Proven Strategies for Securely Sustaining Simulators and Training Systems

Rafael Rivera, Graham Fleener, William Kaczor
U.S. Navy NAWCTSD, U.S. Army PEO STRI, Cybernet Systems Corporation
Orlando, FL
rafael.rivera2@navy.mil, graham.fleener@us.army.mil, wkaczor@cybernet.com

ABSTRACT

One of the biggest challenges in supporting training systems in today's ever evolving cyber threat environment is securely sustaining simulators and training systems. Training systems are special purpose systems that unlike most general purpose information systems require an additional level of analysis before security changes can be implemented. Given the unique nature of these training systems, Information Assurance Technical (IAT) personnel cannot implement patches without rigorous analysis and testing. The need to have improved IA sustainment processes designed to reduce the total time spent on IA maintenance such as vulnerability management, reducing cyber threats, and a reduction of overall lifecycle costs is paramount to the trainer's operational success and budget.

Often times an IA sustainment strategy varies significantly by each training system, and the strategy is typically an afterthought when the system is designed or fielded. Our paper analyzes many of the current labor intensive issues with securely sustaining training systems and describes a strategy for reducing the overall number of hours required to sustain. We will discuss tools, architectures, processes, and configuration management techniques designed with the common goal of minimizing sustainment time once a system is fielded. Our paper will identify and maximize the use of Government licensed IA products and security software. We will discuss the importance and need for a well trained IA sustainment staff. Multiple and proven IA sustainment strategies and case studies will be discussed to include ideas for Program Managers to reduce IA sustainment time for legacy systems, and ideas to lower the overall IA lifecycle costs while designing a new system.

Our paper's goal will be to demonstrate secure architectures, IA sustainment processes and the security tools that will protect our national security information, while keeping the training systems main purpose in mind, and lowering overall IA sustainment costs and effort.

ABOUT THE AUTHORS

Mr. Rafael Rivera, CISSP, is the Command Information Assurance (IA) Manager for the Naval Air Warfare Center Training Systems Division, Orlando since September 2008. He served in A number of IT assignments in his twenty one year Army career before retiring in July 2001, including Chief of IT Division, G6 USARSO from 2009-2001, Combat Service Support Automation Management Officer, G4 Eighth Army, Republic of Korea, 1998-1999 and Information Systems Manager, National Security Agency, Fort Meade, MD, from 1996-1998. He holds a Bachelor degree in Computer Science from EDP College of PR and is a graduate of the Army's Information Systems Manager Course, School of Information Technology, Fort Gordon, GA.

Mr. Graham Fleener, CISSP, PMP is the Information Assurance Manager (IAM) for Project Manager of Training Devices (PM TRADE) in the U.S. Army Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI). Mr. Fleener served in the U.S. Marine Corps and then worked as a contractor for the Army before joining the Army Acquisition Corps as a Government employee. Mr. Fleener obtained both his Project Management Professional (PMP®) and Certified Information Systems Security Professional (CISSP®) certifications. Mr. Fleener holds a Bachelors of Science in Information Systems Technology from the University of Central Florida.

Mr. William Kaczor, CISSP, PMP is the Information Security Division's Technical Manager for Cybernet Systems Corporation and has been in the Information Assurance field for eleven years as well the IT realm for over 15 years. He has a Bachelors degree in Information Technologies with a specialty in Network Security and has multiple security certifications including the Certified Information System Security Professional (CISSP), a Navy Certified Certifier, Information Assurance Security Officer (IASO) from the US Army and Cisco Certified Network

Administrator. He has certified and accredited over 65 training and operational systems for all four branches of the DoD. He has completed a Master's in Business Administration (MBA) degree and achieved the Program Management Professional (PMP) certification.

