three areas were identified by the task force for immediate action to address DoD cyber defense.

Cyber Hygiene

Over the past decade cyber security defense strategies and techniques have matured substantially. The first manifestation of that is that cyber hygiene has become standard commercial practice and is defined as:

> *Cyber hygiene involves organizing IT infrastructure, hardware and devices to facilitate continuous monitoring and report; removal of unauthorized software and hardware; effective patching of authorized software; formalizing informal information security controls; and heightened training and awareness of both security administrators and users.*[4]

Any organization practicing sound cyber hygiene today will have defined a crisp set of quantified metrics that best capture the attributes that describe their system's defense. For example, these metrics may include measures of elapsed time between vendor release and the application of a security patch; strength of passwords; and the time between introduction of a rogue hardware device on the network and its detection. Because each system security defense team tailors its own list of metrics, multiple metric collections have been defined by respected organizations. The specific metrics are not important: instead, it is critical that each organization develop metrics that characterize the state of cyber security for their entire software and hardware system, and then use those metrics to track the state of their cyber hygiene. These metrics should be scrupulously collected and reported. In order for these metrics to be timely, data collection will, for the most part, need to be automated.

There is ample evidence that an organization that practices effective cyber hygiene will deflect the vast majority of attacks, measured in *number* of attacks. The most dramatic examples have been recorded in work by the Australian Signals Directorate[5] and the U.S. Department of State[6]. One result of deflecting most of the attacks is that cybersecurity administration personnel are more available to devote their efforts to the more serious attacks, and able to better protect the most important data and system operations.

Visibility

The second major advance is that system administrators have visibility into their system and know (and can report) where in the system an attack might be detected and mitigated. They have the insight to make sound judgments about what security application code is effectively protecting their specific system. This is now done by the best cyber security administrators monitoring their systems

---

[4] The Center for Internet Security, *The CIS Critical Security Controls for Effective Cyber Defense, version 6.0,* October 2015, p.79

[5] Australian Signals Directors, *Strategies to Mitigate Targeted Cyber Intrusions*, April 2013, accessed at http://www.asd.gov.au/infosec/mitigationstrategies.htm

[6] SANS Institute, *Reducing Federal Systems Risk with the SANS 20 Critical Controls*, page 8, April 2012, accessed at https://www.sans.org/reading-room/whitepapers/analyst/reducing-federal-systems-risk-20-critical-controls-35235

so that they can track an individual attack as it enters and advances through their system. The administrators understand which cyber software defense applications should be able to detect, deflect, destroy, or mitigate an individual attack. Even the best system defenders cannot protect against all attacks.

Cyber Security

A multitude of different issues can be grouped under the cyber security banner. While many of them are addressed in this report, some are not, including: personal systems that DoD employees use in DoD facilities (e.g., cell phones and tablets); Internet of Things (e.g. light bulbs, batteries, thermostats); and supply chain security.

This report presents the key findings and recommendations of the Task Force deliberations. The Task Force's findings and recommendations can be grouped into the seven areas summarized below.

Collect and Analyze Attack Data

For many years, cyber security has been a compliance driven process. Organizations define rules or best practices and direct their IT systems to comply. For example, patch all application software within three days of patch availability or train all employees twice per year. Success is measured by how well the stated rules are followed. A number of organizations that the Task Force interviewed have moved beyond this simplistic approach to a more dynamic performance assessment of their network operations. These organizations perform consistent and careful analyses of their defensive systems' performance against actual attacks. Collecting and collating this data over time gave the organizations a statistically significant basis to use in evaluating the performance of their individual defensive subsystems. The data allows these organizations to determine which defensive subsystems are performing well against specific threats and which systems are underperforming. By evaluating this data and considering costs of acquisition and operation, a rough value assessment can be made. The companies can also see where their combined defensive coverage is strong, where their system has gaps, and where there may be multiple security subsystems doing the same function.

The Task Force did not see any evidence that DoD was doing this type of assessment anywhere on a consistent basis. These assessments provide data that can be used to support and inform investment priorities and can serve as a basis for deriving recommendations for investing the next dollar spent on the network defense portion of the overall cyber security problem.

Recommendation 1

The DoD Chief Information Officer (CIO), in conjunction with the Service and Agency CIOs, should investigate how to best use the attack data they experience on their various networks to evaluate the performance of their defenses.

The DoD Chief Information Officer (CIO), in conjunction with the Service and Agency CIOs, should begin collecting data on each attack against their networks, and data on how each defensive element performed in response to that attack. Several months of data collection should yield a statistically

significant sample. The DoD CIO, as well as the Service and Agency CIOs, should then adopt one of the example processes the Task Force reviewed, or devise their own analytic process. It is not important whether the same approach that Lockheed Martin, Goldman Sachs, or the Australian Signals Directorate is used, or if the Department invents their own process. But "leaving all this data on the table" is not the best way to proceed. Cyber security has long been a compliance dominated process, focused on doing specific actions on a checklist. Examining the attack data to determine what is working well, what is not, where changes need to be made, and where investment is required to better defend against troublesome or emerging threats would move the Department beyond a compliance approach towards a more dynamic performance evaluation. This will contribute strongly toward answering the four questions highlighted in this study's TOR.

Inform and Engage Executives

One important aspect for driving improvements to cyber defense is increasing engagement by executives in their organization's cyber security. Regularly informing and actively engaging DoD leadership in DoD's cyber security status and plans will help accelerate both short-term performance and long-term improvements.

The DoD has recently made a good start towards this by generating a monthly status report on IT network security by Service and Agency. This report covers compliance with basic network hygiene measures, such as proper patching, two factor authentication, removal of XP machines, use of Host Based Security System (HBSS), and use of the standard security configuration. All these improvements have positive, demonstrable, and measurable impacts on cyber defense. To date, most of the data in the report is manually collected and self-reported causing parts to be incomplete or inaccurate. Overall, the report is generating improved insight and visibility on the topic and has resulted in improved compliance metrics.

In addition to tracking the progress of compliance measures, comprehensive cyber security improvement requires a much better decision making framework for executives. In our survey of commercial and defense companies we found some best practices regarding how they engage their executives and boards which lead to our recommendations in this area.

Recommendation 2

Based on industry best practices, the Task Force recommends the DoD CIO, in conjunction with the Service and Agency CIOs, expand their monthly cyber security status report.

The expanded report should include the following topics:

1. **Threat background and trends** – a summary of key attacks experienced in DoD networks and systems in the reporting month including source of origin, means of access, and attack intentions. Also, how these attacks compared to previous months noting any changes or trends. In addition, include similar threat information beyond DoD as compiled by security research firms. Finally include data on emerging threats and attack techniques that may be seen in the near future.

2. **Defensive system performance –** assess how well each individual deployed defensive system performed in terms of detecting an attack, stopping the progress and eliminating the threats experienced that month. Which software components are not performing as expected? Where are there overlaps in defensive coverage? Where are there gaps? How does the cost of acquiring and operating the defensive system compare to its performance?
3. **Security controls** – report on metrics for key cyber hygiene controls that DoD mandates for use by the system. In addition to measuring compliance, examine the effectiveness of the controls in detecting or eliminating threats. Compare this to other effectiveness ratings of security controls produced by outside agencies.
4. **Top five risk areas** – compile top five lists, based on expert judgment, for critical cyber security risks being faced by DoD. These lists should prioritize the risks from 1-5 and be for the following topics:
    a. Greatest cyber risks faced on a daily basis
    b. Greatest cyber risks faced during conflict with a cyber capable adversary
    c. Most sensitive data holdings
    d. Key areas requiring immediate investment
5. **Tracking –** Report on the status of the "Top Five" of previous months (e.g., investigations initiated, measures taken, progress made, metrics, …), highlighting any close-outs that have occurred.

The Task Force drafted a sample monthly report (Appendix 1), designed for executive consumption, to give an example of what we recommend be used to provide a factual basis for executive review and decision making. The sample report is largely self-explanatory and includes many of the best practices and examples collected from commercial companies and the defense industry.

Automate Network Management Operations

The manual collection of compliance metrics indicates that DoD's enterprise IT environment is outdated. Until updated, slowness and inaccuracy will cause significant cyber vulnerabilities in addition to inefficient operations. Current management of cyber security in DoD is a largely manual and very labor-intensive process. It is overly expensive to continue operations in this manner and also makes it difficult for CIOs, Chief Information Security Officers (CISOs) and network administrators to get reliable, timely, and comprehensive reporting on important cyber security metrics. If the metrics are used to feed a decision cycle (Observe, Orient, Decide and Act (OODA)), it will not succeed if the core observations are outdated, of suspect quality, or too costly to collect.

Modern, well run IT enterprises employ highly automated cyber management processes to both keep the security features updated as quickly as possible and to drive down the expense of running the system. The processes that are automated include patch management, configuration management, system discovery, system configuration audit, and security log analysis. Once implemented these systems are much less expensive to operate and provide near real time insight into the security status of the network. Based on discussions with several CIOs that met with the Task Force, the cost of

operating an automated cyber management process was between 10 and 30 percent of the manual process. Automated systems also make it easier to incorporate changes as the threat evolves.

Because DoD networks are highly segmented, developing procedures to work within the scope of control is an important issue when automating cyber management operations. The Task Force reviewed several commercial organizations that operate networks of a similar or larger size than DoD and have successfully implemented highly automated cyber security management processes. **The conclusion from those discussions is that the large scale and complexity of the DoD network is not a valid excuse for inaction in automating cyber management operations in DoD.**

Recommendation 3

The DoD CIO and CISO should architect and plan for increasingly automated cyber management operations in order to reduce the time networks are vulnerable to known attack vectors, and to increase visibility.

For the last decade DoD officials have argued that the obsolete and obscure systems running on their network do not allow modernization because functionality of those systems will be lost with modernization. However, not modernizing has continued to drive exorbitant expense and vulnerability into the enterprise. Forcing prioritization to update or discontinue those systems to allow modernization must be a high priority—even if it means delaying other investments. In conjunction with these changes, the Military Service and Defense Agency CIOs should undertake pilot programs for virtual desktop infrastructures wherever appropriate given the numerous cyber defense management benefits. This discussion should be led by the DoD CIO and CISO so that local issues do not inhibit the enterprise's need for better security.

It is critical that the disparate networks be able to communicate with a central system for global visibility and reporting in an automated way. Care should be taken to do this in a very secure manner so as not to give attackers an exploitable opening. Given the complexity of the DoD environment, the guiding principle should be to maintain visibility into the processes needed to move commands and data throughout the enterprise, rather than developing universal toolsets or technology.

The DoD CISO should architect and plan for increasingly automated cyber management operations in order to reduce the time networks are vulnerable to known attack vectors. It is critical that disparate networks are able to communicate with a central system for global reporting. The DoD CISO should issue guiding principles and specific performance and progress requirements to the Service and Agency CISOs for automating the following areas:

- patch distribution and management,
- system discovery,
- configuration management, and
- system configuration audit.

These items should be a specific part of executive decision making and performance management. This will result in considerable cost savings, after a short payback period, which the task force recommends be reinvested to improve defenses against more sophisticated cyber threats.

The automation of cyber management operations should be architected in a secure and resilient manner to avoid unduly increasing the cyber-attack surface. The automation must include the capability to roll back from a bad patch load. When complete, automating the above processes will result in considerable cost savings with a short payback period. The Task Force recommends those cost savings be reinvested to improve defenses against more sophisticated cyber threats.

USD(AT&L), in conjunction with the DoD and Service CIOs, should ensure that all program managers of future IT acquisitions enable their systems by default to be patched, configured, and audited by the chosen automation system for cyber management operations. The only exceptions to this policy should be for those systems that an up-front risk analysis determines that enabling this capability represents a greater risk. One example is when an upgrade will violate a need for system isolation.

Protect Mission Critical Systems

To date, most of DoD's focus and resources have been expended on defending the network-based IT enterprise assets that include the servers, routers, desktops, data bases, and associated operating systems and application software. Front line mission systems are not a priority for cyber security due to their isolation from other DoD networks, but comprise the most critical assets that DoD will need to protect. In time of conflict, a cyber capable adversary could focus their efforts on disrupting DoD's front line mission systems—weapons, sensors, and command, control, communications, computer, intelligence, surveillance and reconnaissance (C4ISR) assets.

Defending all DoD systems equally against the most advanced cyber threats is both unaffordable and unnecessary. Only the most critical assets should be prepared to engage the most sophisticated peer level cyber threats and have defenses above and beyond the automated cyber management operations discussed above.

Recommendation 4

A DoD-wide Executive Oversight Team (EOT) should be created to organize and manage the selection and hardening process to ensure that the most mission critical systems are protected to the highest practical level.

The Department leadership should ensure that the capabilities necessary to accomplish the most critical missions are sufficiently resilient and robust in the face of a determined and sophisticated cyber-attack. The most critical missions may include: conventional force elements with deterrent value; missile defense; essential space operations; nuclear and other essential command and control; and some systems that ensure continuity of government functions.

The team should be chaired by the Deputy Secretary of Defense (DEPSECDEF) and include the Chief of the Joint Chiefs of Staff (CJCS), USD(AT&L), USD(P), DoD CIO, and the Assistant Service Secretaries for acquisition. A small support staff will likely be required to assist the EOT with its responsibilities.

The Task Force recommends that for each of the mission critical systems, the following actions be taken:

- Explain the rationale for selecting this particular mission as "critical," including the current potential and consequence of loss through successful cyber attack
- Conduct a mission-based analysis, then a defensive analysis on critical systems and components
- Develop an understanding of system connectivity and vulnerabilities
- Reverse engineer the critical systems to understand vulnerabilities at the functional level that an adversary would likely attack (including the maintenance and sustainment trails)
- Develop the capability to isolate and segment systems as much as possible
- Forward cache necessary data at appropriate time intervals to further system isolation
- Identify system and supply chain vulnerabilities
- Develop workarounds or back-ups for remaining vulnerabilities
- Evaluate effectiveness through Combatant Commands (CCMDs) with measurement feedback to the leadership
- Establish metrics for this assessment in the CIO offices

Because of the significant expense and difficulty, it is necessary to identify the fewest possible systems and dependencies to achieve mission success in each area. USD(AT&L) and the Joint Staff have already made some progress in determining the most mission critical systems.

The objective should be to have the process started immediately with implementation, completed in 2-3 years. Once implemented, DoD should evaluate the effectiveness of the resulting defense posture through the CCMDs with measurement feedback to the leadership. The DoD CIO should establish metrics for this assessment.

Include Cyber Preparedness in Defense Readiness Reporting

The Combatant Commands (CCMDs) must be prepared to successfully execute assigned missions in the face of cyber threats. The existing Defense Readiness Reporting System (DRRS) provides an excellent vehicle for assessing and reporting the CCMDs readiness with regard to cyber-attacks. It specifies the ability of military units to accomplish their mission essential tasks, from which a commander can specify the overall readiness of his organization to accomplish its assigned missions. The assessments are based on expert judgment taking into account such factors as resource availability and level of training.

These mission assurance assessments can then be used to express the degree of preparation for carrying out tasks comprising missions in the face of cyber threats.

Recommendation 5

For its assigned missions, each CCMD with support of the Services should report their cyber preparedness along with the other elements of the DRRS. Updates to these assessments should follow the normal Defense Readiness Reporting schedule.

For its assigned missions, each CCMD, with support of the Military Services, should report through the DRRS the following:

- Have assets critical for the mission been identified, *e.g.,* thru mission thread analyses?
- How many of those assets have been assessed for cyber vulnerabilities, *e.g.,* by Cyber Protection Teams and Service technical analysts?
- Is there a schedule for cyber-assessing the remaining critical assets?
- To what extent have protection means been implemented for the identified vulnerabilities, both procedural and technical?
- To what extent have contingency plans been established to compensate for the degradation or loss of the critical assets, *e.g.,* fallback and recovery procedures to meet minimum operating requirements?
- Has each exercise been used to determine the value of cyber defense as it pertains to the mission objectives of that particular exercise?
- Have exercises been conducted to assess how well the missions can be accomplished in the face of cyber threats, involving realistic threats, red team play and quantitative assessment of mission execution?

Some activity is ongoing pertaining to most of the items in this recommendation, so it should be possible to quickly initiate implementation of the recommendation. Standards defining how the mission assurance measures are to be reported should first be established so there is common understanding by all parties involved. That definition should not take long (nor should it be allowed to get hung up in bureaucratic process that will take a long time); the Task Force estimates six months should be adequate. The periodic reporting should occur every six months. This frequency is not so frequent that it overburdens those conducting the assessments. Highest priority in the reporting and the associated cyber preparedness improvements should be given to those missions deemed most critical.

Build on Current Modeling Efforts to Inform Investment

The Task Force's Terms of Reference requests a model to assist in determining the DoD systems and networks most at risk from cyber-attack and those that are relatively secure. In addition, the model should assess whether current investments are addressing the most urgent risks, and where to invest "the next cyber defense dollar." It is important to note that a full model capable of achieving these objectives is a very complex undertaking and requires substantiating data, which is generated through the actions described above and elsewhere in this report.

Commercial companies and other government agencies face similar needs. The Task Force's review determined that while a number of companies are becoming more experienced in experimenting with cyber risk models to influence investments, no one with whom the Task Force met has a comprehensive, mature model that they use today to drive cyber investments. Several companies and organizations have developed models to visually show where and how attacks are blocked (or not) relative to the organization's investments made in cyber tools and procedures. The tools reviewed were focused on enterprise networks but could be adapted to include weapons systems. More analytical models are also under development that address portions of the cyber security problem. RAND is playing a lead role in developing these models. Some promising research in the

Office of the Deputy Assistant Secretary of Defense for Command, Control, and Communication (C3), Cyber, and Business Systems (C3CB) (ODASD(C3CB)) is addressing the development of a model.

In response to the challenge for a model to assist in spending the next dollar on cyber, the Task Force broke the issue down into two areas. The first encompasses network defense (Non-Secure Internet Protocol Router Network (NIPRnet), Secret Internet Protocol Router Network (SIPRnet), Joint Worldwide Intelligence Communications System (JWICS), and other communication systems) and the second focused on the defense of systems with embedded cyber (e.g., F-22 and Aegis). The Task Force found examples and models to display and analyze system performance in the network defense area that can certainly drive intelligent investment decisions. Examples contained in this report from Lockheed Martin, Goldman Sachs, and the Australian Signals Directorate (charts attached in Appendix 1), provide a basis for measuring the performance of the various cyber defensive elements against actual attacks and thereby point out where future investments may be warranted. These examples show that a sufficient number of actual attacks are available for a statistically significant analysis of the performance of a network's current defensive systems. This analysis can determine which defensive systems have value in terms of their operating cost versus performance; which systems do not have value; where the organization's defensive coverage is thin; where the system may have excess redundancy; and which security controls are the most effective given a year's worth of attack data. Taken together, the analytic areas listed above provide a broad overview of the cost-effectiveness of a particular system after the analysis.

Recommendation 6

DoD should expand the resources available to the ODASD(C3CB), in conjunction with the Modeling and Simulation Coordination Office (M&SCO) under the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)), to continue and expand the cyber investment modeling work to include financial, heuristic, and effects based assessment models. ODASD(C3CB) and M&SCO should lead an Executive Steering Committee to serve as the coordination body for DoD throughout a multi-phased approach to developing a single model to inform DoD cyber investments, with a particular focus on warfighting systems.

The Executive Steering Committee should develop and mature cyber investment modeling capabilities over the next two years, to include:

- Financial Model with a goal to record, examine, and improve how cyber investment dollars are used within DoD
- Heuristic Model with a goal to identify and understand the key factors affecting cyber investment decisions in terms of the inter-relatedness of organizations, systems, and the tools and products used
- Effects Based Model with a goal to analyze cyber investments and their resulting impact on a system's cyber defense posture, cyber resilience, and mission effectiveness relative to cost

During this development, the Executive Steering Committee should explore how it can make use of existing partial models that have been developed by RAND, Lockheed Martin, Goldman Sachs, and the Australian Signals Directorate.

A multi-phase approach is recommended to leverage the above models in order to create a single model to enable DoD decision makers to choose the most appropriate and cost-effective cyber defense investments. The use of models and simulations has become a key tool for improving and refining the methods and techniques used on a broad variety of DoD missions. Applying modeling and simulation to the cyber risk investment decision process would closely approximate the methods and techniques used by insurance firms when choosing whether to issue coverage or not. While cyber risk investment and assessment modeling is a developing field of expertise with similar complexities found in the data sciences domain, it provides a very pragmatic and scientific method for solving the cyber investment decision problem. More importantly, it provides an opportunity for experimentation and exploration of alternatives while not requiring the actual investment in resources and materials required by traditional try and buy approaches.

Work with COTS Suppliers That Place High Value on the Security of Their Products

Most cyber defense measures—in place and proposed—focus on reacting to discovered vulnerabilities and thwarting would-be attackers. The very best cyber defense measures are those that prevent the acquisition and fielding of highly vulnerable capabilities in the first place. An understandable reliance on commercial-off-the-shelf (COTS) means that DoD systems have the inherent vulnerabilities that the commercial market place has been willing to tolerate. The Task Force observed that the marketplace is changing and DoD can reinforce these changes, to its advantage.

Recommendation 7

USD(AT&L), in coordination with the DoD CIO and CISO, should help shape the commercial marketplace to deliver better cyber security by becoming a more demanding buyer.

