DEFENSESYSTEMS
KNOWLEDGE TECHNOLOGIES AND NET-ENABLED WARFARE

DOD adopts tactical approach to information assurance

Cyber experts build security infrastructure designed to armor-plate sensitive information and critical systems

- **By John Edwards**
- **Aug 18, 2011**

In an age when enemies are met online and on the battlefield, information assurance is evolving from a defensive measure into a tactical strategy. The Defense Department and other government and commercial technology experts are working hard to create an information and communications security environment that meets existing data threats and anticipates future attacks.

DOD is developing a multifaceted information assurance strategy, said Richard Hale, chief information assurance executive at the Defense Information Systems Agency. Hale noted that agency cyber experts are hardening networks against attack by "configuring computers properly, continuously measuring the configuration to make sure it stays secure, using add-on hardening tools in operating systems, using perimeter defenses that can shield vulnerabilities from attack, using PKI credentials to drive out anonymity in every transaction and to remove certain access control vulnerabilities."

RELATED COVERAGE:

Top weapons of mass destruction agency daunted by info assurance

Marines create occupational category for cyber warriors

He added that DOD is also structuring network and computing architectures for safer file sharing and to contain problems and allow proactive maneuvering in response to information about a potential threat. "Dynamic defense, including maneuver, is increasingly important," Hale said.

The buck stops where?

DOD is tightening its information assurance practices in the aftermath of a recent series of high-profile and highly embarrassing security leaks. "After WikiLeaks, DOD has stepped up on their internal security measures," said Kyle Lai, president and CEO of KLC Consulting, a defense industry security and IT consulting firm. Lai noted that lax information assurance practices paved the way for unwanted disclosures on scores of sensitive issues in 2010 and early 2011, including documents related to missions in Iraq and Afghanistan. "DOD contractors that store or process information for DOD may or may not have gone through security assessments to ensure the information is secure," Lai said.

Lai said he feels that thousands of smaller defense contractors pose perhaps the biggest threat to DOD's information assurance strategy because they are the organizations most likely to let business concerns get in the way of national security. "Large DOD contractors have the budget and resources to do a better job on information security practices," he said. "Small firms with little or no budgets will worry about getting contracts and [will] meet deliverables first. Security may be treated as optional or 'whenever the government asks for it, then we deal with it.'" Given the problem's size and scope, Lai said DOD will need a significant amount of time to fully address its contractor security audit/assessment issues.

Information assurance is a responsibility shared by multiple parties at DOD, beginning with the agency's CIO and extending to nearly all uniformed and civilian personnel. "In day-to-day operations, U.S. Cyber Command has the responsibility for operating and defending the department's networks," Hale said. Cyber Command was established in 2009 with the mission of shielding some 15,000 U.S. military networks from domestic and foreign threats. "Every person who uses the infrastructure has a responsibility for appropriate use," Hale said.

Training is key to ensuring that safe information management practices become second nature for all personnel. Each service branch

now requires personnel to undergo information assurance training. The Marine Corps' program is typical. "Marines are now exposed to the cybersecurity training requirements from the time they enter formal training at the recruiting depots through their follow-on schools and unit assignments during their Marine Corps career," said Ray Letteer, cybersecurity chief at the Marine Corps' Command, Control, Communications and Computers Department.

New technologies

Although information assurance applies to all DOD information and communication systems, the weakest link in the agency's security chain are new technologies and their tendency to present fresh and unanticipated security vulnerabilities. Of all emerging technologies, including mobile devices, wireless networks and social media platforms, cloud computing is widely viewed as the technology that most often keeps DOD information assurance experts from getting a full night's sleep.

Hale noted that DISA is focused on providing DOD with a rich set of IT services. "These range from software-as-a-service kinds of offerings, like Web conferencing services and e-mail services, to platform-as-a-service offerings of on-demand computing and storage in the DISA system, called Rapid Access Computing Environment," he said. "These are all available to DOD customers over the DOD's private networks, and so are essentially private cloud services."

DISA has so far steered clear of commercial cloud services. "Given the large number of information assurance questions, we're approaching the use of shared, commercial clouds in a cautious way," Hale said. DISA is building its own cloud environment based on hardened servers to secure DOD data. The agency is also relying on the Defense Advanced Research Projects Agency to seek out and deliver innovative new cloud network security technologies and approaches.

DOD is handling its cloud security needs with an array of high-level tools. "In this private cloud, we're focusing strongly on driving out anonymity through the use of the cyber identity credentials issued by a NSA/DISA service called the DOD Public Key Infrastructure," Hale said. "These PKI credentials are also being rolled out on the Secret IP Router Network this year and next." SIPRNet is cleared to transmit information classified up to and including the secret level. "We expect that everyone on the SIPRNet will be using one" of the credentials by the end of fiscal 2012, Hale said.

DISA is also helping DOD re-engineer the way the department controls user access to information resources, particularly data residing in the cloud. "We believe that direct authentication from a client device to a server via the use of a PKI credential is the right model," Hale said. "This means no middle layers — for instance, portals — are involved in the actual authentication."

DOD would also like to eliminate individual user accounts, which are clumsy to use and prone to negligence, theft and misuse. "The account-based access model inhibits sharing in a place as large as DOD with as many different information services as we have," Hale said. "Access should be granted using…[an] attribute-based access control." Such a system grants authenticated users access to specific resources based on set policies as well as the permission level assigned to the user or group. Access control also often includes authentication, which proves the identity of the user who is trying to log in.

Meanwhile, DOD is using automation to remove the human element from information systems whenever possible. "Automation is the only way to do some of these things fast enough and without the vulnerabilities introduced by human error," Hale said. To this end, DOD cyber experts are turning to the Security Content Automation Protocol, a data standard developed by the National Institute of Standards and Technology to enable automated vulnerability management and measurement in addition to policy compliance evaluation. "DISA buys many of the DOD's enterprise hardening and measurement tools; we require SCAP compliance in all of these so we can better connect these different tools into a more automated security ecosystem," Hale said.

Certified assurance

Information assurance begins even before DOD acquires IT equipment or software. Information assurance assessment starts with vendors, which must submit candidate products to the the DOD Information Assurance Certification and Accreditation Process. "This process evaluates the security properties and vulnerabilities of a new system, service or technology before it is deployed," Hale said.

Lon Berman, principal consultant at the BAI DIACAP Resource Center, a DIACAP consulting and training firm, said DIACAP compliance is an arduous and time-consuming process for DOD contractors. He noted that technologies are carefully scrutinized for potential security weaknesses from every possible angle. "They'll get looked at in terms of how well they do or do not comply with all of the myriad security requirements," Berman said. "All that information will get boiled down into something that a high-level official can digest, and then that person is going to sign a formal authorization to operate."

As it adds and upgrades security technologies and practices, DOD also strives to ensure a uniform level of information assurance across all departments. "The security rules are the same for all DOD personnel, regardless of location," Letteer said. "The threats may be different because of location, such as the tactical edge, [but] the security rules allow for mitigations that can range from some technical implementation to managing user behavior through training and inspections."

As information assurance continues transitioning from a defensive response into a tactical strategy, DOD is moving carefully to ensure that security measures, no matter how well intentioned, never interfere with the department’s fundamental mission of protecting vital national interests. "DOD's information infrastructure exists to support better, faster, cheaper mission execution,” Hale said. “All of us have to treat [information assurance] as the mission-essential tool it is.”

About the Author

John Edwards is a contributing writer for Defense Systems.