Proven Strategies for Securely Sustaining Simulators and Training Systems

Rafael Rivera, Graham Fleener, William Kaczor
U.S. Navy NAWCTSD, U.S. Army PEO STRI, Cybernet Systems Corporation
Orlando, FL
rafael.rivera2@navy.mil, graham.fleener@us.army.mil, wkaczor@cybernet.com

THE IA SUSTAINABILITY CHALLENGE

A training system or simulator contains information systems, such as computers or networking equipment, that are subject to the same Information Assurance (IA) requirements or IA controls set forth in Department of Defense (DoD) Instruction 8500.2, Information Assurance Implementation as any other DoD information system. They are Special Purpose types of system but must undergo a rigorous certification and accreditation (C&A) process and achieve an Authorization to Operate (ATO) before becoming fully operational. The ATO is the authorization granted by a Designated Approving Authority for a DoD information system to process, store, or transmit information. This is directed in DoDI 8510.01, the DoD Information Assurance Certification and Accreditation Process (DIACAP), as well as in each service's IA regulations. Both of these processes and its early implementation into the design and development of a training system have been gaining momentum and familiarity with system integrators over the last several years.

The challenge now has turned to how a program transitions to manage and maintain the ATO and overall system security without having to expend excessive time and resources. According to Defense Acquisition University (DAU), training system maintenance and sustainment accounts for approximately 70%-80% of the total life cycle cost. This paper gives detailed examples of how U.S. Army, Navy and Marine Corps programs have met the challenges of maintaining the ATOs that they have achieved, as well as how future programs can leverage this experience to lower risk and resource utilization.

This paper discusses secure IA sustainment strategies that have been implemented on multiple DoD projects such as the Marine Corps' Aviation Distributed Virtual Training Environment (ADVTE), the Army's Project Manager Training Devices (PM TRADE) Consolidated Product Line Management (CPM) program, and the Navy's Littoral Combat Ship (LCS) and E-2D Hawkeye Integrated Training Systems. These strategies can be applied to limit a program's exposure to cyber security threats, lower the overall cost of security sustainment activities, and define a schedule to lower the cyber security risk.

This paper discusses secure architectures that include security in the initial design development and throughout the entire life cycle. Government Off The Shelf (GOTS) and Commercial Off The Shelf (COTS) tools can be used to validate threats and vulnerabilities while the system is in development and also operational; this concept is key to understanding the cyber threats to simulators and trainers.

Centralized IA management concepts can be built modularly to scale a system's specific security needs; a key for lowering life cycle management costs. Centralized systems in order to be effective should address auditing, back-up, recovery, intrusion detection, intrusion prevention, anti-virus management, and security patch management. These key features are essential in providing the ability to manage and sustain the information assurance controls protecting the trainer or simulator.

This paper provides proven and realistic secure architecture strategies that program managers can use in trainer or simulator design, implementation and life cycle maintenance. These strategies are taken from successful programs and described in a way that can be applied to other DoD simulators and training programs.

Trainers and simulators are special purpose devices that require careful planning and greater consideration to ensure the implementation of IA maintains system functionality. If a security patch or configuration causes the trainer or simulator to malfunction, then mission critical training could be ineffective or downgraded. A risk management process must be incorporated to ensure a trainer can sustain its IA posture and protect against the constantly growing cyber threats.

Training and staffing requirements are addressed to improve budget planning methods throughout the overall system life cycle. There are DoD and service level IA requirements for certified staff and defined security processes. This paper provides examples of how these training costs can be minimized.

This paper closes with discussing the principles of securely sustaining the next generation operational environment of the DoD and the training community.

THREE SUCCESS STORIES

All three authors of this paper actively develop and integrate cyber security solutions for the training community. This is not only our job, but our passion, and we continuously strive to find more economical and secure solutions for DoD training systems.

Within the DoD, Program Managers have the responsibility to ensure IA is implemented on systems that span a wide array of risk, classification, and size levels. Therefore, IA sustainment strategies will be described for a classified network like ADVTE, a standalone classified trainer like the Littoral Combat Ship, and Army live training systems. Each training system requires IA regardless of its classification or status as a standalone device, though the level of cyber security life cycle management effort *is* dependent on the confidentiality level (Public, Sensitive, Classified) and Mission Assurance Category (MAC) of each training system as outlined in Table 1.