For competitive purposes, commercial vendors tend to bundle capabilities into set products. This makes it difficult to buy only the minimum essential capabilities needed by the DoD program. The DoD CIO and CISO, on behalf of DoD, should open a dialogue with vendors as to how buyers can disable unnecessary capabilities. This should also be coordinated with other government agencies to develop a government-wide effort to shape the marketplace.

Actions for becoming a more demanding buyer include:

- USD(AT&L) should favor vendors with strong software development practices and track record of conscientiously fixing vulnerabilities
- The DoD CIO and CISO should specify the use of open standards for security automation
- The DoD CIO in conjunction with the Joint Requirements Oversight Council (JROC) should require that newly acquired software run on a standard secure configuration
- The DoD CISO should work with vendors to build marketplace awareness and demand for cyber-resilient hardware and software

- The DoD CIO should coordinate with CIOs from other government agencies, in particular DHS, to make such conditions part of their future purchases and developments.

Exposing vulnerabilities in complex systems and acknowledging the capabilities that engender those vulnerabilities requires a level of skill that is not currently resident in DoD. The DoD CIO and CISO, in coordination with USD(AT&L), should take immediate steps to develop these skills and augment current staffing in order to support making DoD a more demanding buyer. This can be done through personnel exchanges with NSA and USCYBERCOM, through FFRDC exchanges, and involvement with other outside entities. Clear incentives will be needed to attract real experts in this area. Resources should be provided, as required, to assist in this skill development.

For both traditional programs of record and COTS programs, the onus in on the requirements process to ensure there is adequate cyber security. The DoD CIO and CISO have a presence in the process up to and including JROC deliberations. Their involvement in this process will support minimizing cyber vulnerabilities as a normal aspect of every Program of Record (POR). This process is easier begun with a new POR rather than immediately grafting it onto current programs. Therefore, the DoD CIO and CISO should seek to embed this process of fine-grained cyber-risk management into a target POR. The suggested candidate program is the "next generation bomber" because it is a mission critical system.

Identifying the specific, as well as types of, system capabilities that are most likely to introduce cyber vulnerabilities or otherwise increase the cyber attack surface in a system will improve the overall cyber safe acquisition process. Research should be sponsored by USD(AT&L) and the DoD CIO and CISO, both within and outside of DoD, to better understand the inter-relationships between system capabilities and their vulnerabilities. This research will support DoD's efforts in becoming a more demanding buyer.

Chapter 1: Collect and Analyze Attack Data to Measure Defensive System Performance

For many years, cyber security has been a compliance driven process. Organizations define rules or best practices and direct their IT systems to comply. For example, patch all application software within three days of patch availability or train all employees twice per year. Success is measured by how well the stated rules are followed. A number of organizations that the Task Force interviewed have moved beyond this simplistic approach to a more dynamic performance assessment of their network operations. These organizations perform consistent and careful analyses of their defensive systems' performance against actual attacks. Collecting and collating this data over time gave the organizations a statistically significant basis to use in evaluating the performance of their individual defensive subsystems. The data allows these organizations to determine which defensive subsystems are performing well against specific threats and which systems are underperforming. By evaluating this data and considering costs of acquisition and operation, a rough value assessment can be made. The companies can also see where their combined defensive coverage is strong, where their system has gaps, and where there may be multiple security subsystems doing the same function.

The Task Force did not see any evidence that DoD was doing this type of assessment anywhere on a consistent basis. These assessments provide data that can be used to support and inform investment priorities and can serve as a basis for deriving recommendations for investing the next dollar spent on the network defense portion of the overall cyber security problem.

Because almost every large organization outside DoD will have similar concerns, the Task Force reviewed many companies and other government agencies to see how they addressed these issues. The Task Force found many who indeed had similar concerns, but had found no good approaches for solving them. The Task Force found several, however, that had a process they thought was working and three examples are explained below. The interesting thing to note is that the three examples, while different approaches, all share the same general basis for measuring the performance of their defensive systems using actual attack data on their networks.

The first example is from Lockheed-Martin. The output of their monthly evaluation is summarized in Figure 1.

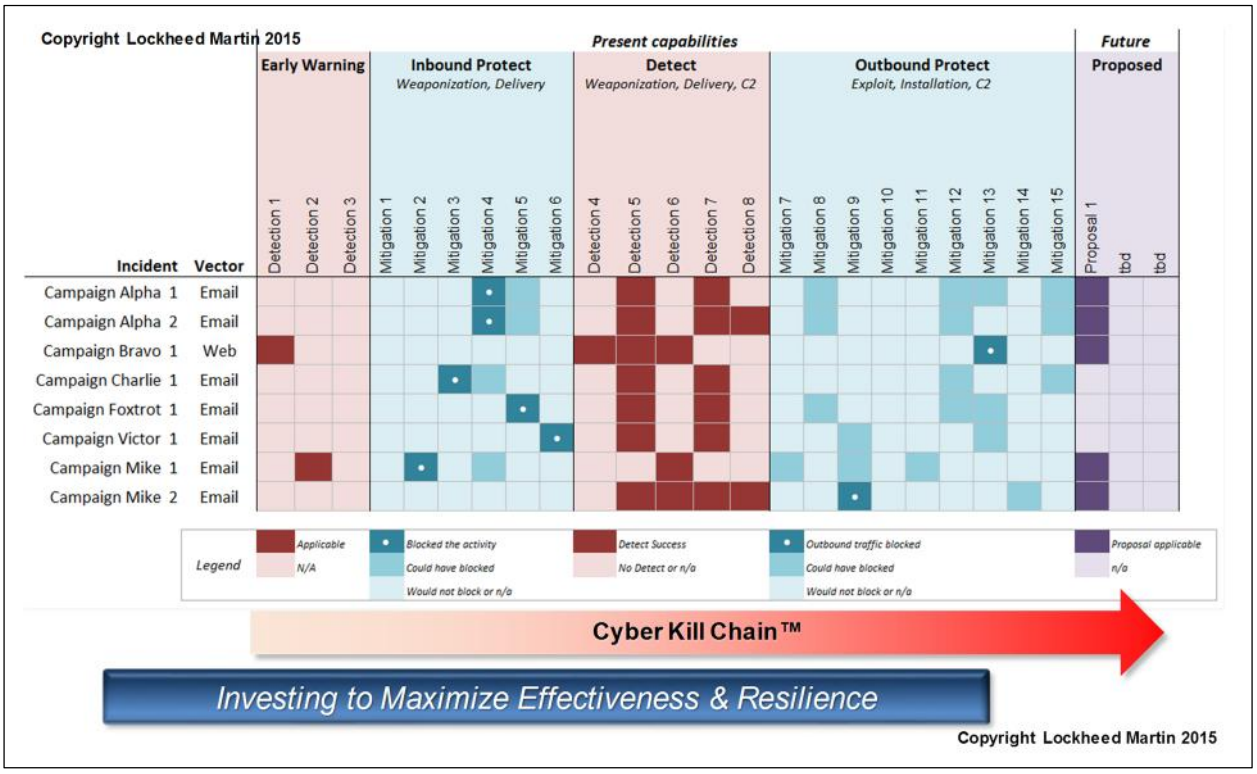


Figure 1: Lockheed Martin System performance against significant incidents monthly evaluation

On the left hand side of the chart are cover names for the most serious attacks their network faced during that particular month. Across the top are the various defensive subsystems providing network protection. They are subdivided into categories for the defensive functions: Early Warning; Inbound Protection; Activity Detection: and Outbound Protection. Proposed systems that they are thinking about adding to their defensive suite are also evaluated. Each of the exact defensive functions are anonymized here so as not to expose details of their security. But one can assume they include firewalls, intrusion detection sensors, proxy blocks, and the like.

Looking vertically down the chart under a specific defensive subsystem, it is readily apparent whether that defense was effective against the various attacks. For example, Detection Measure #3 was ineffective while Detection Measure #5 was highly effective. Examining this data over several months has helped Lockheed Martin to determine what works, what does not, what needs to be changed. This data also helps to determine whether proposed defensive elements will improve cyber security and, if not, where to invest in new approaches to defend against new cyber attacks.

A different way of looking at network performance has been successfully employed by Goldman Sachs. Their process is described in Figure 2.

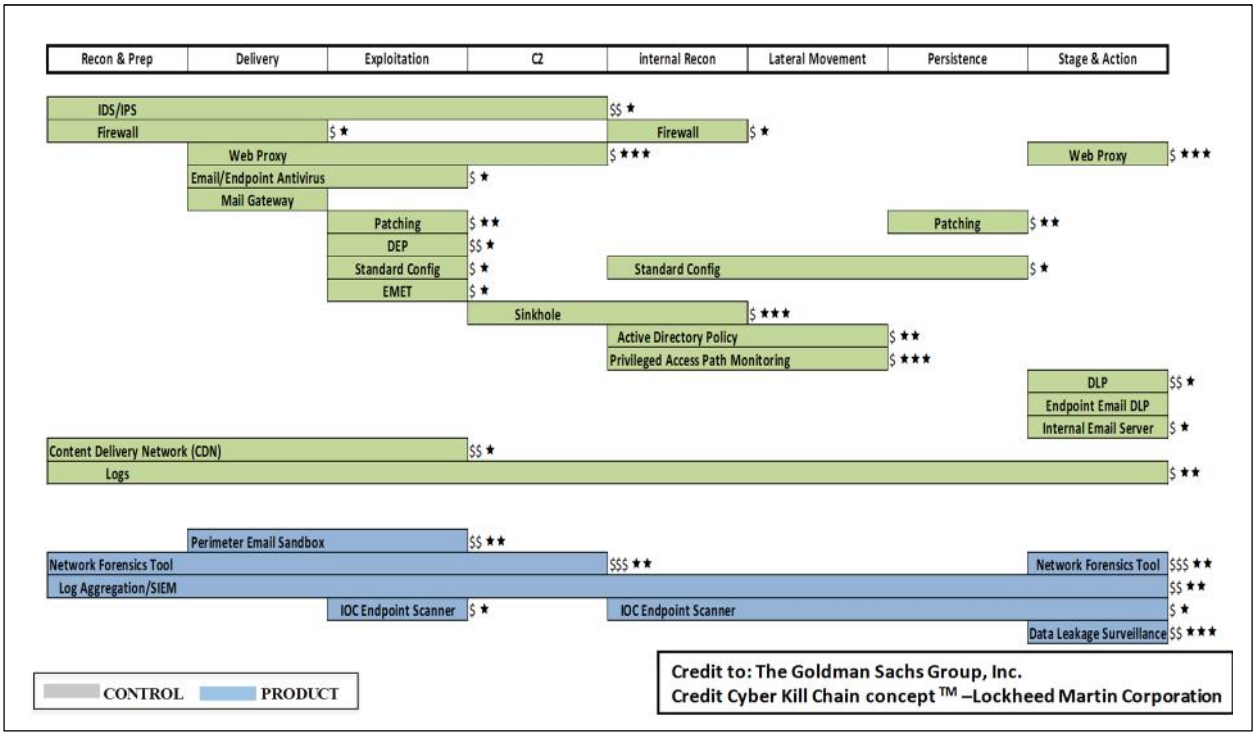


Figure 2: Goldman Sachs best practices for defensive system performance

Across the top of the chart are the various stages of the attacker's process, beginning with reconnaissance and ending with execution of the attack. All their defensive subsystems, whether they are security controls (green) or more complex defensive product suites (blue) are laid out under which stage(s) of attack they are designed to defend against. Looking vertically down under any attack stage it is possible to see where there are multiple subsystems providing coverage in depth and where there may be too little coverage. The Task Force has also added estimates of how expensive each product or control is to operate ($ to $$$) and how effective that product or control has been in defending against attacks (* to ***).

The third example included here is an analysis from the Australian Signals Directorate (ASD). The output of their study, updated on an annual basis is reproduced in Figure 3. The ASD collects data on tens of thousands of attacks each year and examines the performance of a large number of security controls in defending against those attacks. ASD then ranks the security controls in terms of their overall effectiveness against the ensemble of attacks. The analysis for 2015, which has similar results compared to 2013 and 2014, shows that the failure or absence of one of the top four controls was responsible for 85 percent of successful attacks. While this does not mean that one should only implement these four controls, it does mean that implementing these four controls should be absolutely mandatory for good cyber hygiene. The Task Force believes that this type of analysis will be important for DoD to understand their cyber investments.

Effectiveness Rank	Mitigation Strategy	Overall Effectiveness	User Resistance	Upfront Cost	Maintenance Cost
1	Whitelist permitted/trusted programs	Essential	Medium	High	Medium
2	Patch application software	Essential	Low	High	High
3	Patch operating system software	Essential	Low	Medium	Medium
4	Severely restrict administrative privileges	Essential	Medium	Medium	Low
Once organizations have effectively implemented the Top 4 mitigation strategies, firstly on workstations of users who are most likely to be targeted by cyber intrusions and then on all workstations and servers, mitigation strategies can be can then be selected to address security gaps until an acceptable level of residual risk is reached.					
5	Harden user application configurations	Excellent	Medium	Medium	Medium
6	Analyze email and web content in a sandbox	Excellent	Low	Medium	Low
7	Mitigate OS generic exploits	Excellent	Low	Medium	Low
8	Identify anomalous behavior with host based IDS	Excellent	Low	Medium	Medium
9	Disable local admin accounts	Excellent	Low	Medium	Low
10	Segment and segregate the network	Excellent	Low	High	Medium
11	Employ multi-factor user authentication	Excellent	Medium	High	Medium
12	Apply firewall to block incoming malware	Excellent	Low	Medium	Medium
13	Apply firewall to block outgoing malware	Excellent	Medium	Medium	Medium
14	Host virtual sandbox outside internal network	Excellent	High	High	Medium
15	Log successful and failed computer events	Excellent	Low	High	High
16	Log allowed and blocked network activity	Excellent	Low	High	High
17	Filter email by content	Excellent	High	High	Medium
18	Filter web traffic by content	Excellent	Medium	Medium	Medium
19	Whitelist web domains	Excellent	High	High	Medium
20	Block spoofed emails using sender ID	Excellent	Low	Low	Low
21	Configure workstation and servers under hardened SOE	Good	Medium	Medium	Low
22	Deploy anti virus software using heuristics	Good	Low	Low	Low
23	Deny direct internet access from workstations	Good	Low	Low	Low
24	Harden server application configuration	Good	Low	High	Medium
25	Enforce strong passphrase policy	Good	Medium	Medium	Low
26	Use DLP to secure portable media	Good	High	Medium	Medium
27	Restrict access to SMB and NetBIOS	Good	Low	Medium	Low
28	Educate users on spear fishing and social eng	Good	Medium	High	Medium
29	Inspect Microsoft Office files for abnormalities	Good	Low	Low	Low
30	Deploy signature based AV software	Good	Low	Low	Low
31	Use TLS encryption between email servers	Good	Low	Low	Low
32	Block web site access by IP address	Average	Low	Low	Low
33	Use network based IDS with signatures	Average	Low	High	High
34	Blacklist known malicious domains and Ips	Average	Low	Low	High
35	Capture network traffic for post intrusion analysis	Average	Low	High	Low

Figure 3: Australian Signals Directorate Analysis of best practices for cyber-security

The National Institute of Standards and Technology (NIST) compiles a listing of 250 security controls and sub-controls. The DoD uses a subset of approximately 150 of these controls. Ranking the controls against actual attack data in the manner that ASD uses produces some very interesting results.

Recommendation 1

The DoD Chief Information Officer (CIO), in conjunction with the Service and Agency CIOs, should investigate how to best use the attack data they experience on their various networks to evaluate the performance of their defenses.

The DoD Chief Information Officer (CIO), in conjunction with the Service and Agency CIOs, should begin collecting data on each attack against their networks, and data on how each defensive element performed in response to that attack. Several months of data collection should yield a statistically significant sample. The DoD CIO, as well as the Service and Agency CIOs, should then adopt one of the

example processes the Task Force reviewed, or devise their own analytic process. It is not important whether the same approach that Lockheed Martin, Goldman Sachs, or the Australian Signals Directorate is used, or if the Department invents their own process. But "leaving all this data on the table" is not the best way to proceed. Cyber security has long been a compliance dominated process, focused on doing specific actions on a checklist. Examining the attack data to determine what is working well, what is not, where changes need to be made, and where investment is required to better defend against troublesome or emerging threats would move the Department beyond a compliance approach towards a more dynamic performance evaluation. This will contribute strongly toward answering the four questions highlighted in this study's TOR.

Chapter 2: Inform and Engage Executives

As with many large and difficult problems facing any organization, increased executive engagement in cyber defense can be a means to help drive improvements. Because executives are increasingly held responsible for failures in cyber security, those executives will be motivated to drive compliance and improve their organization's cyber defense posture.

The first step in this process is providing executive management with a flow of information, *designed specifically for their consumption*, which addresses the background, status, trends, and remaining risks and challenges in cyber security that pertain to their networks and to the embedded processors in their systems.

The DoD has recently made a good start at this by providing senior leadership with a monthly report containing metrics that report on DoD's cyber hygiene. These metrics include: performance in patching operating systems and application software; use of two factor authentication; removal of Windows XP machines; use of Host Based Security Systems (HBSS); implementation of the DoD's standard security configuration; and other metrics as needed. The metrics are reported by each of the Military Services and Defense Agencies. The Task Force heard claims that even in the few months this information has been collected and presented, the metrics have indicated improvements in cyber hygiene across the Department.

Most of the data to-date on cyber hygiene is manually collected and self-reported owing to limitations in the current IT systems operated within DoD. This manual collection increases labor costs and leads to inaccurate and incomplete data. Improved monitoring and reporting through automation is addressed in Chapter 3 of this report.

To understand this issue, the Task Force met with a number of defense and commercial companies to see how they inform and engage their executives and boards on the topic of cyber security. The briefers included individuals working in insurance, banking and finance, e-retail, information technology, defense, and Federally Funded Research and Development Centers (FFRDCs). As expected, many of the organizations do not engage their executives very often and only if there is a serious breach of security. The Task Force believes that engaging executives at the point of a serious breach of security is too late. However, in contrast, there are also a growing number of companies whose executives and directors discuss cyber security on a regular basis. The Task Force noted some best practices of these organizations and used them as the basis for designing an improved approach for DoD. These best practices go considerably beyond compliance with mandated cyber hygiene controls and more accurately assess the security of the systems of interest.

To assist in driving improvements through executive engagement, the Task Force believes there are five topics that should be addressed, assessed, considered, and discussed on a regular basis with executives. The five topics are:

- Developments in the threat that include emerging attack techniques; systems that are frequently targeted; understanding of threat intentions; and the most concerning threat trends

- Performance of deployed defenses against actual intrusion sets experienced in the reported month and a trend-line based on previous months' performance
- Compliance with network hygiene measures as currently reported; however, compliance metrics should be prioritized in order of most effective to least effective based on the security controls that deter, detect or defeat the intrusions
- A set of "Top Five" critical areas based on expert judgment on topics such as: Risks to DoD on a daily basis (where risk involves the combination of threat likelihood, system vulnerability, and impact to the mission if degraded/lost); risks to weapon sensors or command and control (C2) systems in a combat situation; most critical or sensitive information holdings; and most critically needed technology developments; the point of these Top Five lists is to generate discussion on broader cyber issues beyond the IT *per se*
- Status of the "Top Five" of previous months (*e.g.,* investigations initiated, measures taken, progress made, metrics), highlighting any close-outs that have occurred

A monthly engagement with executives will likely be sufficient, unless circumstances dictate more immediate attention.

Recommendation 2

Based on industry best practices, the Task Force recommends the DoD CIO, in conjunction with the Service and Agency CIOs, expand their monthly cyber security status report.

The expanded report should include the following topics:

1. **Threat background and trends** – a summary of key attacks experienced in DoD networks and systems in the reporting month including source of origin, means of access, and attack intentions. Also, how these attacks compared to previous months noting any changes or trends. In addition, include similar threat information beyond DoD as compiled by security research firms. Finally include data on emerging threats and attack techniques that may be seen in the near future.
2. **Defensive system performance –** assess how well each individual deployed defensive system performed in terms of detecting an attack, stopping the progress and eliminating the threats experienced that month. Which software components are not performing as expected? Where are there overlaps in defensive coverage? Where are there gaps? How does the cost of acquiring and operating the defensive system compare to its performance?
3. **Security controls** – report on metrics for key cyber hygiene controls that DoD mandates for use by the system. In addition to measuring compliance, examine the effectiveness of the controls in detecting or eliminating threats. Compare this to other effectiveness ratings of security controls produced by outside agencies.
4. **Top five risk areas** – compile top five lists, based on expert judgment, for critical cyber security risks being faced by DoD. These lists should prioritize the risks from 1-5 and be for the following topics:
   a. Greatest cyber risks faced on a daily basis
   b. Greatest cyber risks faced during conflict with a cyber capable adversary
   c. Most sensitive data holdings

d. Key areas requiring immediate investment

5. **Tracking –** Report on the status of the "Top Five" of previous months (e.g., investigations initiated, measures taken, progress made, metrics, …), highlighting any close-outs that have occurred.

The Task Force drafted a sample monthly report (Appendix 1), designed for executive consumption, to give an example of what we recommend be used to provide a factual basis for executive review and decision making. The sample report is largely self-explanatory and includes many of the best practices and examples collected from commercial companies and the defense industry.

Chapter 3: Automate Network Management Operations

The DoD mission requires a very complex, worldwide IT enterprise, with many difficult operational needs and constraints. In addition to providing the needed capabilities, IT providers must deal with new security challenges. What is the current state of readiness of DoD's IT systems to support operations? If a new vulnerability is reported in a key IT component (e.g., "Patch Tuesday"), what are the risks across the enterprise? If adversary cyber tactics and tradecraft have succeeded in gaining access to the network, how can DoD search the enterprise for artifacts or indicators in order to assess the scope of penetration?

For DoD overall, generation and gathering of the data needed to manage cyber security is often a very manual and labor intensive process. When a crisis hits, DoD responses range from highly automated and instrumented technology to humans running around counting things, followed by the equally daunting challenge of integrating data across many disparate sources into a coherent picture. It is very expensive and of increasingly limited effectiveness to continue to operate in this manner. This manual process also makes it difficult for CIOs, CISOs and Network Administrators to get reliable, timely, and comprehensive reporting on important cyber security metrics.

If this process is thought of as an observe, orient, decide and act (OODA) loop-type of decision cycle, then it will not succeed if the core observations are outdated, of suspect quality, or too costly to collect.

Modern, well-run IT enterprises employ highly automated cyber management processes, to both update the security features as quickly as possible and to drive down the expense of running the system. These automated processes include patch management, configuration management, system discovery, system configuration audit, and security log analysis. In general, focusing on and automating a small number of key actions, rather than trying to automate all of the processes, is a cheaper option. Once implemented these systems are much less expensive to operate and provide near real time insight into the security status of the network. Based on the CIOs that met with the Task Force, the cost of operating an automated cyber management process was between 10 and 30 percent of the manual process.

In order for DoD to be successful, new technologies may be required. This should not, however, shadow the importance of implementing key processes. For example, having the operational discipline and the workforce acceptance to minimize the number of unique desktop configurations and applications can make patching dramatically easier and faster by minimizing incompatibility and regression testing.

Further, a commercial best practice is to use the data created by automation as the basis for executive accountability and performance measurement. **Error! Reference source not found.** is an example executive performance plan based on the information gathered by the Task Force during their deliberations.

1: Take deep ownership of SSL/TLS termination:

- **1.1: Exit 2016 with no SSL VIPs**
- **1.2: Exit 2016 with all HTTPS endpoints supporting the < … > recommended configuration**
- **1.3: By April 2016, understand with clarity what TLS protocol, ciphers, and options your customers use, and keep that understanding current.**

2: Radically restrict and monitor human access to data:

- **2.1: Reduce human interaction with your hosts by 80% of November 2015 activity**
- **2.2: Have <…log…> coverage for 100% of your production infrastructure and 100% of where production keys/credentials are deployed.**

5: Harden internal services:

- **5.1: Exit 2016 with zero clear text, unauthenticated services.**

6: Patching:

- **6.1: Exit 2016 with zero hosts outside of the < … > Patching SLAs.**
- **6.2: Exit 2016 with zero hosts running deprecated OSes or packages**
- **6.3: Exit 2016 with an inventory of your package dependencies and a patching strategy for each that meets the < … > Patching SLAs.**

9: Aggressively rotate credentials:

- **9.1: Exit 2016 with no passwords or API keys older than 6 months.**

Figure 4: Example executive performance plan

DoD networks are highly distributed, segmented, and diverse in many dimensions. Segment "ownership" is also quite diverse. These factors could be an issue in automating the network management operations, **but the large scale and complexity of the DoD network is not a valid excuse for inaction.** The Task Force reviewed several commercial organizations that operate networks of a similar or larger size than DoD and each has successfully implemented highly automated cyber security management processes.

Recommendation 3

The DoD CIO and CISO should architect and plan for increasingly automated cyber management operations in order to reduce the time networks are vulnerable to known attack vectors, and to increase visibility.

For the last decade DoD officials have argued that the obsolete and obscure systems running on their network do not allow modernization because functionality of those systems will be lost with modernization. However, not modernizing has continued to drive exorbitant expense and vulnerability into the enterprise. Forcing prioritization to update or discontinuing those systems to allow modernization must be a high priority—even if it means delaying other investments. In conjunction with these changes, the Military Service and Defense Agency CIOs should undertake pilot programs for virtual desktop infrastructures wherever appropriate given the numerous cyber

defense management benefits. This discussion should be led by the DoD CIO and CISO so that local issues do not inhibit the enterprise's need for better security.

It is critical that the disparate networks be able to communicate with a central system for global visibility and reporting in an automated way. Care should be taken to do this in a very secure manner so as not to give attackers an exploitable opening. Given the complexity of the DoD environment, the guiding principle should be to maintain visibility into the processes needed to move commands and data throughout the enterprise, rather than developing universal toolsets or technology.

The DoD CISO should architect and plan for increasingly automated cyber management operations in order to reduce the time networks are vulnerable to known attack vectors. It is critical that disparate networks are able to communicate with a central system for global reporting. The DoD CISO should issue guiding principles and specific performance and progress requirements to the Service and Agency CISOs for automating the following areas:

- patch distribution and management,
- system discovery,
- configuration management, and
- system configuration audit.

These items should be a specific part of executive decision making and performance management. This will result in considerable cost savings, after a short payback period, which the task force recommends be reinvested to improve defenses against more sophisticated cyber threats.

The automation of cyber management operations should be architected in a secure and resilient manner to avoid unduly increasing the cyber-attack surface. The automation must include the capability to roll back from a bad patch load. When complete, automating the above processes will result in considerable cost savings. The Task Force recommends those cost savings be reinvested to improve defenses against more sophisticated cyber threats.

USD(AT&L), in conjunction with the DoD and Service CIOs, should ensure that all program managers of future IT acquisitions enable their systems by default to be patched, configured, and audited by the chosen automation system for cyber management operations. The only exceptions to this policy should be for those systems that an up-front risk analysis determines that enabling this capability represents a greater risk. One example is when an upgrade will violate a need for system isolation.

Chapter 4: Protect Mission Critical Systems

To date, most of the DoD cyber defense focus and resources have been on defending the network-based IT enterprise assets such as servers, routers, desktops, databases, and associated software. There has not been as large an effort on protecting mission critical systems to all forms of cyber-attack.

In time of conflict, a cyber capable adversary can focus attacks on mission enabling assets and degradation of core capabilities. Such targets might include command and control (C2) systems, weapons systems, associated logistics support, and the vulnerable embedded cyber components of these systems and supporting databases.

While all systems should be fully defended against the most common, but less sophisticated cyber threats, it is both unaffordable and impractical to attempt to defend every system against the most sophisticated peer-level cyber threats.

The Task Force found that the desired capabilities of hardened systems include the ability to:

- Test and continually monitor system functional capability
- Monitor or control all data entry points
- Meet critical sensor and communication needs
- Determine how system availability is impacted by adversary attack so that improvements can be prioritized
- Assess supply chain vulnerability for potential issues requiring monitoring

Throughout the deliberations, the Task Force discussed methods for reducing the attack surface of cyber operations in DoD. The following technologies were all discussed as methods to reduce the attack surface:

- Segmentation of platforms, support systems (e.g., ISR, maintenance)
- Having a war reserve or out-of-band capability
- Determining what data are most critical, forward caching them and refreshing at a frequency determined to be appropriate
- Manage graceful system degradation

The leadership in DoD can, and should establish and execute a strategy to protect the **most critical DoD mission systems against all** forms and levels of cyber threats. This may include such capabilities as: conventional force elements with deterrent value; missile defense; essential space operations; essential command and control; and continuity of government functions. It is important to maintain a conventional force with credible deterrent value to give commanders options other than escalation to a nuclear option that all adversaries correctly realize have a high threshold for use. Because of the significant expense and difficulty to robustly defend these systems, it will be necessary to identify the fewest possible systems and dependencies to achieve mission success in each designated area. The USD(AT&L) and the Joint Staff have made good progress in determining these most mission critical systems.

Recommendation 4

A DoD-wide Executive Oversight Team (EOT) should be created to organize and manage the selection and hardening process to ensure that the most mission critical systems are protected to the highest practical level.

The Department leadership should ensure that the capabilities necessary to accomplish the most critical missions are sufficiently resilient and robust in the face of a determined and sophisticated cyber-attack. The most critical missions may include: conventional force elements with deterrent value; missile defense; essential space operations; nuclear and other essential command and control; and some systems that ensure continuity of government functions.

The team should be chaired by the DEPSECDEF and include the Chief of the Joint Chiefs of Staff (CJCS), USD(AT&L), USD(P), DoD CIO, and the Assistant Service Secretaries for acquisition. A small support staff will likely be required to assist the EOT with its responsibilities.

The Task Force recommends that for each of the mission critical systems, the following actions be taken:

- Explain the rationale for selecting this particular mission as "critical," including the current potential and consequence of loss through successful cyber attack
- Conduct a mission-based analysis, then a defensive analysis on critical systems and components
- Develop an understanding of system connectivity and vulnerabilities
- Reverse engineer the critical systems to understand vulnerabilities at the functional level that an adversary would likely attack (including the maintenance and sustainment trails)
- Develop the capability to isolate and segment systems as much as possible
- Forward cache necessary data at appropriate time intervals to further system isolation
- Identify system and supply chain vulnerabilities
- Develop workarounds or back-ups for remaining vulnerabilities
- Evaluate effectiveness through Combatant Commands (CCMDs) with measurement feedback to the leadership
- Establish metrics for this assessment in the CIO offices

Because of the significant expense and difficulty, it is necessary to identify the fewest possible systems and dependencies to achieve mission success in each area. USD(AT&L) and the Joint Staff have already made some progress in determining the most mission critical systems.

The objective should be to have the process begun immediately with implementation, completed in 2-3 years. Once implemented, DoD should evaluate the effectiveness of the resulting defense posture through the CCMDs with measurement feedback to the leadership. The DoD CIO should establish metrics for this assessment.

How to Begin

The Task Force recommends that the EOT select one mission critical system as a preliminary initial effort. Preferably, this system will be associated with an F-35 wing or Ballistic Missile Defense (BMD)

since they are both new systems that are expected to have long lives. The goal will be to determine the system's current resiliency and then determine the necessary system enhancements and support architecture to take the system to a high level of resiliency to cyber-attacks. This assessment should also include an analysis of the resources that will be needed to fund the necessary upgrades.

This effort should be led by a small team of 8 to 10 people that includes subject matter experts. This team would be called the Expert Team and will be responsible for undertaking the bulleted actions listed above.

Characteristics of the Expert Team

The recommended approach is similar to the DSB Nuclear Task Force or the Navy Cyber Awakening program. The Expert Team should contain mission experts from one or more CCMDs, system experts, adversary capability experts, and cyber security experts. To be effective, the Expert Team should be limited to 8 to 10 people. The Expert Team should have input from mission owners, system operators, acquisition, policy, and the CIO.

The Secretary of Defense (SECDEF) will charter the effort and the Expert Team will report to the EOT chaired by the DEPSECDEF.

The goal of the initial preliminary effort is to define system modifications that give a high level of assurance for mission success.

The team should develop a range of 2 to 3 options that provide varying cost points versus levels of assurance. The goal is not to harden and maintain our full force but to credibly maintain a deterrent for our most capable adversaries. All options should be subjected to an aggressive and robust red team challenge

After the initial scoping effort, the Executive Oversight Team shall charter the full effort to identify the full range of mission critical systems to be treated, develop a schedule to implement the hardening, and then implement the hardening program using the knowledge gained in the initial effort to guide the goals and objectives for all remaining systems.

Chapter 5: Include Cyber Preparedness in Defense Readiness Reporting

The Task Force was asked to determine methods to assess and provide DoD leadership with improved management insight into the level of cyber protection that currently exists or is planned. Historically, readiness reporting has been used to inform leadership at all levels about the preparedness of military units to engage in combat. Preparedness to operate in cyberspace should be a part of that overall reporting since the ability to conduct operations in all other domains—land, sea, air, and space—depends on the ability to conduct cyberspace operations.[7] For example, the ability to conduct command and control of forces depends on the ability to pass information through cyberspace, as does the ability to control the operation of weapon and sensor platforms.

Preparedness to operate in cyberspace is not now included in the Defense Readiness Reporting System (DRRS), although there is recognition of the need to do so. The discussion in this section will provide a basis for including cyberspace preparedness. There are two ways to think of this preparedness—in terms of static measures of cyber defense, and in terms of how the state of cyber defense enables mission accomplishment. Both will be discussed below, although the latter method is preferable.

These two methods have their analogy in traditional readiness reporting. Originally, a unit's state of readiness was given in terms of static measures such as the number of hours of unit training or the number of platforms (e.g., tanks) ready to deploy. While useful, these measures did not directly indicate the readiness of a unit to accomplish its missions. For this reason, readiness reporting now includes an assessment of the ability of units to accomplish their formally defined mission essential tasks (METs), which units derive from the universal joint task list prepared by the Joint Staff.[8] Based on this assessment, a commander can then aggregate the lower level unit readiness and specify the overall readiness of his command to accomplish its assigned missions.

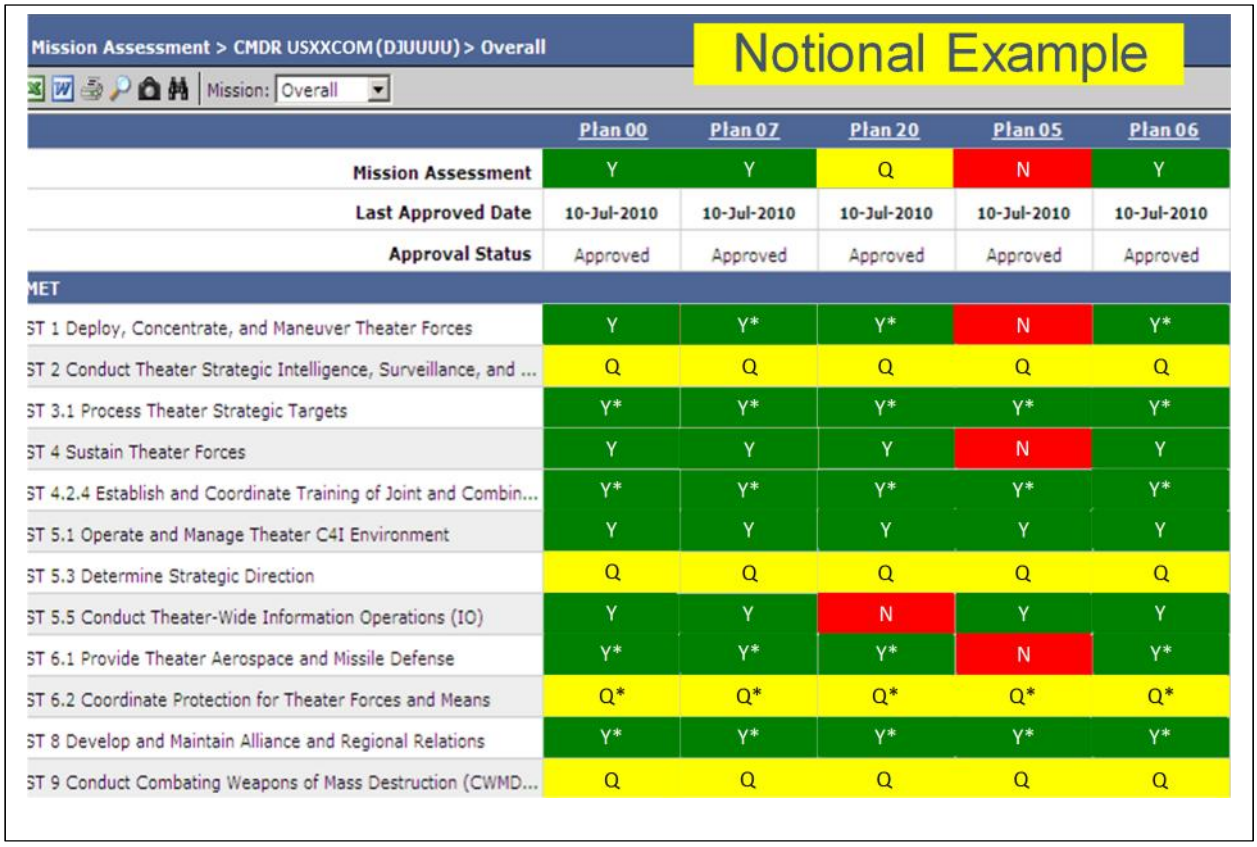
Figure 5 gives a notional example of such current readiness reporting.[9] The state of readiness for each MET (rows) for the command's set of plans (columns) is given by the colored blocks in the chart—green for ready, yellow for questionable, and red for not ready. The overall roll-up for each plan is given at the top of the chart.

[7] In keeping with the subject of this report, the discussion here pertains only to cyber defense. Cyber offense is a separate, important topic.

[8] The Joint Staff, *Joint Mission Essential Task List (JMETL) Development Handbook,* September 2002.

[9] The METs shown on the left-hand side of the figure are at the strategic-theater level (ST), such as would be reported by a Combatant Commander. METs also exist at the lower operational and tactical levels.

As indicated, current readiness reporting as exemplified by Figure 5 does not factor in cyber preparedness. The objective is that future reporting will do so.



	Plan 00	Plan 07	Plan 20	Plan 05	Plan 06
Mission Assessment	Y	Y	Q	N	Y
Last Approved Date	10-Jul-2010	10-Jul-2010	10-Jul-2010	10-Jul-2010	10-Jul-2010
Approval Status	Approved	Approved	Approved	Approved	Approved
MET					
ST 1 Deploy, Concentrate, and Maneuver Theater Forces	Y	Y*	Y*	N	Y*
ST 2 Conduct Theater Strategic Intelligence, Surveillance, and ...	Q	Q	Q	Q	Q
ST 3.1 Process Theater Strategic Targets	Y*	Y*	Y*	Y*	Y*
ST 4 Sustain Theater Forces	Y	Y	Y	N	Y
ST 4.2.4 Establish and Coordinate Training of Joint and Combin...	Y*	Y*	Y*	Y*	Y*
ST 5.1 Operate and Manage Theater C4I Environment	Y	Y	Y	Y	Y
ST 5.3 Determine Strategic Direction	Q	Q	Q	Q	Q
ST 5.5 Conduct Theater-Wide Information Operations (IO)	Y	Y	N	Y	Y
ST 6.1 Provide Theater Aerospace and Missile Defense	Y*	Y*	Y*	N	Y*
ST 6.2 Coordinate Protection for Theater Forces and Means	Q*	Q*	Q*	Q*	Q*
ST 8 Develop and Maintain Alliance and Regional Relations	Y*	Y*	Y*	Y*	Y*
ST 9 Conduct Combating Weapons of Mass Destruction (CWMD...	Q	Q	Q	Q	Q

Figure 5: Defense Readiness Reporting System display

Findings

During deliberations, the Task Force discussed the differences between static reporting measures and mission-based reporting measures for the state of cyber preparedness in our defense forces. Below are descriptions of both methods with a conclusion of which method is preferable.

Static Reporting Measures

Two current examples of static reporting measures are described here. The first is the requirement in the DoD Cybersecurity Discipline Implementation Plan that "Commanders at all levels will report their status with the requirements in this Implementation Plan via the Defense Readiness Reporting System."[10] The referenced requirements refer to progress in four lines of effort:

- Strong authentication

[10] DoD Cyber Security Implementation Plan, October 2015, Amended February 2016, page 3, accessed at http://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf

- Device hardening
- Reduced attack surface
- Alignment to cybersecurity and computer network defense providers

The reported measures are a set of 17 binary results (achieved or not achieved) for individual units – e.g., "do all web servers and web applications internal to the NIPRNet require DoD approved user authentication."

The second example comes from the U.S. Navy's Pacific Fleet (PACFLT) and is illustrated in the Figure 6. This report refers to a carrier strike group (CSG), in this case the Theodore Roosevelt CSG. Six cybersecurity measures (groups of columns) for relevant networks (individual columns) are given for the carrier and its major companion ships (rows). The definition of the measures, how they are to be measured, and the criteria (green, yellow, red) associated with them are given at the bottom of the chart. The intent is that reports like this be produced monthly for the CSGs in PACFLT.

ACAS/Retina Scans	VRAM								WSUS					
	Scan Currency		Scan Integrity		Scan/Patch/Scan Results				Synchronization		Configuration		Patch Deployment	
	NIPR	SIPR	NIPR	SIPR	SF NIPR	SF SIPR	POR NIPR	POR SIPR	NIPR	SIPR	NIPR	SIPR	NIPR	SIPR
Theodore Roosevelt	2	4	97	95	.32	2.7	5.4	6.6	1	1			96	82
Normandy		4	95	100	.49	.46	4.8	-	2	2			98	86
Winston Churchill		1	100	100	.19	.51	2.2	7.0	1	1			98	96
Forrest Sherman		1	97	93	.10	.08	5.4	5.5	1	4			99	96
Farragut	1	2	97	100	2.4	10	3.1	13	1	1			95	91
What	Sites will conduct monthly scanning. In addition, scan results for all assets will be uploaded NLT 20th of each month		After SCAN upload, validates SF used the appropriate credential, audit file, scan engine and covered all assets and clients		Measures #'s of patches which SF did not apply and are available		Identify # of patches which POR's have not made available and is within the ability of the POR to provide		the tracking of the Ships SWUS server to successfully sync with the NOC server		The tracking of which mode WSUS is currently in; either Replica or Autonomous		The total package of approved updates installed by the ship	
How	Verfity Scan Currency via Scanned Assets Summary/Days Since Last Scan		Verfity Scan Integrity via Scanned Assets Summary/Scan Integrity; Verfity All Systems Scanned		Requires system x system analysis of POR available vs. Site application		Requires system x system analysis of POR available vs Site application		FRD verify # synchronization days from SSC LANT provided weekly report		FRD verify configuration mode from SSC LANT provided weekly report		FRD verify % Approved Updates Installed from SSC LANT provided montly report	
Criteria	100% Pass		>90%			<2.6 (Minor)			<7 Days		Replica		>90%	
	<100% Not Passing		70%-89%			=>2.5 - <3.5 (Moderate)			7-14 Days		Autonomous		70%-89%	
	# reflects systems not current		<70%			=>3.6 (Critical)			>14 Days				<70%	

Figure 6: PACFLT Example – CSG Cyber Readiness Report

The two examples above provide information that can be quite useful to their respective unit commanders and superior officers, as well as to civilian leadership, particularly if monitored on a continuing basis. They will indicate if the cybersecurity postures of the units in question are improving or declining, and will identify particular problems. Unfortunately, they still do not bear directly on the ability of a unit to accomplish its mission. That topic will be addressed next.