The PM TRADE Live Training Transformation (LT2) Product Line through the Consolidated Product-Line Management (CPM) contract has the mission to focus on shared requirements to maximize commonality and component reuse of software for the live training community. This mission has brought various advancements to the manner in which IA is applied to live training systems. The LT2 program has implemented a lab environment with virtualization capabilities that has the ability to test and distribute Information Assurance Vulnerability (IAV) messages (Alerts, Bulletins, and Technical Tips) to the numerous sites supported by the lab. IAV and Security Technical Implementation Guide (STIG) execution and testing can be completed in the lab and developed into packages for distribution to site. Travel dollars and on site downtime are minimized by using a Post Deployment Software Support (PDSS) lab environment to support IA in addition to the primary mission of software support.

The Littoral Combat Ship trainer is a standalone classified simulator. Accreditation was required so a solution to lower labor costs for IA maintenance needed to be developed. The main issue was the training schedule which left minimal time to complete tasks such as security audits, backup and recovery or patch management. This was the genesis of the need to consolidate and centralize the requirement for an IA management system.

The ADVTE network is comprised of legacy and new USMC aviation trainers that needed the ability to connect locally at each base as well as long haul to other USMC air stations. The first step was to certify and accredit all 32 of the trainers. At the time this paper was written 16 of the systems received their ATOs in only 20 months. Instead of hiring an IA officer for each trainer or even each base, the program developed an ATO Currency (ATOC) program that allows the system patches to be updated by a team that travels to each base over a certain frequency of time. This allows the trainer to maintain the security posture that the ATO requires.

Throughout this paper we include how the lessons learned from each of these three successful programs can be used by program managers, development teams and maintenance staff to save money and lower risk.

CYBER SECURITY THREATS FOR TRAINERS AND SIMULATORS

In order to understand the IA requirements for a simulator or trainer we first have to identify some of the threats to the training environment. As trainer fidelity has increased, the additional threat to sensitive and classified information has also grown. Adversaries have tried to discover aircraft and missile vulnerabilities by prying through simulator data. Classified tactics are also a large piece of information that enemies could use to their advantage against our troops.

There is not a panacea against cyber security threats. In fact there is no amount of money or technical solutions that can 100% protect an information system from being hacked, damaged, or its data compromised. The best plan is to manage the risk of the system and have the tools in place to defend against the risk. Additionally, ensuring a properly trained staff is in place to identify the risk and take action if an incident occurs.

The case of Gary McKinnon, a British citizen who hacked into dozens of DoD and NASA computer systems demonstrates why even training systems need to be built and maintained securely. He hacked into training systems in NAS Patuxent River, MD and deleted information spanning dozens of computers on several training systems causing over $900,000 worth of damage. (U.S. vs. McKinnon, 2005).

According to the Defense Security Service's (DSS) 12th annual "Targeting U.S. Technologies" unclassified report to Congress, "Foreign entities continued to target information systems technology most frequently, primarily focusing on modeling and simulation software for military modernization programs."

There are several other incidents that have released classified information that could be used on the battlefield such as missile data and tactics. This release puts training systems and simulators at risk of further exploitation and damage.

Threats from virus's and Trojan horses are a constant threat that has to be identified as one of the top attacks against DoD networks and infrastructure. The ability to bring a virus into a closed system can occur with relative ease. A DVD or flash drive with a virus on it can wreak havoc. See Figure 1 for the most common security threats to security systems.