Mission-Based Reporting Measures

Mission-based reporting measures are founded on the notion of mission assurance—Combatant Commanders (CCDR) must be prepared to execute assigned missions successfully in the face of cyber threats. Three ways for the CCDRs (and their subordinate commanders) to prepare are:

- Conduct cyber dependency analyses for missions and ensure that adequate cyber protection is provided for the critical dependencies;
- Augment operation plans with contingency measures to enable operation in cyber degraded conditions; and
- Conduct exercises to test the adequacy of protection means and contingency planning for missions.

Each of the mission assurance activities is next considered in more detail, followed by a discussion of how their measures can be factored into overall readiness reporting.

Cyber Dependency Analyses

The cyber dependency analyses can be broken into the following steps:

1. For a given mission, identify the essential operational tasks necessary for mission execution
2. For each essential task, identify the critical cyber components upon which task execution depends
3. Characterize the anticipated threat to the cyber components
4. Characterize the vulnerabilities of the cyber components
5. Develop procedural & technical means to mitigate the threat & vulnerabilities
6. Implement the means for mitigation

To illustrate how to approach this analysis, a representative mission, Joint Close Air Support (JCAS), is depicted in Figure 7. The mission is initiated by the Joint Tactical Air Controller (JTAC) making a request for air support that passes through the Army chain of command and then to the Air Force at the Air Support Operations Center (ASOC). This leads to the assignment of an attack aircraft to provide close air support. Once the attack aircraft is assigned, it and the JTAC interact directly in conducting the attack. Having a mission description such as this, one then proceeds through the threat, vulnerability, and mitigation steps. All are key to the cyber dependency analysis.

The CCMDs, as owners of the missions, must assume the lead for the dependency analyses, with broad DoD and IC support. Specific responsibilities are:

- CCMDs carry out the analyses for their missions (e.g., as given in their Operational Plans (OPLANs))
- Military Service components to the CCMDs, USCYBERCOM, National Security Agency (NSA), and Defense Information Systems Agency (DISA) support execution of these analyses
- CCMDs implement the procedural mitigation measures identified
- Military Services, USCYBERCOM, NSA, and DISA implement the identified technical mitigation measures

Elements of DoD are beginning to carry out these dependency analyses. Cyber Protection Teams, resourced by the Military Services and assigned to USCYBERCOM, are allocated to CCMDs with the specific purpose of conducting mission assurance analyses. Some initial results are available from the Cyber Protection Teams, and this body of information will grow as the teams reach full operational capability in Fiscal Year 2018 (FY18). The Military Services themselves have also begun conducting the analyses. The mission assurance measures defined above will provide a systematic way to track, on a mission basis, the extent the dependency analyses have been conducted and the means of protection means that are implemented in response.

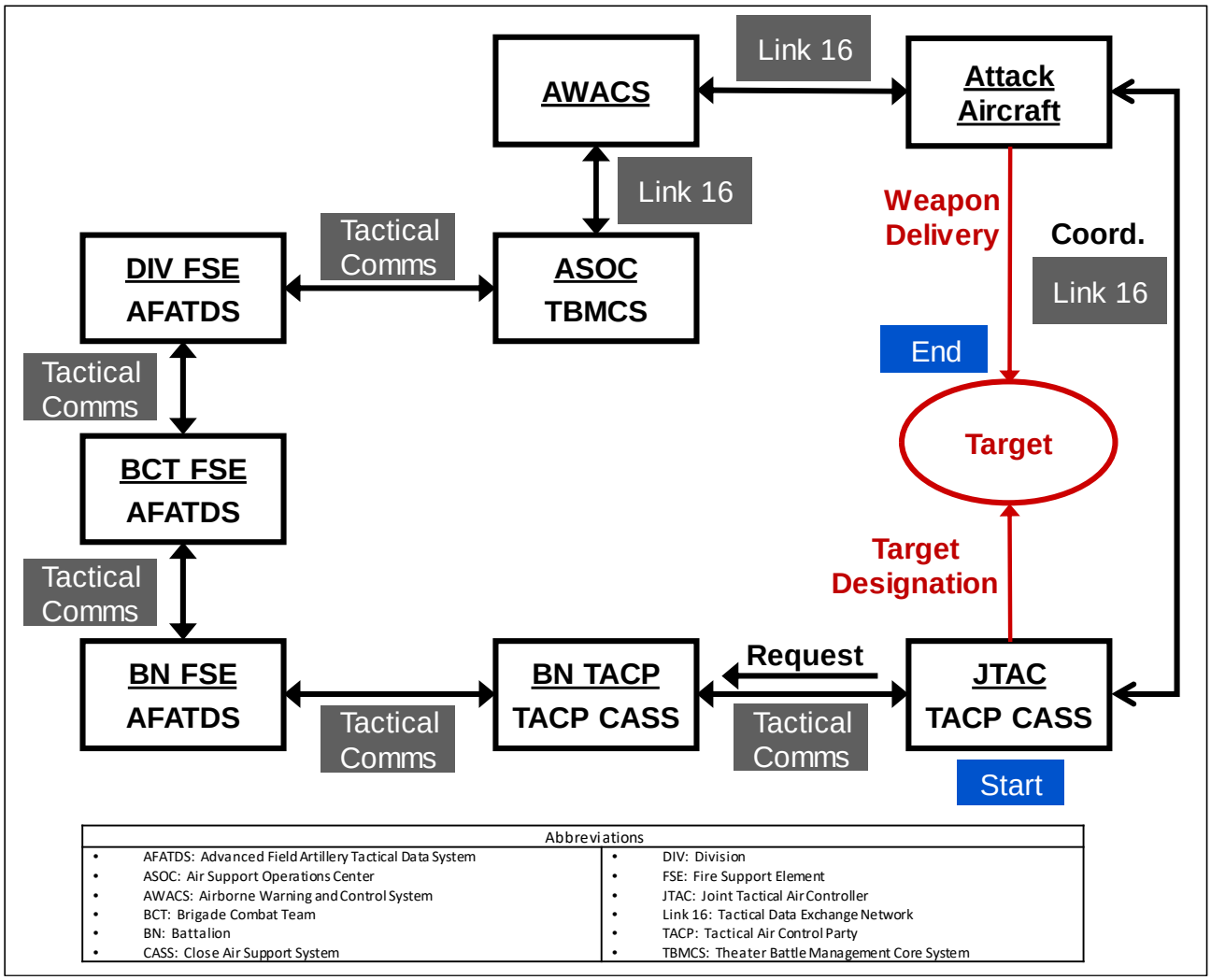


Figure 7: Joint Close Air Support Mission Thread

Contingency Planning

No matter how thorough the dependency analyses and implementation of the associated protection means, the possibility of some successful cyber-attacks by an adversary must be assumed. Thus, contingency measures to enable "fighting through" in cyber-degraded conditions are necessary. The contingency measures are "work-arounds" to accommodate the loss or degradation of critical cyber

assets identified in the dependency analyses. These "work-arounds" are both procedural and technical. Representative contingency means are:

- Fallback procedures to deal with loss or compromise of data, degraded or lost connectivity and processing
- Survivable war reserve networks
- Data backup with integrity checks
- Recovery procedures for hosts and networks, including use of out-of-band networks

The mission assurance measure for contingency planning will assess the degree to which contingency plans have been established to compensate for the degradation or loss of critical assets. This measure would be reported as a percentage of the critical assets for which contingency means have been established for the serious degradation or loss of the asset. Note that for this measure to be meaningful, the contingency plans need to be assessed as both implementable and effective, at least in a qualitative sense.

Each CCMD, with support from the Services, would conduct their own contingency planning and implement the contingency means. Currently, such efforts are being conducted to a limited extent by the U.S. Pacific Command (USPACOM) and the PACFLT.

Exercises

Exercises should be conducted to test the adequacy of protection means and contingency planning for the missions. Important elements of the exercises are to:

- Define mission objectives and measure the extent they are met in degraded cyber environments
- Use realistic cyber threats, unrestricted to the extent feasible
- Conduct rigorous after-action reviews to assess execution and derive improvements

The mission assurance measure for exercises is the extent that exercises have been conducted to assess how well the missions can be accomplished in the face of cyber threats.

The second aspect is the percentage of a command's missions examined in exercises using realistic cyber threats and rigorous assessments, the realism in threat play, and the depth of assessment being provided. The degree of success is a value measure that is the percentage of each mission objective (e.g., deployment rate, weapons delivery) met in the exercise.

The CCMD conducts the exercises, drawing on Service resources. The major CCMD exercises are of limited utility for the purposes described here. Those exercises have to satisfy many other purposes and hence cannot allow cyber disruptions to impede overall progress of the exercises. Smaller, more dedicated joint environments are required. Some of the Military Service exercise venues (e.g., the Air Force's Red Flag) would also be useful.

Aggressive cyber play may not be allowed on general-purpose networks because of the side effects that can result, and also adversary observation of the tools and techniques being employed. Closed cyber ranges, augmented to represent full mission play (e.g., simulations), could be an important

environment for conducting the exercises. DoD is currently giving increased attention to the use of cyber ranges.

Measuring value can be pursued in more detail. Exercises can be used to measure the value of cybersecurity enhancements, or conversely the cost in operational effectiveness of not having the enhancements. The idea is to conduct an exercise with and without a set of enhancements and measure the difference in operational effectiveness (the degree mission objectives are accomplished).

Exercises conducted to assess the results of dependency analyses and contingency planning can also be used to extract empirically derived planning factors. For example, the command and control processes used in an exercise can be examined to understand the impacts on planning factors such as how decision speed was impeded or target location accuracy was degraded. Analytical models of the processes can be built and the planning factors used therein. The models would then be used to assess the value of implementing suggested cybersecurity enhancements.

This approach based on analytical models and planning factors is speculative. It is not addressed further in this report, but it could be a promising approach worthy of further investigation.

Relationship to Readiness Reporting

The discussion above derived five mission assurance measures that include:

- Identifying critical cyber assets for the mission
- Assessment that those assets for cyber vulnerabilities
- Implementation of protection means for identified vulnerabilities
- Establishment of contingency plans to compensate for the degradation or loss of critical assets
- Conduct exercises to assess how well the missions can be accomplished in the face of cyber threats

This study advocates that these measures be reported by each of the CCMDs for their forces since they are mission-based assessments. The measures can be included in the DRRS as an adjunct to the information currently reported.

The measures can also be folded into overall readiness reporting, thereby incorporating the state of cyber preparedness into the overall preparedness of military units to engage in military operations. As stated above, current readiness reporting expresses the ability of military units to accomplish their mission essential tasks (METs). Those assessments take static measures (e.g., resource availability, level of training, etc.) and applies expert judgment to come up with the MET assessments. Similarly, the cyber mission assurance measures can be used in this process along with expert judgment to provide the MET assessments. The ability to accommodate the cyber measures will not happen immediately. An experience base must be built.

Overall Conclusions

CCDRs must be prepared to execute assigned missions successfully in the face of cyber threats. Mission assurance assessments (defined above) can be used to express the degree of preparedness for carrying out tasks comprising missions in the face of cyber threats. While limited assessments are now being conducted, a much more robust program is required.

These mission assurance assessments can be included in the DRRS, the standard DoD vehicle for reporting the readiness of military units and commands to engage in military operations. First, as the separate mission assurance measures referring to cyber preparedness, and second, as folded into the overall readiness statements for units and commands.

Recommendation 5

For its assigned missions, each CCMD, with support of the Services should report their cyber preparedness along with the other elements of the DRRS. Updates to these assessments should follow the normal Defense Readiness Reporting schedule.

For its assigned missions, each CCMD, with support of the Military Services, should report through the DRRS the following:

- Have assets critical for the mission been identified, *e.g.,* thru mission thread analyses?
- How many of those assets have been assessed for cyber vulnerabilities, *e.g.,* by Cyber Protection Teams and Service technical analysts?
- Is there a schedule for cyber-assessing the remaining critical assets?
- To what extent have protection means been implemented for the identified vulnerabilities, both procedural and technical?
- To what extent have contingency plans been established to compensate for the degradation or loss of the critical assets, *e.g.,* fallback and recovery procedures to meet minimum operating requirements?
- Has each exercise been used to determine the value of cyber defense as it pertains to the mission objectives of that particular exercise?
- Have exercises been conducted to assess how well the missions can be accomplished in the face of cyber threats, involving realistic threats, red team play and quantitative assessment of mission execution?

Some activity is ongoing now pertaining to most of the items in this recommendation, so it should be possible to quickly initiate implementation of the recommendation. Standards defining how the mission assurance measures are to be reported should first be established so there is common understanding by all parties involved. That definition should not take long (nor should it be allowed to get hung up in bureaucratic process that will take a long time); approximately six months should be adequate. The periodic reporting should occur every six months. This frequency is not so frequent that it overburdens those conducting the assessments. Highest priority in the reporting and the associated cyber preparedness improvements should be given to those missions deemed most critical.

Chapter 6: Build on Current Modeling Efforts to Inform Investment

These four tasks described in the terms of reference for the task force serve as the basis for establishing the goals and objectives of the models required for understanding relationships between DoD cyber investments and the amount of increased resilience. A successful family of models that account for past and future successes and failures of DoD's cyber investments will serve to improve DoD's ability to analyze its overall cyber investment decisions.

The four tasks are:

- Task 1 - Provide DoD leadership with improved management insight into the level of cyber protection that currently exists and is planned within DOD networks, sensing, weapon and support systems
- Task 2 - Develop approaches to assess system resilience or surrogates for informing system resilience, to different kinds and levels of cyber attack
- Task 3 – Develop methods to understand relationships between DoD cyber investments and the amount of increased resilience to attack
- Task 4 - Develop prioritized recommendations for the "next dollar spent" for maximum effect against cyber threats, and the priorities for investment

Task 1 above, when accomplished, provides the data necessary to partially drive the other three tasks. Quantitative data collection and analysis on the current state of cyber protection across DoD is critical in understanding the gaps that must be addressed. A critical element of this task is the establishment and standardization of the data and metrics that will be used. The department must identify and train organizations on the methods and techniques for capturing and reporting the required data. Additionally, having an established technology roadmap that addresses both sustainment and insertion plans provides decision makers with the insight necessary to determine how best to select and time upgrades appropriately.

Beyond the processes, procedures, and techniques resulting from performing Task 2 and Task 3, completing these tasks provide an opportunity to employ modeling, simulation, and analysis (MS&A), such as predictive analytics. A key required skill necessary for the execution of Tasks 2 and 3 are data scientists. Data scientists provide the necessary support for optimizing what data is captured, the processes involved that generated the data and what analysis must be performed to extract the knowledge or insights from the data. These analyses are a means to predict the impact of evolving threats and determine the resilience of the system and its mission assurance based on the counter measures DoD might employ in response. Predictive analytics is the use of data, statistical algorithms, and machine-learning techniques to identify the likelihood of future outcomes based on historical data.

The data required to drive the analysis and modeling is a byproduct of the deployment of continuous monitoring services mandated by the Risk Management Framework (RMF) and now being adopted

across DoD. RMF is the unified information security framework for the entire federal government that is replacing the legacy certification and accreditation (C&A) processes within the DOD, the intelligence community (IC) and other government agencies (OGA). The adoption of the RMF across DoD is providing improved insight and understanding of the level of cyber protection now in place across our military systems and correspondingly, the level of risk being accepted by data and system owners. Throughout DoD, systems are being retrofitted or designed to comply with continuous monitoring capabilities, which allow increased awareness of the security posture of our military systems. The work is by no means done. RMF, if fully adopted and enforced, does have the capacity to significantly improve upon the security posture of our systems.

Discrete modeling and simulation techniques coupled with the use of the Markov decision process and stochastic math models enhance the results by accounting for the inherent randomness found within systems operating within a cyber-contested environment.

Task 3 is challenging as it requires the establishment of a uniform set of metrics across all DoD elements, a means to aggregate and normalize the data, and finally the creation of a cross-reference matrix between the data results and the corresponding cyber defense expenditures. A model is now being built in DoD that provides the basis for partially satisfying the objectives of this task. The model provides visibility into past and current DoD cyber defense expenditures as well as an understanding of how various expenditures have been prioritized. The critical element needed to satisfy this task is identifying, capturing, and mapping the metrics representing the resulting cyber resilience created as RMF-based controls are deployed across the enterprise. As part of this work, some effort is being expended to understand what are the most critical systems and how each of the military systems' operational effectiveness is impacted as cyber defense capabilities are introduced. It is important to recognize that an increase in resilience does not always equal an increase in operational effectiveness.

In achieving the objective defined for Task 4, a combination of models is required to adequately address all contributing factors and to provide OSD with a keen insight into the value of alternative cyber defense investments. Modeling and simulation holds the potential to enable DoD decision makers to rely upon analytics as their primary means for understanding how a cyber defense investment may impact mission assurance and system resiliency when operating in a cyber contested environment. As illustrated in Figure 8, a combination of financial, heuristic, and effects-based operational assessment modeling will enable DoD to predict how an investment may improve overall system risk and how that investment may impact system resiliency and mission assurance.

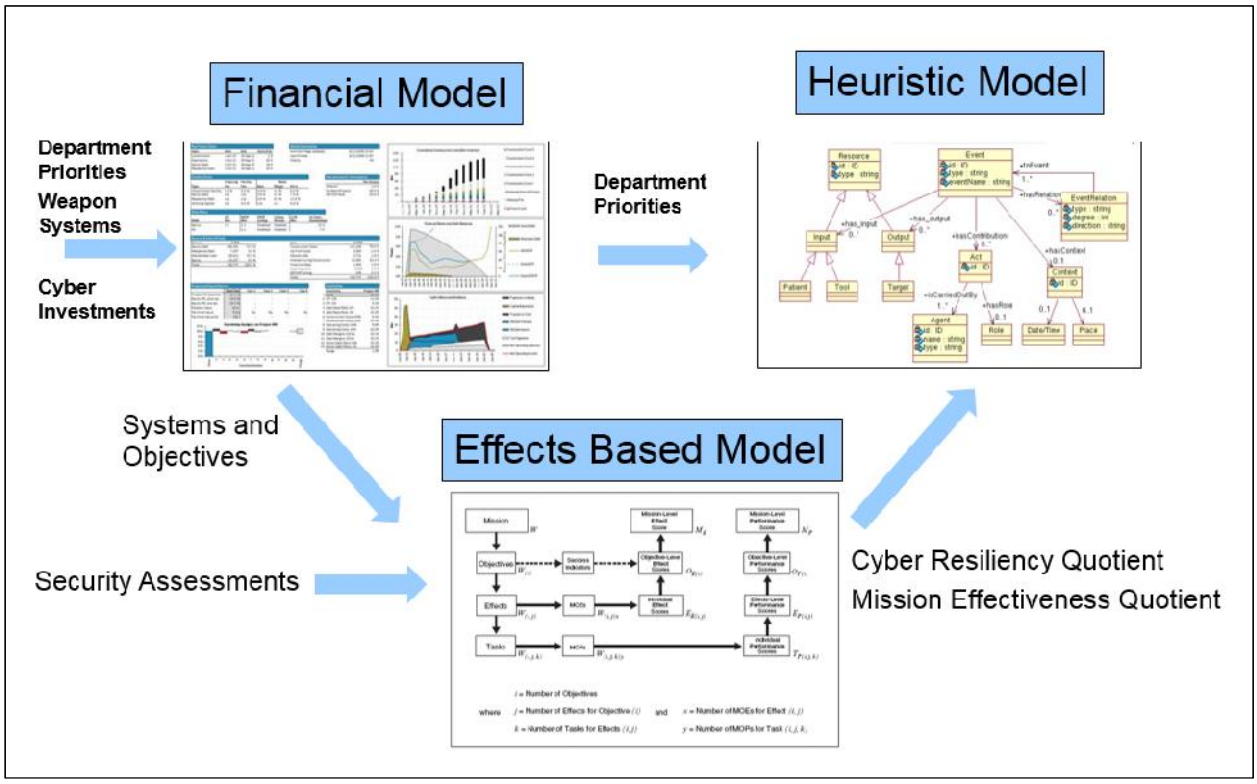


Figure 8: Cyber investment modeling enables quantitative decision making

The financial model and the heuristic models are addressed partially by the effort required to perform Task 3. Efforts now being performed by ODASD(C3CB) serve as a foundation for addressing the objectives of Task 3 and provide the inputs necessary to successfully accomplish Task 4.

In Task 4, a new concept is introduced for use in cyber investment modeling, effects based modeling. The goal is to quantitatively establish how a cyber defense investment applied to a category of military systems may result in improved effectiveness of that system in a cyber contested environment. An essential element to successfully performing Task 4 is the creation of a team with a broad understanding of the various systems and platforms now used within DoD and their overall interdependence in achieving the national security goals of the United States. This data serves as the basis and primary driver of the model.

The objective of the model is to calculate measures of performance (MOP) and measures of effectiveness (MOE) for a system based upon the cyber defensive actions and investments that were made. The model is based on the concept of effects based operations (EBO). EBO provides the basis for determining if a cyber defense investment has the potential to improve the effectiveness of a military system. In essence, by determining how a cyber defense investment performs and what the resulting MOEs are for the system in which the cyber defense actions were applied, it is possible to quantitatively prioritize which investments will provide the highest degree of resilience necessary to allow a military system to meets its objectives. In addition, the resulting measures have the potential to be integrated into the models created under Task 3 for the purpose of understanding the

relationship between increased cyber resilience and overall mission effectiveness. The suggested EBO approach does not account for cost relative to an improvement in resilience.

Back testing will be used to evaluate the accuracy of the model based upon how previous cyber decisions impacted the overall mission. Data science will be incorporated into the model validation process so as to fully understand how specific decisions may affect the overall outcome. In addition, through data science additional knowledge may be gained in terms of intersystem dependence which may further support the investment decision process.

Findings

The DoD has defined three primary missions within the cyber space domain.[11] They are to:

- defend DoD networks, systems, and information;
- defend the United States and its interests against cyber attacks of significant consequence; and
- provide integrated cyber capabilities to support military operations and contingency plans.

In 2015, the DoD budget appropriated over $5.1 billion towards accomplishing these missions, and $5.5 billion has been requested in the 2016 DoD budget. Additional funds also are inherently contained within the budgets of each service branch and major acquisition activity. Similar levels of investments can be found in federal, state, and local governments as well as the private sector. Recent reports estimate that organizations within the United States are spending more than $15 billion each year to provide security for communications and information systems.[12]

Reporting on penetrations of DoD systems clearly demonstrate that the current cyber defense investment approach is not working. The DoD is not the only organization facing poor results. Recent reports estimate the loss to the United States as a result of cyber espionage and cybercrime is over $100 billion dollars per year.[13,14]

The DoD faces a cyber defense investment challenge. If it is to be successful in accomplishing its three cyber missions, it must develop and adopt new and improved decision making strategies that optimize its resources while achieving measurable improvements in the cyber resilience of its networks. Decision making activities for allocating cyber defense investment funds requires careful consideration of the following two factors:

- Cost of implementing a cyber defense capability
- Cost impact that capability will have on the organization

These two factors represent the direct and indirect costs of cyber defense investment strategies and are at the core of how to use limited human and financial resources to best protect U.S. military

[11] Department of Defense, *The DoD Cyber Strategy*, accessed April 2015, available at http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

[12] Market research by the Armed Forces Communications and Electronics Association, 2013; Gartner 2013.

[13] P. W. Singer and A. Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press. 2014.

[14] S. Gorman. & D. Yadron. (23 May 2013) "Iran Hacks Energy Firms, U.S. Says," Wall Street Journal.

systems. The key to improving DoD system resilience is through the optimization of these cost factors to ensure the right investments, are made on the right systems, at the right time. The proper allocation of funding holds the potential to dramatically improve not only the level of cyber resilience in the enterprise, but also realize improvements in mission effectiveness and reductions in operational and maintenance costs as post-penetration clean-up actions are reduced.

Economic Models of Cyber Security

Optimization of cyber defense cost factors can be greatly improved if DoD were to adopt a models based approach for Cyber Defense Investment decision making. Through modeling, DoD is able to address the increasing uncertainty associated with the cyber defense posture within DoD. The uncertainty is driven by a number of factors, many not within the control of DoD.

Table 1: Cyber Defense Investment Models

Model Type	Presented By	Purpose/Goal
Macro-economic input/output	Santos and Haimes, 2004	Evaluate sensitivity of the U.S. economy to cyber attacks in particular sectors
Macro-economic input/output	Garcia and Horowitz, 2006	Determine level of underinvestment in cyber security
Econometric	Campbell et al. 2003	Analyze the loss of market capitalization after a cyber security incident
Financial	Geer, 2001 Gordon and Loeb, 2005 Willemson, 2006	Determine the return on security investment
Real World Simulation	Dynes, Brechbuhl, and Johnson, 2005 Johnson and Goetz, 2007 Pfleeger, Libicki and Webber, 2007	Model real world decision making and use it to recommend future investment decisions
Heuristic	Gal-Or and Ghose, 2005 Gordon, Loeb, and Sohail, 2003	Ranks costs, benefits, and risks of strategies for allocating resources to improve cybersecurity
Risk Management	Baer, 2003 Conrad, 2005 Farahmand et. Al. 2005, Geer 2004, Gordon, Loeb, Sohail, 2003 Haimes and Chittester 2005 Soo Hoo 2000; Baer and Parkinson 2007	Characterize behavior through a risk management and insurance framework
Game Theory	Gal-Or and Ghose 2005 Horowitz and Garcia 2005 Irvine and Thompson, 2005	Resource allocation in cybersecurity

Continuing evolution of threats and vulnerabilities coupled with shifting motivation of attackers and the imputed cost of successful penetrations makes it difficult to decide where cyber defense resources should be focused. Further compounding this difficulty is DoD's increasing and changing use of information technology. As the use of information technology expands, the number of potential targets increases, as does the probability of a successful attack.

Modeling and model-based tools have been developed and used to support decision making and to address the uncertainty inherent within this domain since 2000. What has been learned through previous efforts is that there is no one single model by itself that can account for the wide range of attributes required to effectively support decisions on cyber defense investments. Some examples of attempts to model cyber investment decisions are shown in Economic Models of Cyber Security

Optimization of cyber defense cost factors **can be greatly improved if DoD were to adopt a models** based approach for Cyber Defense Investment **decision making. Through modeling, DoD is able to** address the increasing uncertainty associated with the cyber defense **posture within DoD. The** uncertainty is **driven by a number of factors, many not within the control of DoD.**

Table **1**.

Every model is developed for a specific purpose and, as such, includes a different set of assumptions and constraints. Prior to using any model, it is critical that, it is well understood what the model provides, the data that feeds it, the assumptions and constraints used by the model, and the goals of the model.

A search of available literature has identified at least two sources for creating a set of metrics that may be used to drive the models. The first is from Global Information Assurance Certification (GIAC) enterprises. The metrics described in this report are based upon the SANS Institute's Top 20.[15] The second source is from the MITRE Corporation as part of their Resilient Architectures for Mission Assurance and Business Objectives (RAMBO) project.[16]

Of the models presented in Economic Models of Cyber Security

Optimization of cyber defense cost factors **can be greatly improved if DoD were to adopt a models** based approach for Cyber Defense Investment **decision making. Through modeling, DoD is able to** address the increasing uncertainty associated with the cyber defense **posture within DoD. The** uncertainty is **driven by a number of factors, many not within the control of DoD.**

[15] C.I. Cain and E Couture, GIAC Enterprises, *Establishing a Security Metrics Program: A Final Report*, 14 October 2011

[16] D. Bodeau, R. Graubart, L. Lapadula, P. Kertzner, A. Rosenthal, and J. Brennan, The MITRE Corporation, *Cyber Resiliency Metrics, Version 1.0, Rev. 1*, April 2012.

Table **1** above, two have been identified as having goals that are aligned with the challenge put forth in the Task Force's terms of reference.

- **Financial:** The Gordon-Loeb model is a mathematical economic model analyzing the optimal investment level in information security. From the model, one can conclude that the amount an organization spends to protect information should generally be only a small fraction of the expected loss (i.e., the expected value of the loss resulting from cyber or information security breaches). The Gordon-Loeb Model also shows that, for a given level of potential loss, the optimal amount to spend to protect a given information set does not always increase with increases in that information set's vulnerability. In other words, organizations may derive a higher return on their security activities by investing in cyber or information security activities that are directed at improving the security of other information sets even though their vulnerability may be less. That is because the return on investment for protecting a given information set is a function both of its vulnerability and the cost of a breach.
- **Heuristic:** The heuristic model reflects the interactions among the forces that affect cybersecurity and their impact on the cost of ensuring cybersecurity. These factors include the sum of the losses from cyber attacks, the resources required to mount effective defenses, and the reduction of a network's value based on the restrictions for its use.
- **Risk Management**: The risk management model is defined within the DoD 8500 Risk Management Framework documents. This model is found within the security assessment and authorization process as defined in conjunction with the Risk Management Framework (RMF). While not one of the three models identified as supporting the cyber investment decision process, the Risk Management model does generate Security assessment data used by the effects based model as shown in Figure 8.

The financial and heuristic models form the basis for addressing the goals and objectives of the TOR. Through their inherent focus on economic, cyber defense, cyber resilience and operational system effectiveness factors they provide close alignment with DoD's cyber defense strategy. The concept of using modeling to make decisions on cyber defense investments is maturing as efforts to collect and quantify the results of past investments improve with the requirements established by the RMF. The aggregation of the results of these models will enable DoD to arrive at a decision that accounts for the direct and indirect costs associated with a cyber defense investment.

Cyber Security Effect Based Assessment Model

A third model, the cyber security effect based assessment model, is one based on the concept of operational effectiveness. This concept has been used successfully in establishing whether tasks that are defined and executed are meeting the intended mission objectives. The U.S Air Force has used this approach quite successfully in planning and executing operational missions.

As with any model, uncertainty is a function of the quality of the input data. In the case of effects-based modeling of cyber security, the soundness of the input data is driven by the following three factors. First is the availability and validity of the data itself. Second, this uncertainty is further complicated by the dynamic nature and varying severity of the threats and vulnerabilities that the

enterprise faces. The third factor that contributes to uncertainty is the validity and "noisiness" of the metrics used to measure the effectiveness of mitigation actions taken to counter threats and vulnerabilities. Removing or lessening the uncertainty requires the establishment of an integrated approach whereby a standard set of metrics is defined and collected by all organizations thereby improving the consistency, meaning, and relevancy of the data. Additionally, through increases in vulnerability research, potential future attack vectors and their implication can be identified and incorporated into the model thus avoiding or minimizing the potential effects of zero days.

Measures of Effectiveness: Are We Doing the Right Things?

Using the metrics collected across DoD for the systems and investments being considered, the model shown in Figure 9 is populated to define and establish the objectives and tasks that must be performed to improve cyber defense of a system and improve the mission assurance.

An assessment is then performed to generate measures of performance (MOPs) and measures of effectiveness (MOEs) for each individual task. The result is a quantitative measure that establishes the probability of success or improvement that will be achieved against the established objectives. The operational assessment methodology described is shown in Figure 10.

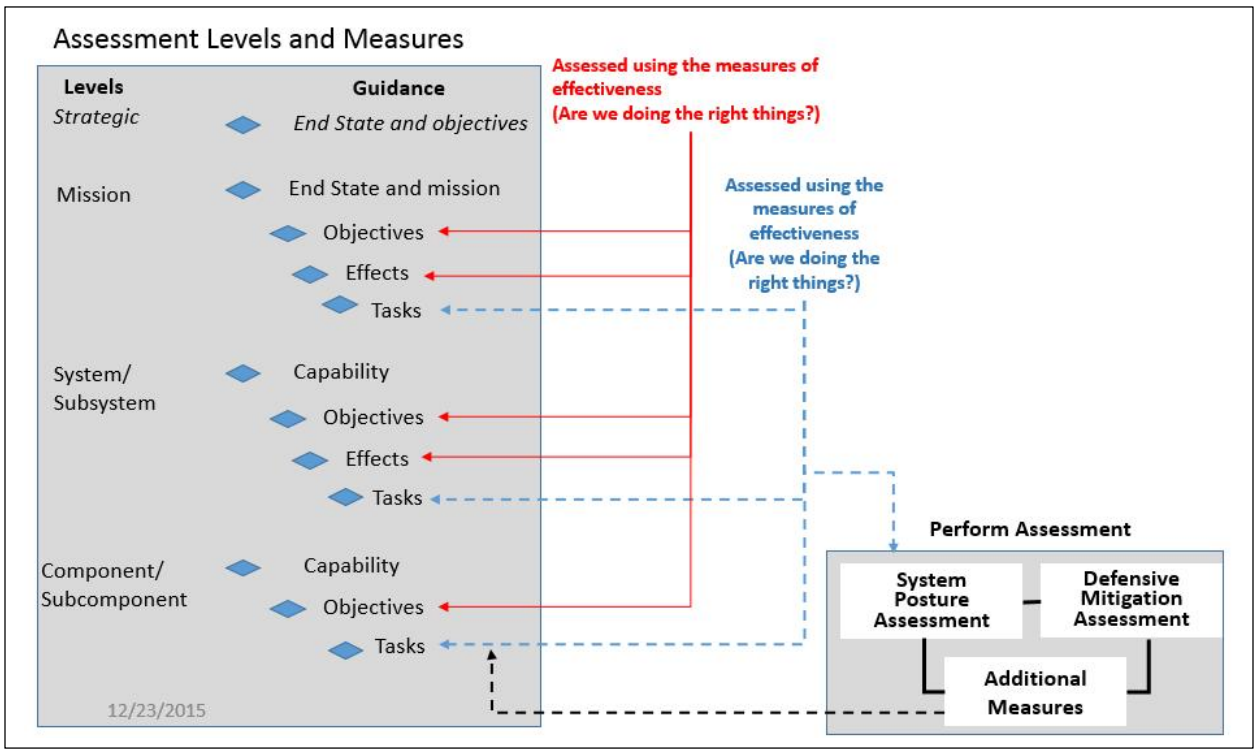


Figure 9: Effects based assessment

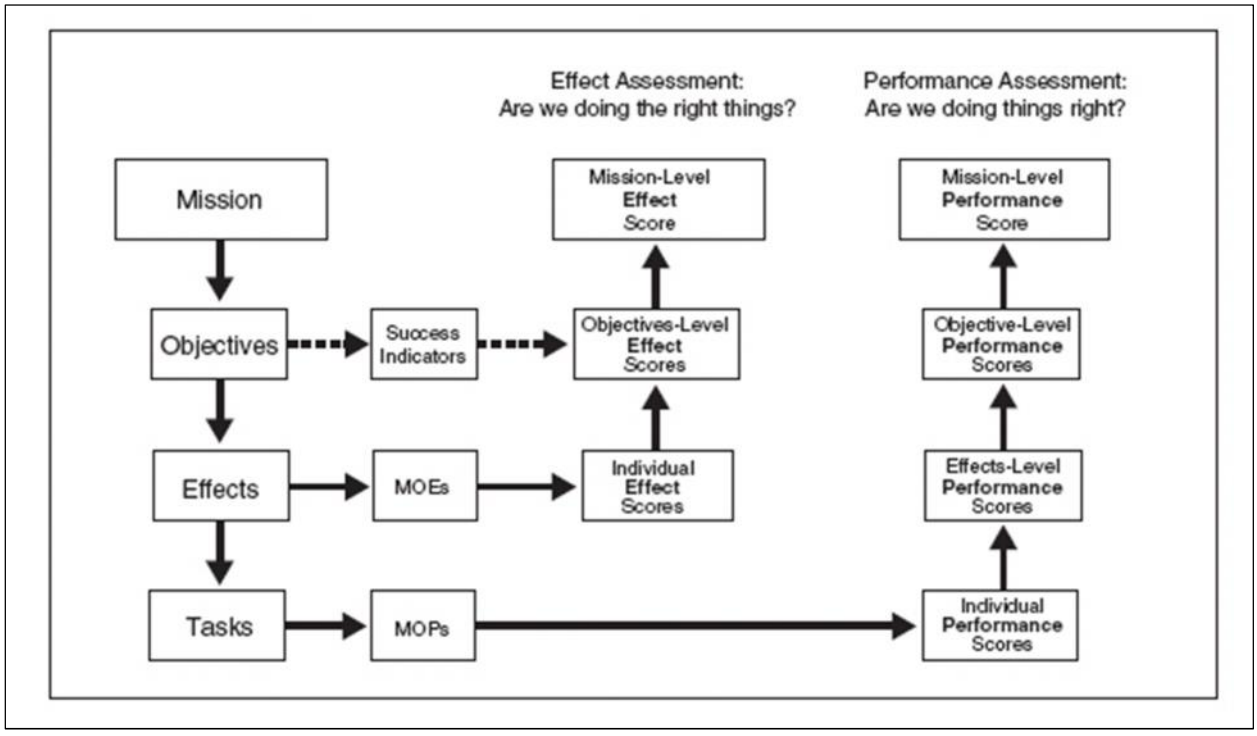


Figure 10: Effects Based assessment methodology

As an example of the scoring models, Figure 11 illustrates the approach that would be used in

satisfying an objective of "Preventing Unauthorized Access" of a system.

The resulting MOP and MOE values are then used within the Heuristic model to establish the benefit

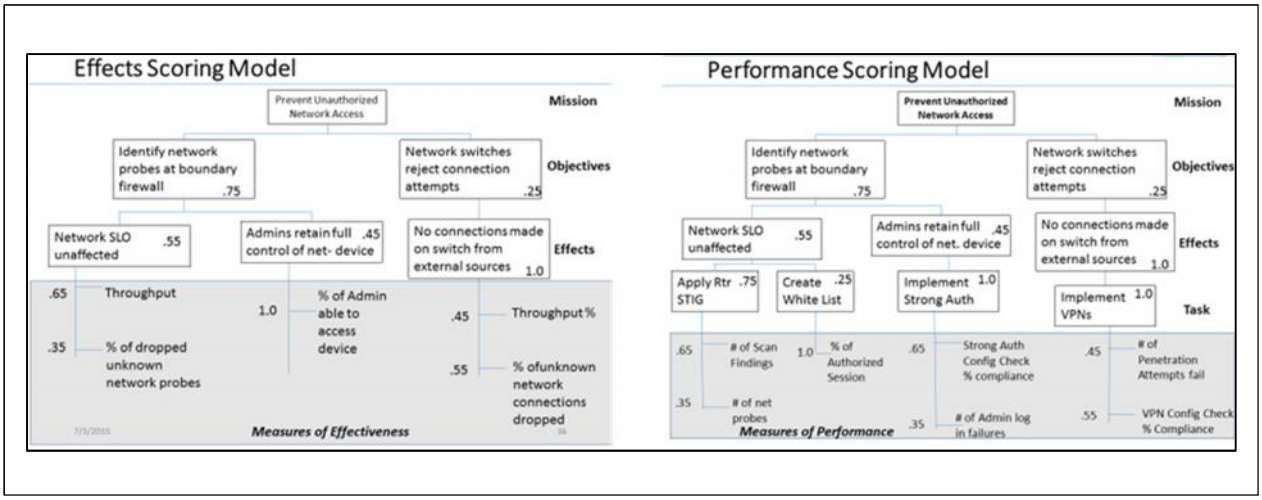


Figure 11: Effects Scoring and performance scoring models

to the overall system as illustrated in Figure 8.

During the course of this investigation, various government bodies and support organizations were contacted to understand what efforts they had underway that may be helpful in addressing the TOR. The most promising activity is the study by the Rand Corporation with co-sponsorship by Juniper Corporation.[17] The study was an attempt to address the need to more efficiently and cost effectively manage the cyber security risks that posed an impact to their business. The research used to drive the study paralleled those in DoD. Specifically, the findings indicated that in spite of increasing levels of cyber security spending, there was not a corresponding increase in the belief that exposure to cyber security risk was being lessened. Based upon this, Juniper and Rand Corporation concluded that the issue was a lack of quantitative data that CISOs could rely on to make informed decisions on the cyber investments being made. In response, Rand Corporation developed a heuristic economic model that correlates the major attributes and decisions that drive the cost of cyber risk within an organization. The model is defined in the paper "The Defender's Dilemma"[18] and includes the cost of security tools, resources, threats, and the projected cost of a cyber-attack resulting in the loss of data.

The model has shown considerable promise and has resulted in Rand Corporation receiving additional tasking by the Air Force and others to pursue more sophisticated and refined approaches. The concept of cyber risk modeling is not new but until now has not received the attention it should. Through the work of Rand Corporation, all indications are that utilizing modeling as a means of predicting the cost of cyber-attacks and how specific investments may influence that cost continues

[17] L. Ablon, M.C. Libicki, and A.A. Golay. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*. Santa Monica, CA: RAND Corporation, 2014. Available at http://www.rand.org/pubs/research_reports/RR610.html.

[18] M.C. Libicki, L. Ablon, and T. Webb. *The Defender's Dilemma: Charting a Course Toward Cybersecurity*. 2015.

to mature and should be strongly considered by DoD as a tool for improving cyber investment decision making.

Recommendation 6

DoD should expand the resources available to the ODASD(C3CB), in conjunction with the Modeling and Simulation Coordination Office (M&SCO) under the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)), to continue and expand the cyber investment modeling work to include financial, heuristic, and effects based assessment models. ODASD(C3CB) and M&SCO should lead an Executive Steering Committee to serve as the coordination body for DoD throughout a multiphased approach to developing a single model to inform DoD cyber investments, with a particular focus on warfighting systems.

The Executive Steering Committee should develop and mature cyber investment modeling capabilities over the next two years, to include:

- Financial Model with a goal to record, examine, and improve how cyber investment dollars are used within DoD
- Heuristic Model with a goal to identify and understand the key factors affecting cyber investment decisions in terms of the inter-relatedness of organizations, systems, and the tools and products used
- Effects Based Model with a goal to analyze cyber investments and their resulting impact on a system's cyber defense posture, cyber resilience, and mission effectiveness relative to cost

During this development, the Executive Steering Committee should explore how it can make use of existing partial models that have been developed by RAND, Lockheed Martin, Goldman Sachs, and the Australian Signals Directorate.