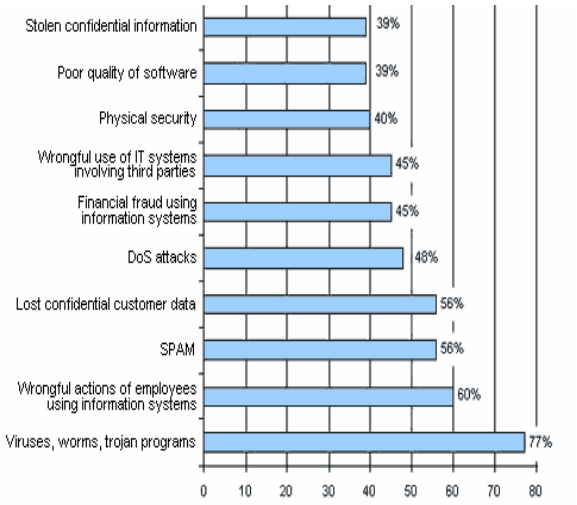

Figure 1 Security Threats to Information Systems

IA MAINTENANCE REQUIREMENTS

All IA requirements, also known as IA Controls, for the DoD are generated from DoDI 8500.2. Each service (e.g. Army, Navy, Air Force) has additional IA Controls that it leverages on its projects. Services can further add controls to ensure that data is protected for a specific regional threat or a potential vulnerability. These controls are to be included into all phases of a simulator or trainer's system lifecycle. See Figure 2 for the standard DIACAP lifecycle management controls.

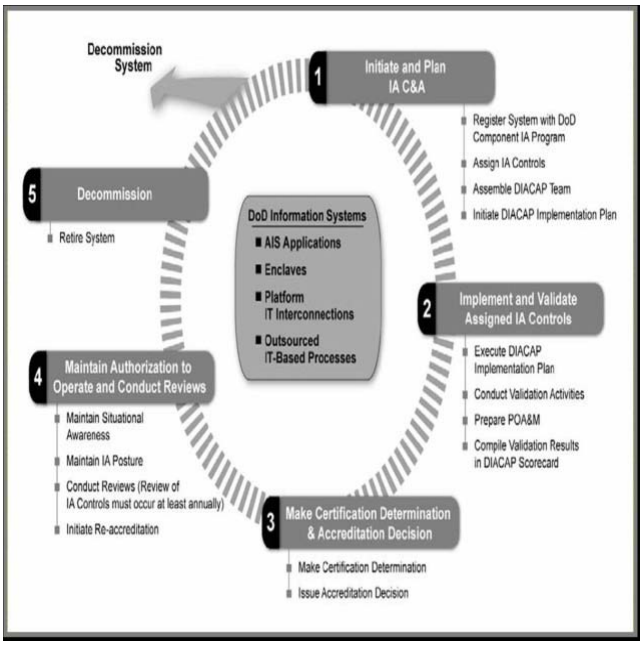

Figure 2. DIACAP Lifecycle Management

Some of the IA Controls that are specifically important for maintaining the IA posture of a system are:

DCDS-1 Dedicated IA Services
Acquisition or outsourcing of dedicated IA services, such as incident monitoring, analysis
and response; operation of IA devices, such as firewalls; or key management services are supported by a formal risk analysis and approved by the DoD Component CIO.

DCPR-1 Configuration Management (CM) Process
A CM process is implemented that includes requirements for:
(1)Formally documented CM roles, responsibilities, and procedures to include the management of IA information and documentation;
(2)A configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes, to include interconnections to other DoD information systems;
(3)A testing process to verify proposed configuration changes prior to implementation
in the operational environment; and
(4)A verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted.

CODB-1 Data Backup Procedures
Data backup is performed at least weekly. Review activity logs, audit records, waivers or other documentation to confirm that data backup is performed at least on a weekly basis.

ECAT-2 Audit Trail, Monitoring, Analysis and Reporting
An automated, continuous on-line monitoring and audit trail creation system is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and with a user-configurable capability to automatically disable the system if serious IA violations are detected.

VIVM-1 Vulnerability Management
A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place.

Wherever system capabilities permit, mitigation is independently validated through inspection and automated vulnerability assessment or state management tools.

Vulnerability assessment tools have been acquired, personnel have been appropriately trained, procedures have been developed, and regular internal and external assessments are conducted. For improved interoperability, preference is given to tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities.