A multi-phase approach is recommended to leverage the above models in order to create a single model to enable DoD decision makers to choose the most appropriate and cost-effective cyber defense investments. The use of models and simulations has become a key tool for improving and refining the methods and techniques used on a broad variety of DoD missions. Applying modeling and simulation to the cyber risk investment decision process would closely approximate the methods and techniques used by insurance firms when choosing whether to issue coverage or not. While cyber risk investment and assessment modeling is a developing field of expertise with similar complexities found in the data sciences domain, it provides a very pragmatic and scientific method for solving the cyber investment decision problem. More importantly, it provides an opportunity for experimentation and exploration of alternatives while not requiring the actual investment in resources and materials required by traditional try and buy approaches.

Phase 1 – Planning and Coordination

The objectives of the planning and coordination phase is to define the appropriate metrics for the three previously identified models: financial, heuristic, and effects based operation models. The risk management framework (RMF) now being used by DoD includes various metrics and measures for determining the security postures of a system. These measures as part of this phase must be reviewed and likely refined to more accurately target the goals and objectives of the model. Once completed,

these measures should be included within the RMF to ensure standardization across the department. The planning and coordination phase will establish a framework by developing consistent and standard definitions of the key metrics for quantifying actions and results. These metrics provide guidance on the input, output, and interfaces required to ensure the models accurately reflect DoD's missions and systems that are selected for inclusion. As part of the definition activity, the following driving factors should be examined and documented:

- Department Priorities
  - Mapping of DoD priorities to programs and their ranking relative to national objectives
- Program inter-relationships
  - Targeted investments can have broad impact across other department programs
- Cost Factors
  - Cost of implementing a cyber defense capability
  - Cost impact of implementing the capability
- Cyber Defense Uncertainties
  - Continuing evolution of threats & vulnerabilities
  - Shifting motivation of attackers
  - Cost implications of successful penetrations
  - DoD's increasing and changing use of information technology

In this phase, create a working group that includes members from ODASD(C3CB), Rand, MITRE and others. This working group will be responsible for creating DoD Cyber Investment Framework. The working group should report to the Executive Committee on a quarterly basis and the ODASD (C3CB) leadership monthly to ensure the tasking remains aligned with the overall goals and objectives.

The working group will also explore how it may use existing partial "models" that have been developed by the Rand Corporation, Lockheed Martin, Goldman Sachs, the Australian Signals Directorate, and others.

Phase 2 – Pilot Model Creation

The objective of Phase 2 is to build a pilot model. To accomplish this a model development team will be assembled. This team will work closely with the Phase 1 working group and report to ODASD(C3CB). The Phase 1 Working group will act as a liaison between the development team and the leadership. The following tasks are accomplished in this phase:

- Broaden and expand modeling activity to include system criticality, resiliency, and interdependence in driving cyber investment decisions of operational war fighting systems.
- DoD should expand upon OSD/ATL/DASD(C3CB) cyber investment modeling work to include financial, heuristic, and effects based assessment optimization models to inform DoD cyber investments, with particular focus on war fighting systems.

- Financial Modeling: Capture, analyze, and optimize how cyber investment dollars are distributed and used within DoD
- Heuristic Modeling: Identify and understand the key factors affecting cyber investment decisions in terms of the interrelatedness of organizations, systems, and the tools and products used
- Effects Based Modeling: Provides the means to analyze cyber investments and their resulting impact on a system's cyber defense posture, cyber resilience, and mission effectiveness relative to cost

- Task M&SCO within ASD(R&E) to develop and mature cyber investment modeling capabilities
- Formally and mathematically define the relationship between DoD's Cyber Investments and Cyber Resilience Posture (TOR Task #3)
- Create a model driven by DoD System Resilience measurements and from which prioritized recommendations for the "next dollar spent" are generated for maximum effects against cyber threats (TOR Task #4)

Phase 3 – Model Validation

The objective of Phase 3 is to validate the pilot model from Phase 2. At this time the pilot model will be tested against previous decisions to determine how well the model can track previous successful investments. In addition, the model will be used on a sampling of upcoming acquisitions and system upgrades. The results should be compared to those of an independent team to understand the differences, if any, between the model and the team.

Subsequent use of the model will require the assignment of the model to the appropriate budgeting organization, likely ODASD (C3CB). The goal upon completing validation and allocating the tool to an organization will be to follow and track the results so as to generate recommended refinements and to tune the underlying data model. Additionally, close association between the model's developers and the organizations defining metric collection must continue to ensure the right data continues to be collected as systems mature and as the cyber threat and cyber investment landscape evolves.

Chapter 7: Work with COTS Suppliers That Place High Value on the Security of Their Products

The Department of Defense buys large amounts of enterprise software and hardware. This reliance on commercial-off-the-shelf (COTS) products means that DoD systems inherit vulnerabilities that the commercial market place has been willing to tolerate. Most cyber defense measures—in place and proposed—focus on reacting to discovered vulnerabilities and thwarting would-be attackers. The very best cyber defense measures would be those that prevent the acquisition and fielding of highly vulnerable capabilities in the first place.

Diligence is required to acquire those capabilities, and only those capabilities, that are essential to the mission and implemented in a way that minimizes vulnerabilities. Every capability entails some level of vulnerability, particularly when the capability is partly instantiated in software. Good cyber defense measures are intended to assure that the acquisition and fielding of military capabilities have minimal vulnerabilities.

Some vendors are improving the security of their COTS software. As DoD improves its cyber hygiene and incorporates more disciplined IT administration processes, DoD can make known to vendors what processes, software tools, software features, and levels of cyber security are required. Doing so would not be overly costly. Even though DoD is not the dominant customer for most vendors, it can help shape the commercial marketplace to improve cyber security by expressing its need for better security in COTS products.

DoD IT leaders can express these needs in open settings such as the Software Assurance Forums sponsored by NIST, as well as websites such as the NIST discussion site for Security Content Automation Protocol. DoD can be a leader for better cyber security and defense among government agencies, making it a stronger customer voice in a large, noisy market.

Recommendation 7

USD(AT&L), in coordination with the DoD CIO and CISO, should help shape the commercial marketplace to deliver better cyber security by becoming a more demanding buyer.

For competitive purposes, commercial vendors tend to bundle capabilities into set products. This makes it difficult to buy only the minimum essential capabilities needed by the DoD program. The DoD CIO and CISO, on behalf of DoD, should open a dialogue with vendors as to how buyers can disable unnecessary capabilities. This should also be coordinated with other government agencies to develop a government-wide effort to shape the marketplace.

Actions for becoming a more demanding buyer include:

- USD(AT&L) should favor vendors with strong software development practices and track record of conscientiously fixing vulnerabilities
- The DoD CIO and CISO should specify the use of open standards for security automation

- The DoD CIO in conjunction with the Joint Requirements Oversight Council (JROC) should require that newly acquired software run on a standard secure configuration
- The DoD CISO should work with vendors to build marketplace awareness and demand for cyber-resilient hardware and software
- The DoD CIO should coordinate with CIOs from other government agencies, in particular DHS, to make such conditions part of their future purchases and developments.

Exposing vulnerabilities in complex systems and acknowledging the capabilities that engender those vulnerabilities requires a level of skill that is not currently resident in DoD. The DoD CIO and CISO, in coordination with USD(AT&L), should take immediate steps to develop these skills and augment current staffing in order to support making DoD a more demanding buyer. This can be done through personnel exchanges with NSA and USCYBERCOM, through FFRDC exchanges, and involvement with other outside entities. Clear incentives will be needed to attract real experts in this area. Resources should be provided, as required, to assist in this skill development.

For both traditional programs of record and COTS programs, the onus in on the requirements process to ensure there is adequate cyber security. The DoD CIO and CISO have a presence in the process up to and including JROC deliberations. Their involvement in this process will support minimizing cyber vulnerabilities as a normal aspect of every Program of Record (POR). This process is easier begun with a new POR rather than immediately grafting it onto current programs. Therefore, the DoD CIO and CISO should seek to embed this process of fine-grained cyber-risk management into a target POR. The suggested candidate program is the "next generation bomber" because it is a mission critical system.

Identifying the specific, as well as types of, system capabilities that are most likely to introduce cyber vulnerabilities or otherwise increase the cyber attack surface in a system will improve the overall cyber safe acquisition process. Research should be sponsored by USD(AT&L) and the DoD CIO and CISO, both within and outside of DoD, to better understand the inter-relationships between system capabilities and their vulnerabilities. This research will support DoD's efforts in becoming a more demanding buyer.

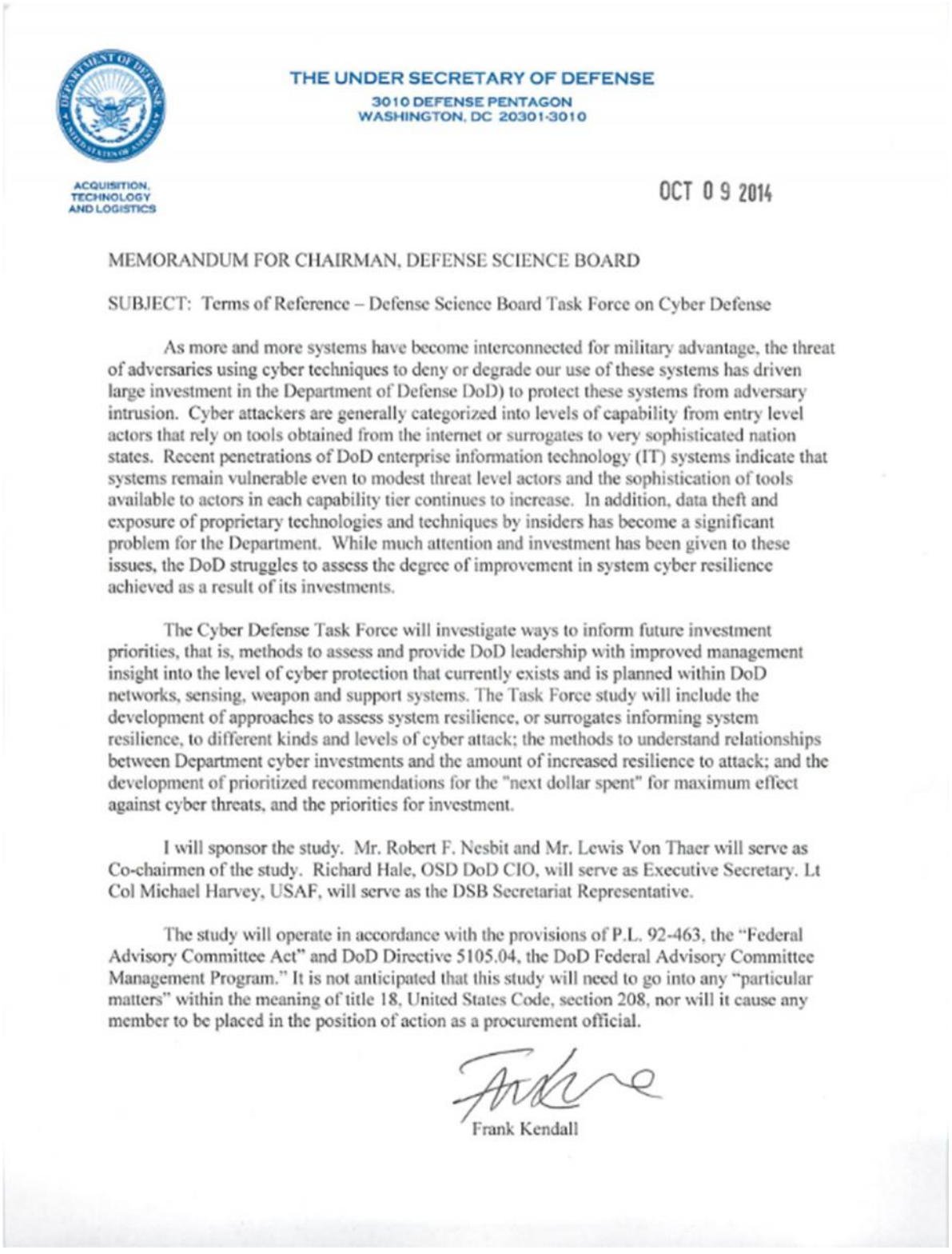
Acronym List

AFATDS	Advanced Field Artillery Tactical Data System
AFCEA	Armed Forces Communications and Electronics Association
ASD	Australian Signals Directorate
ASD(R&E)	Assistant Secretary of Defense for Research and Engineering
ASOC	Air Support Operations Center
AWACS	Airborne Warning and Control System
BCT	brigade combat team
BMD	Ballistic Missile Defense
BN	battalion
C&A	certification and accreditation
C2	command and control
C4ISR	command, control, communications, computers, intelligence, surveillance and reconnaissance
CASS	Close Air Support System
CCDRs	Combatant Commanders
CCMDs	Combatant Commands
CIO	chief information officer
CISO	chief information security officer
CJCS	Chief of the Joint Chiefs of Staff
COTS	commercial-off-the-shelf
CSG	carrier strike group
DARPA	Defense Advanced Research Projects Agency
DEPSECDEF	Deputy Secretary of Defense
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DIV	division
DoD	Department of Defense
DRRS	Defense Readiness Reporting System
DSB	Defense Science Board
EBO	effects-based operations
EOT	executive oversight team
FFRDCs	Federally Funded Research and Development Centers
FSE	fire support element
FY	fiscal year
GIAC	global information assurance certification
HBSS	host based security system
IC	intelligence community
ISR	intelligence, surveillance and reconnaissance
IT	information technology
JCAS	Joint Close Air Support
JCS	Joint Chiefs of Staff
JROC	Joint Requirements Oversight Council
JTAC	Joint Tactical Air Controller
JWICS	Joint Worldwide Intelligence Communications System

ACRONYM LIST

Link 16	Tactical Data Exchange Network
M&SCO	Modeling and Simulation Coordination Office
METs	mission essential tasks
MOEs	measures of effectiveness
MOPs	measures of performance
MS&A	modeling, simulation and analysis
NIPRnet	Non-secure Internet Protocol Router NETwork
NIST	National Institute of Standards and Technology
NSA	National Security Agency
ODASD(C3CB)	Office of the Deputy Assistant Secretary of Defense for Command, Control, And Communication (C3), Cyber, and Business Systems (C3CB)
OODA	observe, orient, decide and act
OPLANs	operational plans
OSD	Office of the Secretary of Defense
PACFLT	U.S. Pacific Fleet
PMs	program managers
POR	program of record
RAMBO	Resilient Architectures for Mission Assurance and Business Objectives (a MITRE Corporation project)
RMF	risk management framework
SECDEF	Secretary of Defense
SIPRnet	Secret Internet Protocol Router Network
TACP	tactical air control party
TBMCS	Theater Battle Management Core System
TOR	terms of reference
USCYBERCOM	United States Cyber Command
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics
USD(P)	Under Secretary of Defense for Policy
USPACOM	United States Pacific Command

Terms of Reference



THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION, TECHNOLOGY AND LOGISTICS

OCT 09 2014

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board Task Force on Cyber Defense

As more and more systems have become interconnected for military advantage, the threat of adversaries using cyber techniques to deny or degrade our use of these systems has driven large investment in the Department of Defense DoD) to protect these systems from adversary intrusion. Cyber attackers are generally categorized into levels of capability from entry level actors that rely on tools obtained from the internet or surrogates to very sophisticated nation states. Recent penetrations of DoD enterprise information technology (IT) systems indicate that systems remain vulnerable even to modest threat level actors and the sophistication of tools available to actors in each capability tier continues to increase. In addition, data theft and exposure of proprietary technologies and techniques by insiders has become a significant problem for the Department. While much attention and investment has been given to these issues, the DoD struggles to assess the degree of improvement in system cyber resilience achieved as a result of its investments.

The Cyber Defense Task Force will investigate ways to inform future investment priorities, that is, methods to assess and provide DoD leadership with improved management insight into the level of cyber protection that currently exists and is planned within DoD networks, sensing, weapon and support systems. The Task Force study will include the development of approaches to assess system resilience, or surrogates informing system resilience, to different kinds and levels of cyber attack; the methods to understand relationships between Department cyber investments and the amount of increased resilience to attack; and the development of prioritized recommendations for the "next dollar spent" for maximum effect against cyber threats, and the priorities for investment.

I will sponsor the study. Mr. Robert F. Nesbit and Mr. Lewis Von Thaer will serve as Co-chairmen of the study. Richard Hale, OSD DoD CIO, will serve as Executive Secretary. Lt Col Michael Harvey, USAF, will serve as the DSB Secretariat Representative.

The study will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act" and DoD Directive 5105.04, the DoD Federal Advisory Committee Management Program." It is not anticipated that this study will need to go into any "particular matters" within the meaning of title 18, United States Code, section 208, nor will it cause any member to be placed in the position of action as a procurement official.

Frank Kendall

Study Membership

Study Chairs

Mr. Robert Nesbit	Private Consultant
Mr. Lewis Von Thaer	DynCorp International

Executive Secretary

Mr. Richard Hale	DoD CIO
Ms. Jenine Patterson	DoD CIO

Members

Mr. Christopher W. Day	Packet Forensics
Ms. Lynn A. Dugle	Private Consultant
Mr. Page Hoeper	Private Consultant
Dr. Rich Ivanetich	Institute for Defense Analyses
Dr. Anita K. Jones	University of Virginia
Dr. Paul Kaminski	Technovation, Inc
Dr. Ronald L. Kerber	Private Consultant
Dr. John L. Manferdelli	Google
Dr. Joseph Markowitz	Private Consultant
Maj Gen Paul D. Nielsen (Ret.)	Software Engineering Institute, Carnegie Mellon University
Mr. Tony Sager	Council on CyberSecurity
Mr. Steve Schmidt	Amazon Web Services
Mr. Daniel Teijido	Raytheon Company

Defense Science Board

Lt Col Michael Harvey	Deputy for Operations, U.S. Air Force
Mr. David Jakubek	Executive Director, DSB Office (through December 2015)
Lt Col Victor Osweiler	Deputy for Operations, U.S. Air Force
Mr. Robert Ramsey, III	Executive Director, DSB Office

Observer

Mr. Paul Balek	MITRE

Staff

Ms. Erin Erickson	Strategic Analysis, Inc.
Dr. Toni Marechaux	Strategic Analysis, Inc.
Mr. Michael Rauseo	Redhorse Corporation
Ms. Stephanie Simonich	Redhorse Corporation
Mr. Ted Stump	Redhorse Corporation

Briefings to the Task Force

January 28-29, 2015

DoD CIO Overview and Priorities
Mr. Terry Halvorsen, Acting DoD Chief Information Officer (CIO)

Threat Environment
National Security Agency

DoD Cybersecurity Policy
Mr. Dominic Cussatt, Director Cybersecurity Policy, Strategy, and Workforce, Office of the Deputy CIO for Cybersecurity

Implementation of Policy
Mr. Mitchell Komaroff, Director, Cybersecurity Implementation & Acquisition Integration, Office of the DoD CIO

The Role of the Principal Cyber Advisor and Focus Areas for the New Cyber Strategy
Jonathan Reiber, Special Assistant in the USDP Cyber Office

Joint Staff Perspective on Cybersecurity
LTG Mark Bowman, Director, Command, Control, Communications and Computers/Cyber, J6

March 3-4, 2015

USCYBERCOM Welcome
Maj Keffer, USCYBERCOM Chief of Staff

Cyber Portfolio Management Decisions
Mr. Terry Carter, Deputy Director, Capabilities and Resource Integration, USCYBERCOM (J8)

Operational Cyber Risk Management Decisions
Brig Gen Robert Skinner, USAF, Joint Task Force, Department of Defense Information Network (DODIN)

Joint Enterprise Risk Assessment Model (JRAM)
RADM Michael Gilday, USN, Director, Operations (J3), USCYBERCOM

Cyber National Mission Forces (CNMF)
Mr. Charles Berlin, Deputy Commander, Cyber National Mission Forces

U.S. Fleet Cyber Command/U.S. TENTH Fleet Discussion
VADM Jan Tighe, USN, Commander, U.S. Fleet Cyber Command & Commander, U.S. 10th Fleet

Cyber Awareness
Col Scott Lathrop, Deputy Director Advanced Concepts and Technologies (J9), USCYBERCOM

JHU/APL Discussion
Ms. Christine Fox, Assistant Director for Policy and Analysis, JHU/APL

Directorate Discussions
ADM Michael Rogers, Commander, USCYBERCOM & Director, NSA
Lt Gen James K. McLaughlin, Deputy Commander, USCYBERCOM

Cyber Task Force
National Security Agency

NTOC Discussions
National Security Agency

CH TAO Discussions

National Security Agency

Director, Information Assurance Directorate

National Security Agency

March 31-April 1, 2015

Cybersecurity Resiliency and Regeneration: Leveraging Automation & Integration

Phil Quade, Director, Cyber Task Force, National Security Agency

EY Cyber Economic Risk Insights: Executive Overview Of Cyber-Assisted Economic Campaign And Mitigation Recommendations

Brandon Ahrens, Cybersecurity Lead, Ernst & Young Federal Practice

Jeff Johnson, Executive Director, Cyber Economics Lead

Corporate Information Security Overview for State Street Corporation

Mark Morrison, Senior Vice President & Chief Information Security Officer, State Street Corporation

Amazon Web Services Security

Steve Schmidt, Vice President and Chief Information Security Officer, Amazon Web Services

USAA

Bill Wright, Executive Director/Technical Fellow, USAA

Intelligence Risk Driven Cybersecurity Investment

Byron Collie, VP, Technology Fellow, Director of Cyber Intelligence

Cyber Investment Management Board

Adam Nucci, Associate Director for Cyber Capability & Resource Analysis Office, Deputy Assistant Secretary of Defense, C3 Cyber and Business Systems

Raytheon Cyber Investment Strategy

Jeff Brown, Vice President and CISO, Raytheon Company

Investment Scenarios

Richard Hale & Jenine Patterson, DoD CIO Office

May 5-6, 2015

Intelligence Driven Defense: Managing Cyber Security Risk

Scott Rush, Director Enablement, Corporate Information Security, Enterprise Business Services, Lockheed Martin Corporation

MITRE Cyber Investments

Gary Gagnon, Senior Vice President, Chief Security Officer and Corporate Director, Cybersecurity

Efficient Management of Cyber Risk

John Watters, Founder, Chairman & CEO of iSIGHT Partners

Economics of Cyber Security: Guidelines for Making Investment Decisions

John Gilligan, Present and COO, Schafer Corporation

June 2-3, 2015

Task Force Cyber Awakening

Mr. Matthew Swartz, Director, Task Force Cyber Awakening

July 7-8, 2015

NIM for Cyber Briefing

Mr. Jim Richberg, Office of the Director of National Intelligence

LIST OF MEETINGS AND BRIEFERS

APL Threat Effort

Mr. Mitch Komaroff, Director, Cybersecurity Implementation and Acquisition Integration, Office of the DoD CIO

Readiness Reporting

Mr. Michael Skelly, Deputy Director, DRRS Implementation Office, Readiness Directorate, Office of the Secretary of Defense for Personnel & Readiness

USPACOM SVTC

Mr. Randy Cieslak, Chief Information Officer, USPACOM

Mr. Bob Stephenson, Technical Director for Fleet Readiness, Space and Naval Warfare Systems Command

Appendix

Department of Defense Cyber Security Update

Executive Summary

Report #1
September 2015

This report is intended for consumption by the DoD's executive leadership*. Its purpose is to

1. Describe current and projected cyber threats
2. Assess the performance of the various defensive subsystems against actual attacks
3. Measure the DoD networks with regard to basic cyber hygiene
4. Enumerate the top risks currently being assumed by the Department

The report is designed to inform, stimulate discussion, serve as a forcing function for improvements and provide a more fully informed basis for investment decisions in cyber security.

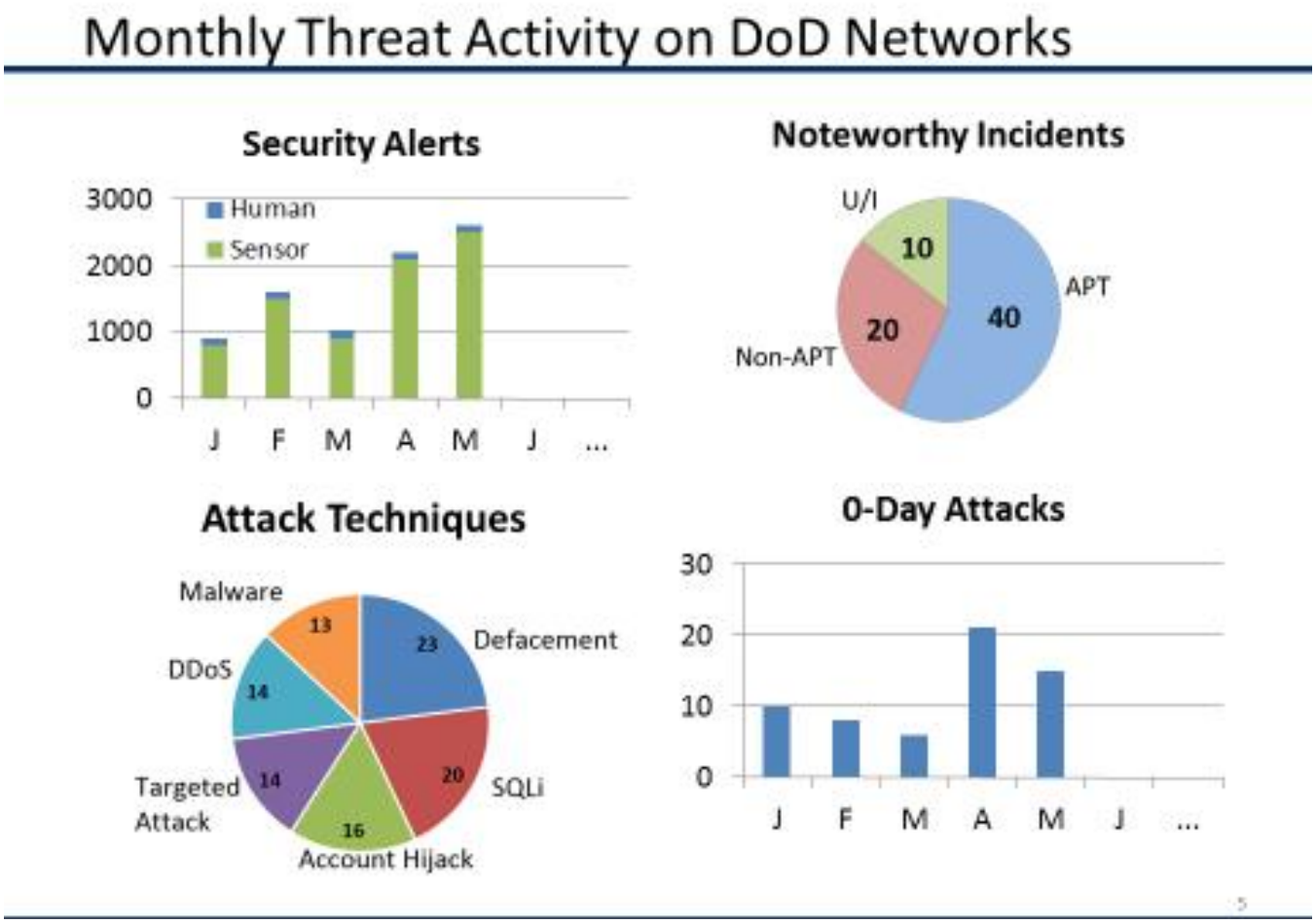
*This is an executive summary. The Department's CIOs, CSOs and network administrators require considerably more detailed information

MONTHLY THREAT SUMMARY

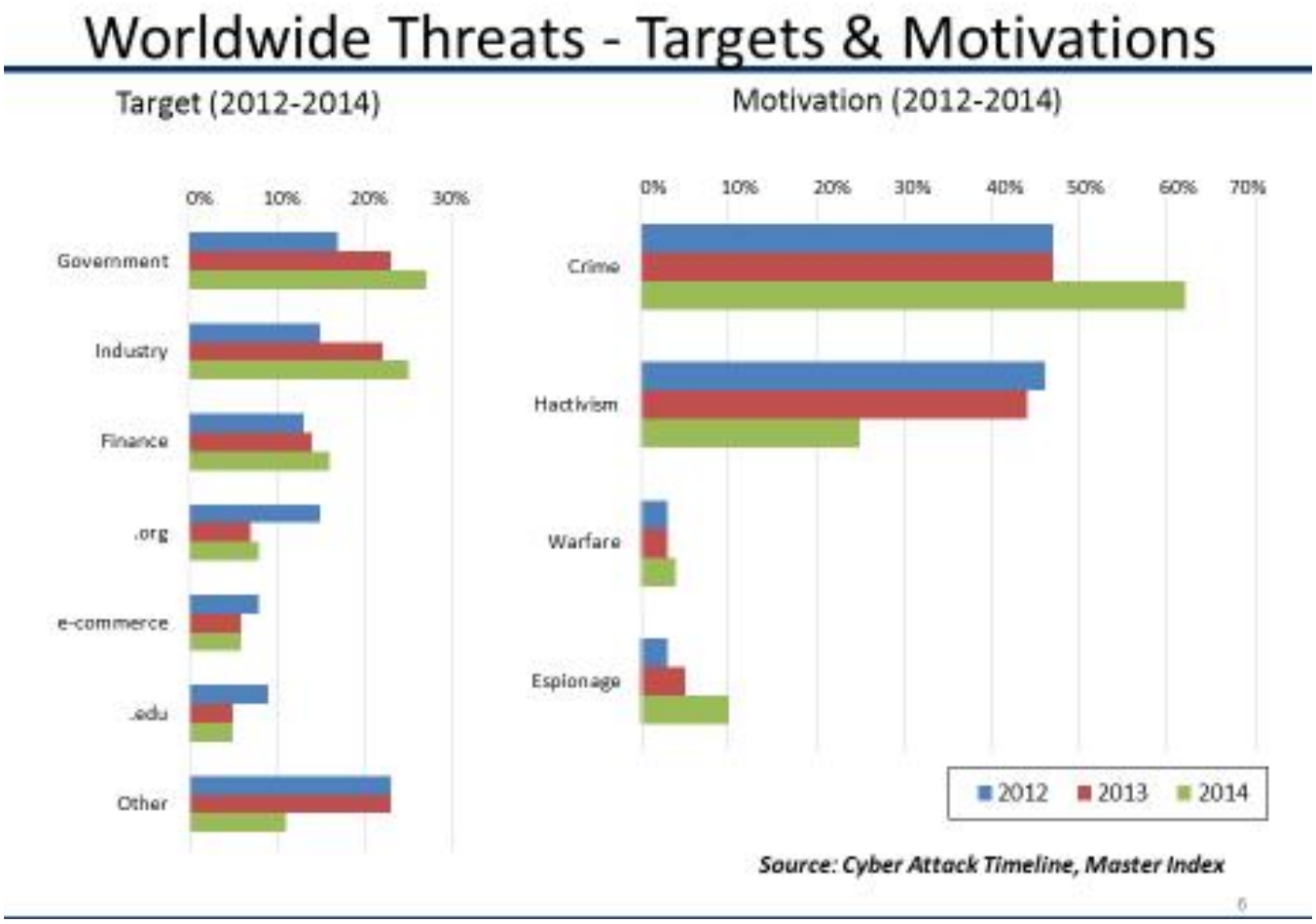
Significant Intrusions

Ref.	Date	Author	Target	Description	Attack	Target Category	Attack Category	Country
1	9/3	Team Dead Dream	Picatinny Arsenal	Saudi Hackers from Team Bad Dream deface the official website of the US Army Picatinny Arsenal (pica.army.mil).	Defacement	Military	CC	US
2	9/7	?		The Defense Contract Management Agency (DCMA) the US federal government entity responsible for performing contract administration services for the DoD is victim of a suspected cybersecurity breach pulls a number of its servers offline.	Unknown	Government	CC	US
3	9/8		N	The CyberCaliphate hacks the Newsweek Twitter Account (@ newsweek) and threatens US President Barack Obama.	Account Hyjacking	News	H	US
4	9/12	CODOSO (APT Group)	Forbes	Invincea reveals that a Chinese APT group called Codoso compromised. Forbes.com in late 11/2014. It set up a watering hole style web-based drive-by attack against the US Defense and Financial Services.	Targeted Attack	Defense Contractor Financial Services	CE	US
5	9/17			Security researchers from Insight Partner claim to have uncovered a three-year-old internet espionage campaign targeting military personnel, diplomats, and defense contractors in the US, UK and Israel. The campaign, using fake social media profiles, has affected over 2,000 individuals.	Social Network Poisoning	News	CE	US, IL, UK
6	9/23			The pro-Russian hacktivist Cyber Perkus leaks several documents allegedly hacked from the mobile device of a Green Group Defense Services official, who recently visited Kiev as a member of an American military delegation	Unknown	Industry Defense Services	H	US
7	9/27			The Twitter and YouTube accounts for the US military command that oversees operations in the Middle East (CENTCOM) are hacked by the cyber Caliphate. Several maps and diagrams are also posted by the attackers, despite CENTOM states that no sensitive information has been compromised.	Account Hyjacking	Military	CW	US

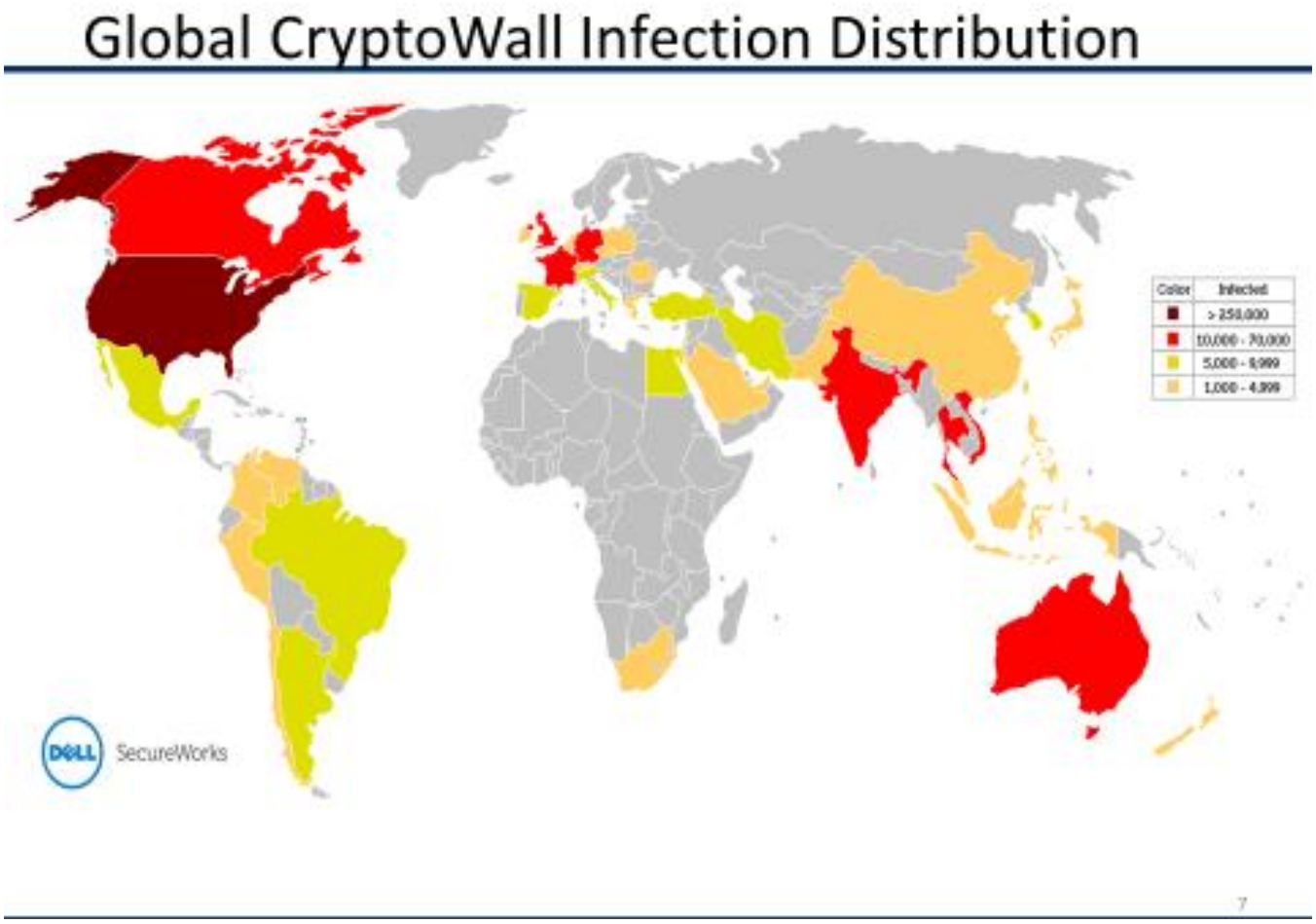
Note - This attack timeline is for example purposes only, ref Hackmageddon.com.



Note – For example purposes only, ref. Hackmageddon.com.

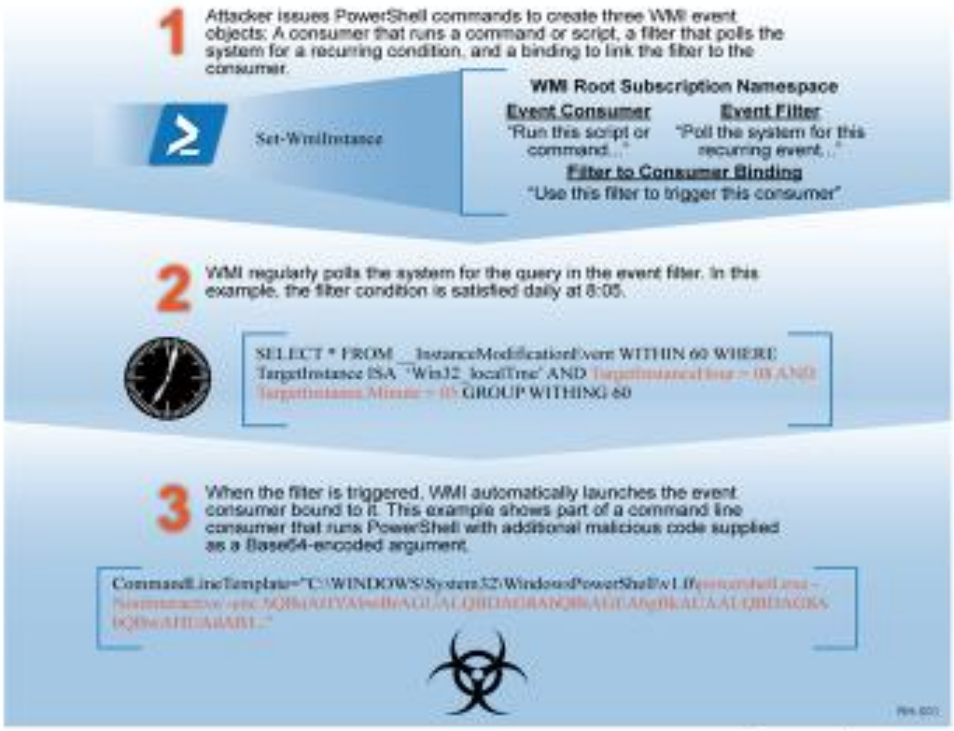


Note – For example purposes only, ref Hackmageddon.com.



Note – Example of a trend in which the attacker enters a system and encrypts the files, then charges the owner a ransom to decrypt.