The Federal Information Security Management Act of 2002 (FISMA) requires an annual review to be conducted for any system after the Authorization to Operate (ATO) has been issued. Additionally, FISMA requires a reaccreditation every three years. Included in the IA controls assigned to all DoD ISs are IA controls related to configuration and vulnerability management, performance monitoring, and periodic independent evaluations (e.g., penetration testing). The Information Assurance Manager (IAM) continuously monitors the system or information environment for security-relevant events and configuration changes that negatively impact IA posture and periodically assesses the quality of the IA controls implementation against performance indicators such as security incidents, feedback from external inspection agencies (e.g., IG DoD, Government Accountability Office (GAO)), exercises, and operational evaluations. In addition the IAM may, independently or at the direction of the CA or DAA, schedule a revalidation of any or all IA controls at any time.

DoD Information Systems (ISs) with a current ATO and found to be operating in an unacceptable IA posture through GAO and DoD IG audits, events such as an annual security review, or compliance validation shall have the newly identified weakness added to an existing or newly created Plan of Actions and Milestones (POA&M). Without a working POA&M, there is a likelihood the trainer or simulator may be denied to operate.

Classified	High level required for Systems Processing Classified Information
Sensitive	Medium level required for Systems Processing Sensitive Information
Public	Basic level required for Systems Processing Public Information

MAC	Loss of Integrity	Loss of Availability	Protection Measures
MAC I	Unacceptable	Unacceptable	Stringent
MAC II	Unacceptable	Difficult	Additional Safeguards
MAC III	Tolerated	Tolerated	Protective; Commensurate with Best Practices

Table 1. Sensitivity and Mission Assurance Capability Definitions

SECURE SYSTEM ARCHITECTURE

If a house is built with a solid foundation, then there is a high probability that it will stand for hundreds of years. If it is built on shifting sands it is doomed to collapse. The same can be said for protecting a trainer or simulator from cyber security threats and attacks. The information systems and networks that make up today's trainers and simulators must have security built in to ensure initial security and a plan must be developed from the beginning on how to maintain that security level.

A method of security design and integration the DoD is currently mandating is the use of Host Based Security System (HBSS). HBSS is a COTS suite of security software available as a GOTS product for use on any DoD system. HBSS includes virus protection, security policy auditor, anti-spyware, and host intrusion prevention. HBSS integrates McAfee products into a suite of software which can be used to "monitor, detect, and counter against known cyber-threats to Department of Defense (DoD) Enterprise."

Unfortunately, this HBSS mandate is also creating challenges for the training community of all branches within the DoD. Using tools like HBSS can cause simulator slow down, interference with applications

which takes away from the main purpose of the simulator or trainer. If security tools or settings detract from the main mission of a simulator or trainer then a work around must be developed.

When HBSS is implemented on a trainer or simulator the odds are very high it will conflict with system functionality or not work as advertised so the IA maintenance requirement is very high. Even though there is a dire need for security tools such as HBSS, system architects and the development team must incorporate it with care as to not break the simulator or trainer. So early testing to ensure full functionality and security compliance is the key to this product integration. Without proper IA and functional testing of the HBSS implementation, there may either be a downgrade in functionality or a security risk that could be exploited.

A common example of an ongoing issue is the screensaver and its automatic activation. In a simulation environment where multiple screens are being used without human interaction, the possibility exists the screensaver activation will cause a disruption in the training. One solution is to design and develop a software workaround. Another solution is to request approval of an exception. This risk management approach includes requesting approval for the need to extend the time limit as well as defining the additional security measures that will be put in place to reduce the risk. For example, the identification of a computer or tablet, such as the Instructor Operator Station (IOS), that requires this exception and documenting the details associated with the risk mitigation. The key point is it comes down to acceptable level of risk and gaining approval in the beginning of a project.

Another architectural concern is that of the operating environments. The days of repeatedly and manually following checklists to secure operating systems or network equipment is rapidly, and thankfully, coming to a slow end. The need to reduce the overall man hours that are involved in patching and securing just one computer is critical to lowering costs and staying on schedule. The DoD has begun to move away from the manual STIGs and has begun to develop automation.