Dangerous Threat Trends - Using WMI* to Deploy Covert Malware

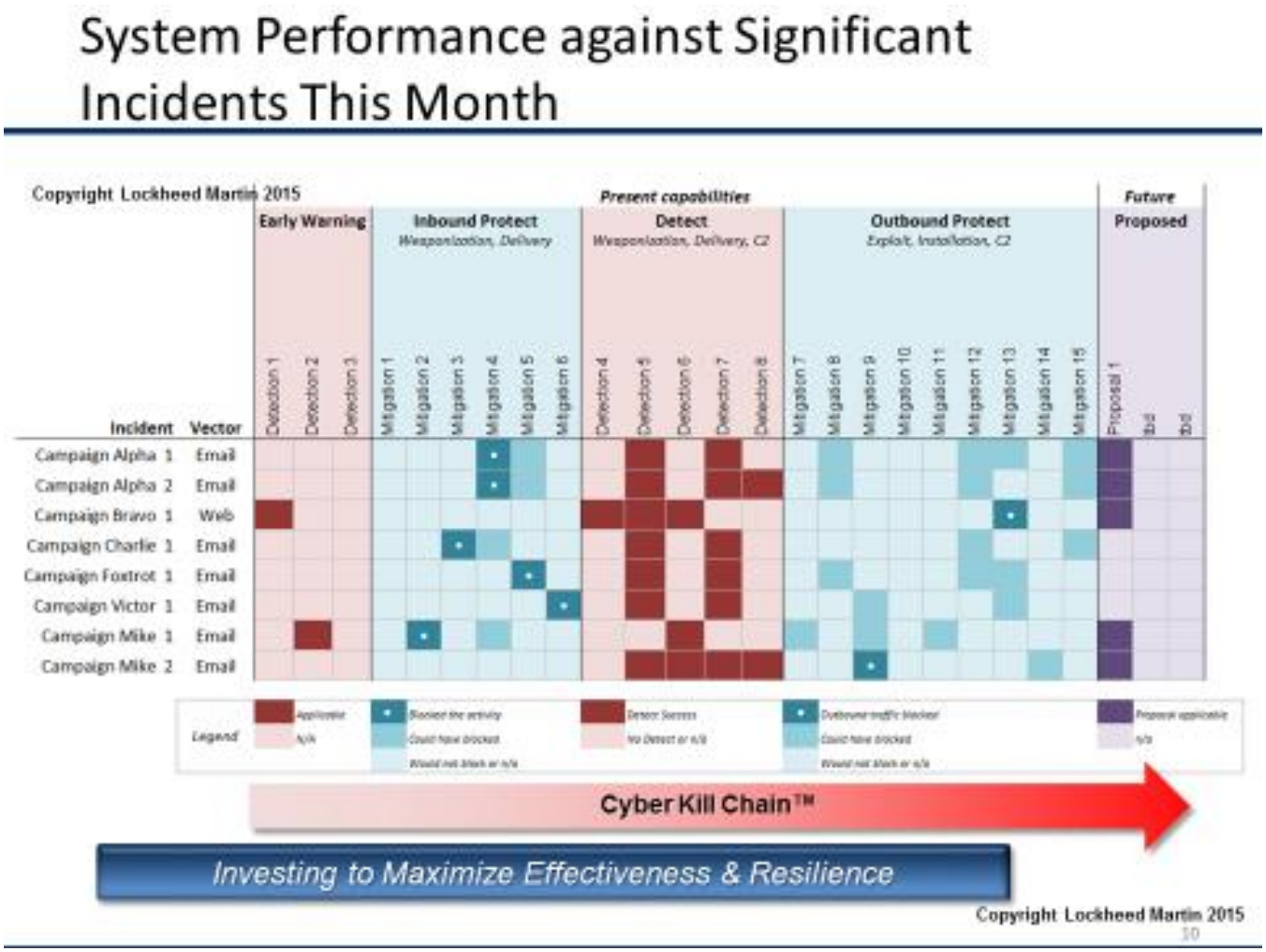


*WMI – Windows Management Instrumentation

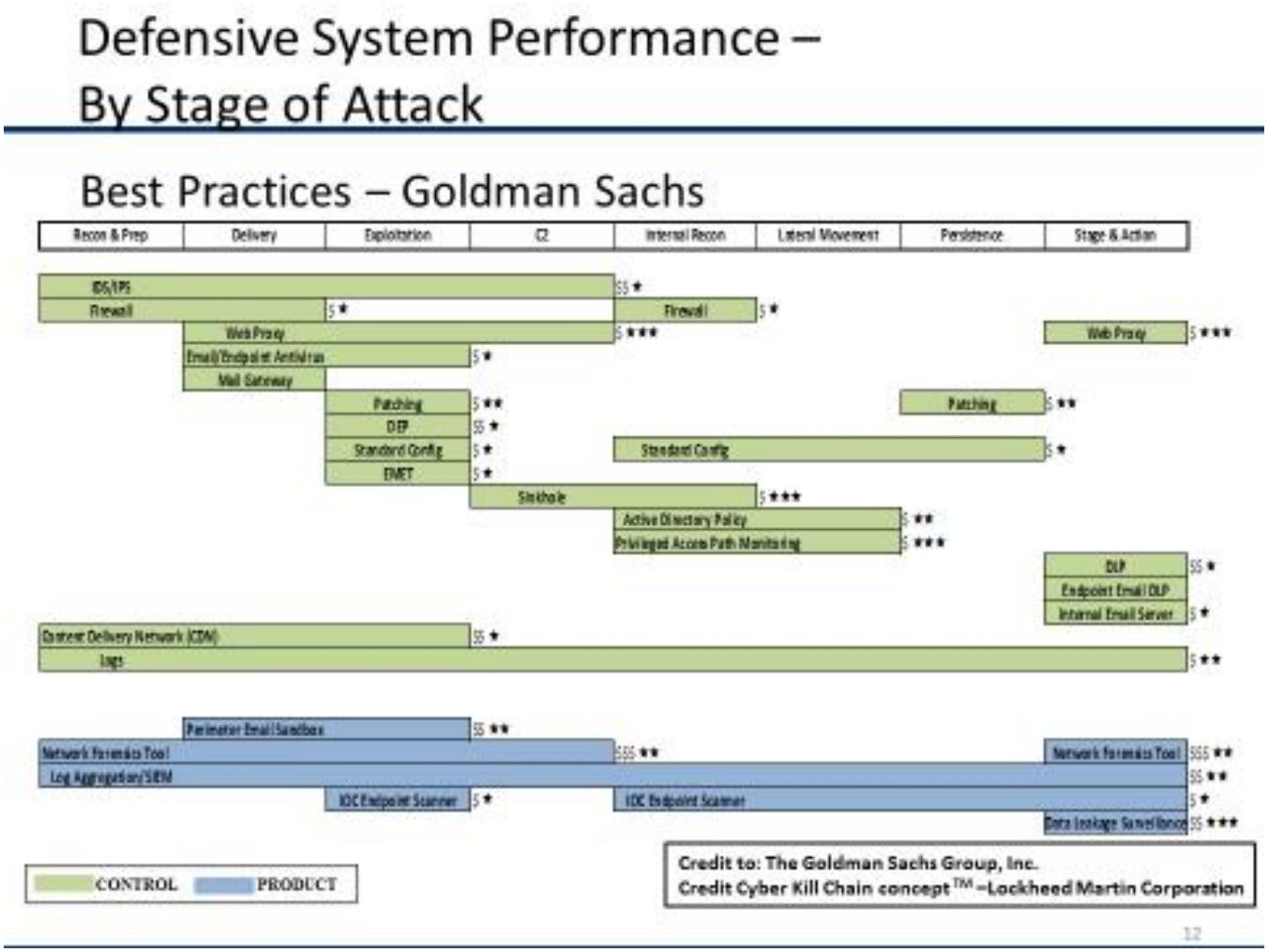
Ref: Mandiant Trends - 2015

APPENDIX

DEFENSIVE SYSTEM PERFORMANCE AGAINST SIGNIFICANT ATTACKS



Note – This shows actual attacks during the reporting month and how each of the defensive systems performed, whether it detected the attack or not or whether it stopped or would have stopped the attack. It also shows how proposed defenses would have performed so you can see if it might be worth adding to the defensive portfolio.



Note – This shows how the company's defenses are aligned by phase of the attack. It allows you to see where there is defense in depth and where the defenses may be thin. It also looks at the cost of acquiring and operating the defensive system ($ thru $$$) and the performance of that system (* thru ***).

NETWORK HYGIENE METRICS

Use Attack Data to Rank Security Controls(1)

Ref : Australian Signals Directorate, 2015

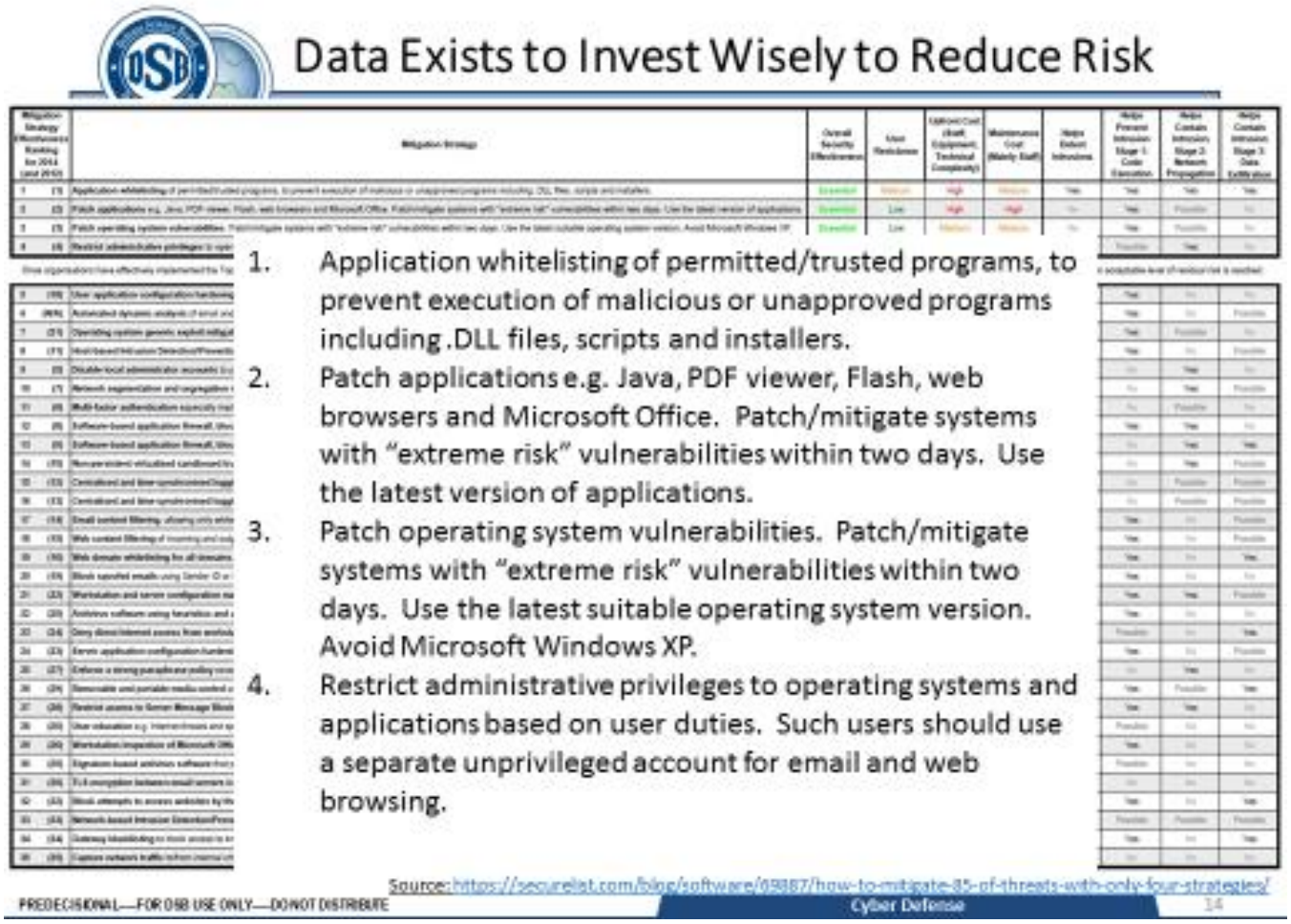
Effectiveness Rank	Mitigation Strategy	Overall Effectiveness	User Resistance	Upfront Cost	Maintenance Cost
1	Whitelist permitted/trusted programs	Essential	Medium	High	Medium
2	Patch application software	Essential	Low	High	High
3	Patch operating system software	Essential	Low	Medium	Medium
4	Severely restrict administrative privileges	Essential	Medium	Medium	Low
Once organizations have effectively implemented the Top4 mitigation strategies, firstly on workstations of users who are most likely to be targeted by cyber intrusions and then on all workstations and servers, mitigation strategies can be can then be selected to address security gaps until an acceptable level of residual risk is reached.					
5	Harden user application configurations	Excellent	Medium	Medium	Medium
6	Analyze email and web content in a sandbox	Excellent	Low	Medium	Low
7	Mitigate OS generic exploits	Excellent	Low	Medium	Low
8	Identify anomalous behavior with host based IDS	Excellent	Low	Medium	Medium
9	Disable local admin accounts	Excellent	Low	Medium	Low
10	Segment and segregate the network	Excellent	Low	High	Medium
11	Employ multi-factor user authentication	Excellent	Medium	High	Medium
12	Apply firewall to block incoming malware	Excellent	Low	Medium	Medium
13	Apply firewall to block outgoing malware	Excellent	Medium	Medium	Medium
14	Host virtual sandbox outside internal network	Excellent	High	High	Medium
15	Log successful and failed computer events	Excellent	Low	High	High
16	Log allowed and blocked network activity	Excellent	Low	High	High

13

Note - There are hundreds of different security controls that have been recommended for use. This analysis performed by the Australian Signals Directorate ranks the top 35 controls in terms of how they performed during a year of attacks. Note that the performance falls off rather quickly, and in fact they claim that the failure or absence of the top four controls resulted in 85 percent of the successful attacks.

Note – The Task Force suggests that the leadership give priority attention to the top four controls, ensuring they are implemented and updated to the maximum extent possible across DoD networks. The following R/Y/G charts show metrics for these controls.

APPENDIX


Data Exists to Invest Wisely to Reduce Risk
1. Application whitelisting of permitted/trusted programs, to prevent execution of malicious or unapproved programs including .DLL files, scripts and installers.
2. Patch applications e.g. Java, PDF viewer, Flash, web browsers and Microsoft Office. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest version of applications.
3. Patch operating system vulnerabilities. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest suitable operating system version. Avoid Microsoft Windows XP.
4. Restrict administrative privileges to operating systems and applications based on user duties. Such users should use a separate unprivileged account for email and web browsing.
Source: https://securelist.com/blog/software/69187/how-to-mitigate-85-of-threats-with-only-four-strategies/
PREDECISIONAL—FOR DSB USE ONLY—DO NOT DISTRIBUTE
Cyber Defense
14

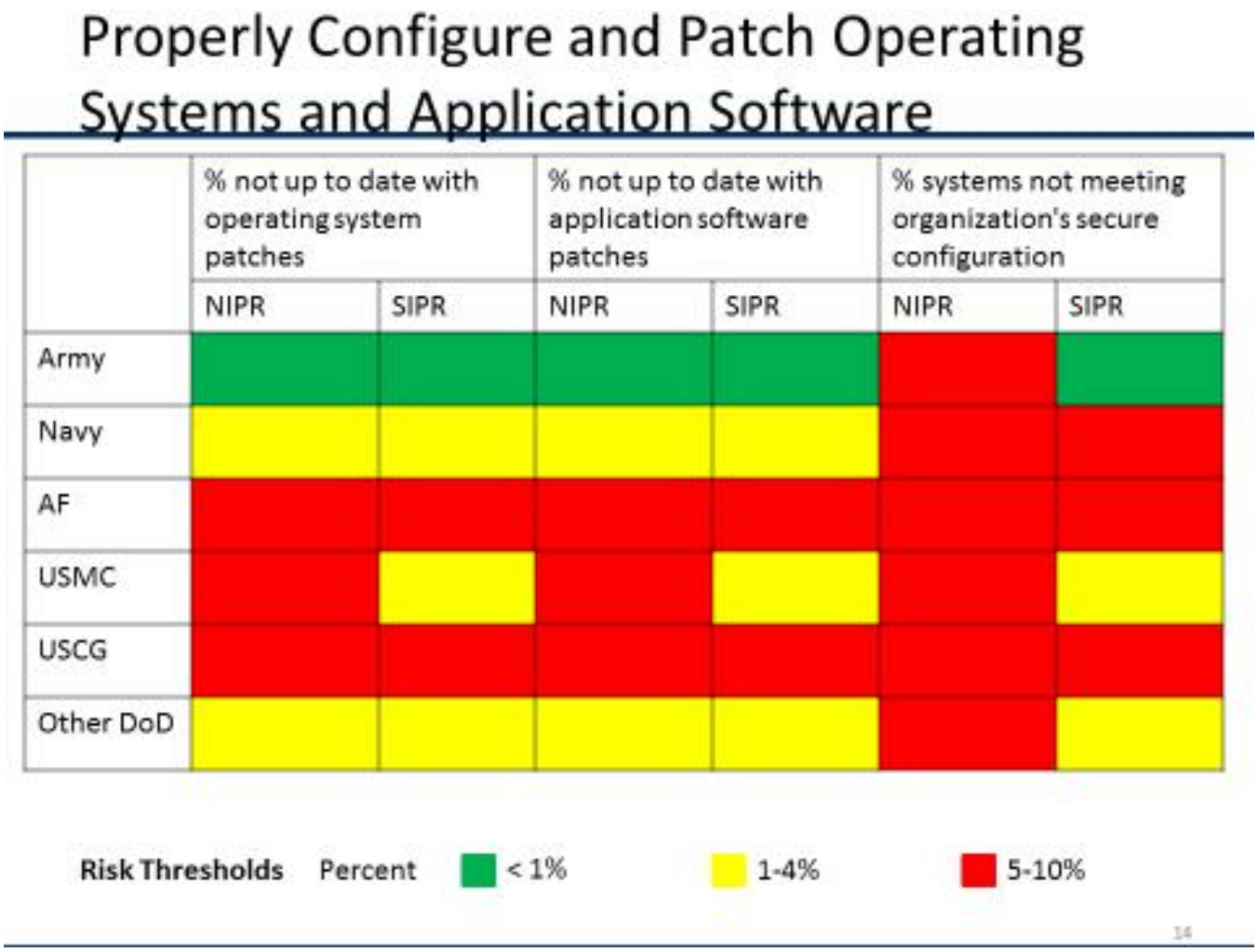
Maintain Control of Devices and Software on the Network

	Time to detect additions to the network		Time to alert administrators to additions		Time to isolate and remove unauthorized adds		Is application whitelisting used?	
	NIPR	SIPR	NIPR	SIPR	NIPR	SIPR	NIPR	SIPR
Army							NO	YES
Navy							NO	YES
AF							NO	YES
USMC							NO	YES
USCG							NO	YES
Other DoD							NO	YES

Risk Thresholds

Time	1 hour	1 day	1 week
Percent	< 1%	1-4%	5-10%

13



Note – The Task Force has combined the patching of application software and operating system software into this one chart.

Track and Restrict Administrative Privileges

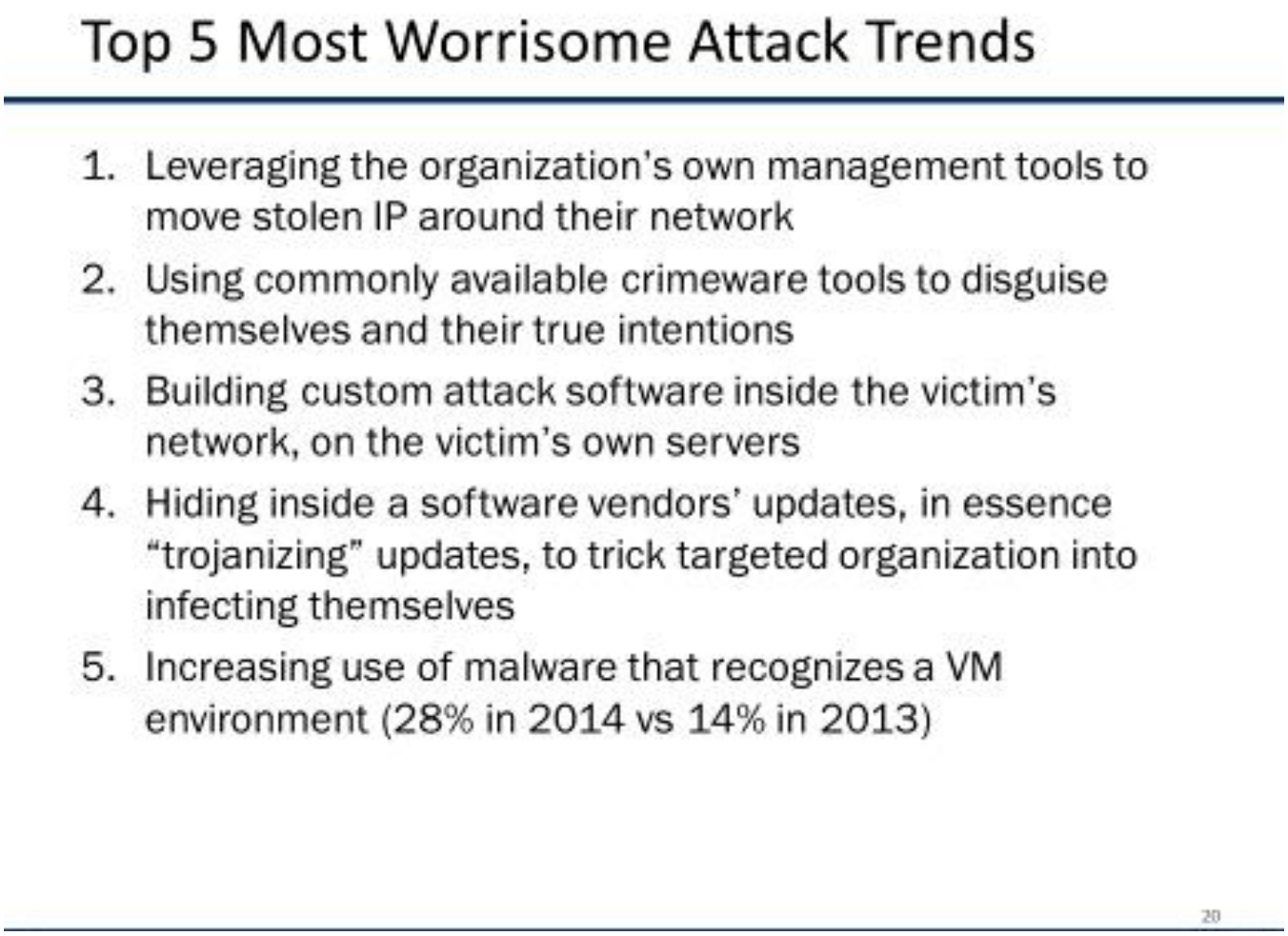
	% of users with elevated privileges		Does system report privilege escalation and authorizing source		% of admin accounts without two-factor authentication	
	NIPR	SIPR	NIPR	SIPR	NIPR	SIPR
Army			NO	YES		
Navy			NO	YES		
AF			NO	NO		
USMC			NO	NO		
USCG			NO	YES		
Other DoD			NO	NO		

Risk Thresholds Percent < 1% 1-4% 5-10%

15

APPENDIX

TOP 5 RISK LISTINGS


Top 5 Most Worrisome Attack Trends
1. Leveraging the organization's own management tools to move stolen IP around their network
2. Using commonly available crimeware tools to disguise themselves and their true intentions
3. Building custom attack software inside the victim's network, on the victim's own servers
4. Hiding inside a software vendors' updates, in essence "trojanizing" updates, to trick targeted organization into infecting themselves
5. Increasing use of malware that recognizes a VM environment (28% in 2014 vs 14% in 2013)
20

Top 5 Most Critical Cyber Defense Tech Needs

1. Automated methods to detect any hardware, software or firmware changes made in the supply chain
2. Cyber defense capabilities tuned particularly to work with embedded processors
3. Analytics designed to detect patterns associated with insider threats that continuously learn to increase P_d and decrease P_{fa}
4. Cyber defense for mobile applications
5. Reverse engineering to determine computed behavior to uncover malicious content before execution

21