A method that should be applied to ensure a secure architecture is to use only approved operating systems that support the use of automation. On the ADVTE program there has been development of an automated Windows 7 process that will reduce the manual labor by 30% in initial startup and continuing IA support.

The Army has addressed automation by releasing and supporting the Army Golden Master (AGM) Operating Systems (OS). AGM is a GOTS version of a Windows operating system, either XP, Vista, or 7, already preconfigured with many security management tools and security setting. Not all necessary security settings and configurations are implemented due to operational and functional considerations. The Air Force has a similar trusted desktop GOTS product available for implementation. The only warning to development teams is that with the OS already hardened, there could be a security setting enabled or service disabled that is needed for the trainer or simulator's functionality. A secure developmental path would be to lock down the trainer and then perform development working through any issues coming as a result of the pre-configured security. As you may have seen so far in this paper, there is no panacea to cyber security.

Another method of automation is in the form of security policies that can be standardized across many systems and can be continually edited as new security configurations and settings emerge in a given DISA Security Technical Implementation Guide (STIG). The standardization of security policies allows for an easy to use step by step update and activation process. DISA is currently releasing security policies in the form of an .inf file that updates the security configuration of many of the Common Criteria approved Operating Systems.

For Linux systems, scripts have been created to automate another 20% of the manual functions that usually make up a large portion of the overall IA budget. Scripts are the key to reuse and cost savings. Many IA tasks can be automated and then reused on simulator or trainer Linux operating systems and servers.

A centralized solution also facilitates a secure architecture. It allows a PM and system maintainers to incorporate all scripts and reuse methods so that total IA maintenance time is reduced by 60%.

This will be discussed further in the tools section of this paper but from an architecture standpoint, it is a key component.

IA MAINTENANCE TOOLS AND TECHNIQUES

In the "old days" of IA the largest cost of the effort used to be the generation of thousands of pages of paperwork. Today's major cost driver for IA resides in the sustainment of accredited and fielded systems.

Tools and techniques for IA maintenance and cyber security protections are dependent on system design and how the protections are implemented. For example, if a virus scanner is turned off and there is no procedure on how or when to run a manual scan then there is an unacceptable lapse in security.

The primary IA design element that a program should employ is a centralized IA management solution. A solution that combines all the tools for auditing, back-up, recovery, intrusion detection/prevention, patch management for Windows and Linux operating systems, and virus definition management.

Centralized solutions have been proven to lower overall IA maintenance costs by 60%. The example in Table 2below shows the difference in time to complete a standard monthly IA maintenance process.

Example: Monthly IA activities on a 12 computer trainer or simulator with both Windows and Linux			
Solution	Hours to back up each system	Hours to install Windows and Linux Patches	Hours to perform all other IA tasks
Manual	24 (avg. of 2 hours per system)	84 hours (7 hours per system)	24 (2 hours per system)
Centralized	12 hours (1 hour per system)	54 hours (4.5 hours per system)	12 (1 hours per system)
Time Savings (hours)	**12**	**42**	**12**
Total savings = 66 hours are saved each month			

Table 2. Centralized IA Solution Savings

These statistics were captured during 1 year of IA maintenance on the ADVTE program for the ATO Currency task order. The hours were then compared to the activities on the LCS trainer and the CH-53 CFTD. The 66 labor hours saved over each month multiplied by a 3 year support contract is 2376 total hours which is greater than 1 FTE. If a project director has 10 programs to maintain that may save over $2 Million dollars in 3 years.

A second tool that should be used in the development of a simulator is the security lockdown toolset that is used during the formal IA testing. In other words, the tools that are used during testing should be the same tools that are used to do final system integration. Unfortunately, this tool set changes as the DISA and DoD services change the required tools. That is why it is important to create the tool set during development and maintain it throughout the trainer/simulators life cycle. If there is no continuity in maintaining this toolset there will be a waste of time downloading or purchasing the tools required to securely sustain the trainer or simulator.

A third set of tools that should be utilized while the simulator or trainer is in development are automated IA tools. As discussed previously, automation of repeatable tasks such as creating a standard IA image that would be installed on all new computers/servers is a time saver. Automating the activities that are required to secure an Operating System, such as Windows 7 registry edits, can be automated and with a little time and dedication can be maintained to reduce overall IA costs.

IA MAINTENANCE PROVEN STRATEGIES AND PROCESSES

As budgets for real equipment training continue to be reduced, simulators and trainers are being used more frequently as real-world substitutes. Therefore, the training systems of tomorrow will most certainly need to provide as realistic training as possible. This may involve the use and dissemination of classified information. The protections that must be in place to protect classified information are key to national security and must be balanced to meet the needs of the training community.

A program must have a plan which details how it will implement a secure sustainable training system. The plan, whether it is an Information Assurance Vulnerability Maintenance Plan (IAVMP) or a Continuity of Operations Plan (COOP), should include a schedule of events at a high level and step by step repeatable procedures. The step by step procedures are the key to sustaining security as it allows the maintainers a repeatable process that can be completed. One example of this process in action is the USMC ADVTE ATOC program. The program maintains the ATOs for all Marine Corps trainers that have received an ATO.

WHAT CYBER PROTECTIONS DOES MY PROGRAM NEED?

A well trained staff is the first line of defense in limiting cyber security threats. The staff needs to be trained on the security architecture as well as the tools

that reside on the trainer or simulator. The hands on knowledge and use of the tools will limit exposure by identifying the threats and vulnerabilities that are developed during a trainer's life cycle.

The staff member who is the designated Information Assurance Officer (IAO) should meet the requirements outlined in DoDD 8570.01, Information Assurance Training, Certification, and Workforce Management. Depending on the level of interaction with the security tools the team member should meet have achieved one of the certifications identified in the next section.

Another protection that a trainer or simulator needs is a solid information assurance vulnerability management (IAVM) plan. The IAVM plan should include detailed methods of installing patches and updating security settings, along with a method for management of security documentation updates.

A third protection that a trainer or simulator needs is solid physical security procedures. The procedures should be documented for access to the trainer, approved use procedures, and include documentation on how the DoDI 8500.2 physical security IA controls are met. This plan is critical to ensure that IA compliance is maintained for the entire life cycle of the trainer.

WHAT TRAINING DOES THE STAFF NEED?

The first item that the training staff needs is its own certified IA expert. This involves more than just passing a DoDD 8570.01 certification such as the CISSP, although that is a requirement, there must also be comprehensive hands on training of how to maintain the security of the system. The program via its acquisition should require the contractor to build an IA training plan so that the simulator or trainer is not just "thrown over the fence" without any training on how to maintain the IA of the system. The Littoral Combat Ship program has developed a detailed training document and provided up to 16 hours of on the job training that involves job shadowing, step by step procedure instruction and actual IA maintenance scenarios.

There are a multitude of training programs that an organization can send its people to so that they understand the complete IA process. This will increase the Governments knowledge and activity in the IA realm.

DoDD 8570.01 is the official guidance for what IA Technicians and IA Managers must be certified to complete the activities necessary of any IA process.

A second highly recommended training item that a program needs is that of a regimen of hands on experience. The developer/integrator should provide the Government with a detailed training plan and then use at least 16 hours to show the maintainer how to do the work. This will give the maintainer confidence that the plan is detailed enough to train new staff and that he/she knows the intricate parts of IA maintenance process.

Hands on training, formal IA training, and certification are the three pillars to having a solid IA team for your organization.

MANAGING THE SECURITY LIFE CYCLE

Management of a simulator or trainer program is a challenge in and of itself but when cyber security is added to the mix, the attention to risk management and security compliance must be a priority. Every week new vulnerabilities and exploitations are discovered which increase the risks to DoD information systems and networks.

During acquisition of a simulator or trainer the requirements must be clearly defined for what is expected from the contractor to meet the IA requirements. The requirements developers and source selection team should work closely with the Information Assurance Manager (IAM) to ensure IA is clearly and specifically documented in the Statement of Work and Performance Work Specifications. It is vital to have IA requirements sent to industry which clearly specify what the program intends to implement so industry can accurately provide proposals to meet the requirements in a cost effective manner.

It is critical that cyber security configuration management be integrated with a program's overall configuration management plan. If not, problems will result. For example, if the development team re-images or cold starts a machine after the cyber security was applied, then the IA controls will be erased causing a extensive rework. That is why it is important for the development team to involve the IA team members in the process so that security settings and patch issues can be worked together as a team.

During testing, the IA team conducts internal testing prior to formal government testing. This ensures that all IA requirements are met. It is never advisable to go

from development right into Government testing. If there are errors found by the Government appointed testers then it will cause extra work to fix plus it will cause a loss of trust with the certifying authority. This loss of trust may lead to a higher level of scrutiny on the second or third attempts and could lead to a denial to operate.

As previously discussed, IA maintenance is the key to ensuring that the simulator or trainer is secure throughout its life cycle. A plan and budget must be in place to maintain the IA posture of the trainer or simulator. If the money is not there the plan is worthless. If the money is there and there is no plan then it is a waste of money.

Disposal takes place whenever a system has reached the end of its service life and normally includes a concerted effort to sanitize or destroy all hard drives and non-volatile memory. This necessary step of destroying hard drives prevents mission data or even personnel data from falling into the hands of our enemies or even identity thieves. If these destruction or sanitization steps are not taken our enemies could piece together several unclassified pieces of information to form a classified plan or tactic. When in doubt shred it out.

THE FUTURE FOR SECURE SUSTAINABILITY

Cyber threats and attacks are a constantly evolving challenge and can leave management in the difficult position of having to choose an unacceptable level of risk in order to meet cost and schedule constraints. If a program plans for security that will be required 18 months (Moore's Law) from now, as opposed to the immediate need, then the DoD will have more flexibility in future growth with the security already in place.

Mobile security will continue to be an item of interest in the near future as the Army and USMC have the desire and plan to have Soldiers and Marines use hand held smart phones for various military activities. This is flowing over into the training community for such tasks as combat training, and system setup and maintenance documents.

Distributed Long Haul IA Maintenance can be a reality once training networks are better integrated and better connected. This will allow the organization to push necessary patches to a simulator on the network. For higher risk patches or security configurations, detailed instructions or live video chat can provide the intermediate to advanced level technician the ability to patch the simulator or trainer from one central location. Distributed Long Haul IA Maintenance will also provide real time configuration management, backup recovery, intrusion detection and even intrusion prevention. This will allow for an organization to use only 1 to 3 people to manage 12 sites as opposed to each site having their own team of 1 to 3 IA engineers. This centralized management solution of the future can only happen once the networks become more integrated.

CONCLUSION

Cyber security is an ever changing threat. There is no panacea that can be applied to protect information systems from the threats or the adversaries that want to obtain our classified information. Instead a well developed and fully executable security plan, including secure sustainability, for a training system or simulator is key to managing risk and providing cyber security for its life cycle.

REFERENCES

Department of Defense, 8510.01. (2008). *DIACAP Application Manual*.

Department of Defense Directive, 8500.1. (2002). *Information Assurance*.

Department of Defense Instruction, 8500.2. (2003). *Information Assurance Implementation*.

Department of Defense Directive, 8570.01. (2004). *Information Assurance Training, Certification, and Workforce Management.*

Department of the Navy, 5239. (2005). *Information Assurance Program*.

Department of the Army, Army Regulation 25-2. (2009). *Information Assurance*.

Defense Security Service (DSS). (2010). *Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry*.

PEO STRI Basic Accreditation Manual (BAM). (2008).

U.S. vs. Gary McKinnon. Retrieved June 14, 2011, from http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/cyberlaw/usmck1102vaind.pdf

Global Information Security Survey. (2004). Ernst&Young. Retrieved June 14, 2011, from http://www.secrecykeeper.com/news/news1-e.html