THE AMERICAN FOREIGN POLICY COUNCIL

Defense Technology Program Brief

April 2015 Washington, D.C. No. 10

Understanding Information Assurance

By Trey Herr and Eric Ormes

Briefing Highlights

Information Assurance focuses on ensuring the confidentiality, integrity and availability of information. It encompasses a cluster of topics, including the defense of information systems and networks against compromise, design of secure software, protection of critical infrastructure, and the challenge of educating and hiring qualified professionals.

• • •

The best information assurance strategy will depend on the context of the threat, and the organization being protected. There is no single plan capable of protecting everyone. The golden rule for any organization is that the cost of the defense should not exceed the value of the information being protected. A thorough risk assessment for every organization is the only way to determine what countermeasures are best and how to design a defensive strategy.

• • •

In the realm of Information Assurance, vulnerability management is one of the most important areas for strengthening defenses. Vulnerabilities are the weaknesses that can be exploited by a threat in order to compromise the confidentiality, integrity or availability of information.

• • •

Critical Infrastructure Protection (CIP) is the protection of hardware and the specialized software that controls it, as well as of information systems that are deemed to be of national importance (like those used in the financial sector). CIP falls under Information Assurance as well. For all of its specialized challenges, the basic steps are similar: to isolate and protect key applications from the Internet, to remove or patch vulnerabilities in software, and to make sure users don't break anything.

Information Assurance is the art and science of securing computer systems and networks against efforts by third parties to disable, intrude, or otherwise impede operations. It is the focus of most "cybersecurity" professionals in the technical community. The principal goals are to maintain an information system's Confidentiality (the secrecy of information as it is used and stored), Integrity, reliability of data and equipment, and Availability, that a computer system is ready and able to function as needed.[1] Information Assurance includes writing secure software, deploying it safely, and managing it to minimize the risk of compromise.

The breach experienced by the Target Corporation in 2013 demonstrated that determined opponents are only half of the equation in cybersecurity. In that incident, the company's point of sale systems were compromised because an employee at a third party company clicked on the wrong attachment, allowing attackers to jump into the Target corporate network and move their code onto merchant systems around the country.[2] Securing the third party vendor's systems, as well as Target's corporate network, against these sorts of attackers are Information Assurance challenges. This paper highlights and describes five related priorities; network and system security, software vulnerabilities, information sharing, critical infrastructure protection, and workforce training and qualification.

Network and Information System Defense

When it comes to network defense, there are two main categories of defensive systems: host-based (the defensive mechanism resides on a system to protect it) and network-based (the defensive system focuses on looking at network traffic to protect systems).[3] Regardless of the category of defensive system, they are deployed utilizing various techniques in order to form a defensive strategy. Here are a few key concepts and ideas:

Defense-in-depth: This is the overarching strategy employed by most

Mr. Eric Ormes *is a cybersecurity consultant for the U.S. Government and private sector and a former United States Air Force Communications and Information Officer.* ***Mr. Trey Herr*** *is a senior research associate with Cyber Security Policy and Research Institute and a PhD candidate in political science at George Washington University. He consecutively works as an adjunct researcher at the Institute for Defense Analysis (rch760@gwu.edu).*

organizations. Conceptually similar to medieval castles, defense-in-depth is composed of multiple defensive rings, from the outermost curtain wall to the inner ward. The strength of the design is the multiple levels of protection and redundancy, all of which must be defeated, bypassed or neutralized before an attacker can penetrate to the inner sanctum and achieve his objective.

While based upon solid concepts, defense-in-depth runs into difficulties in the virtual world, where a new vulnerability might turn even the stoutest fortress into a house of cards overnight. Newer technologies emphasize access controls and the behavior of network traffic and individuals moving in and out of the fortress, rather than relying solely on layered defenses.[4]

Honey Nets: Using systems that appear genuine, this strategy is based upon trying to hide real network traffic and computers among fake versions.[5] While this is the epitome of a somewhat criticized practice known as "security through obscurity,"[6] the defender has two objectives in employing a Honey Net. First, to cause so much confusion for an outside attacker regarding what is real and what is fake that it makes their task exponentially more difficult to execute. Second, to have the attacker target fake systems and traffic instead of real ones. Since this is a defender-controlled environment, typically with various forms of detection tools that activate the moment a breach occurs, the attacker will likely tip his hand and reveal his presence. This defensive strategy is one that acknowledges the difficulty of stopping 100% of the threats, 100% of the time, and relies instead on attackers to fall for a trap and reveal themselves. So long as attackers are willing to take the bait, the strategy can be effective.

Virtualization: A virtual machine is an emulation of a computer system, a digital "replica" of a computer within a real machine, that enables the encapsulation and containment of processes as they run on the host system.[7] This means that when a program runs, whether malicious or not, it is only granted access to a set amount of resources and does not interact directly with important system processes. Therefore, it does not matter if a threat reaches the target, as it will be contained within the virtual environment. This means that the virtualized software does not care about what vulnerabilities might be present in the various other applications and programs, because once the virtual process is shutdown, the malware is gone as well. This is not a foolproof method, and there are attacks—referred to as Virtual Machine (VM) escape—that could allow a malicious process to try and break out of its container and infect the host system.[8] Currently however, many of these attacks are either technically difficult or resource intensive to execute.

Federal Standards: U.S. government information assurance standards are rooted in the Federal Information Security Management Act of 2002 (FISMA). This was the original source of responsibility for the National Institute of Standards and Technology (NIST) to develop information security and risk management standards for the Federal government. It resulted in a set of requirements and checklists, which have received varying degrees of criticism since.[9] There have been several recent efforts to reform FISMA, including a large provision in the failed 2012 Lieberman/Collins bill (Cybersecurity Act of 2012, S. 2105)[10] and the 2014 Federal Information Security Modernization Act,[11] which successfully implemented reforms to reporting requirements and operational standards.

Some of the 2014 changes included a shift toward the practices of the NIST Risk Management Framework (RMF) which is in the process of being implemented across Federal civilian and national security IT systems.[12] The RMF is based on a series of NIST Special Publications that lay out a common risk assessment and mitigation process, including a compendium of security controls, applicable based on an information system's risk category. These Special Publications form the basis for Federal organizations to a develop information assurance security plan and secure their IT environments.

As with many things, the best information assurance strategy will depend on the context of the threat, and the organization being protected. There is no single plan capable of protecting everyone. The golden rule for any organization is that the cost of the defense should not exceed the value of the information being protected. A thorough risk assessment for every organization is the only way to determine what countermeasures are best and how to design a defensive strategy.

UNDERSTANDING INFORMATION ASSURANCE

The key to understanding risk, in other words, is understanding scarce resources. No organization or business can protect everything, everywhere, all of the time. Choices have to be made to prioritize some things over others. Identifying which data and systems are most vulnerable or could present catastrophic damage if they are lost or unavailable is critical to assuring information security.

Vulnerabilities

In the realm of Information Assurance, vulnerability management is one of the most important areas for strengthening defenses.[13] Yet it generally receives scant attention from organizations working to prevent breaches. Vulnerabilities are the weaknesses that can be exploited by a threat in order to compromise the confidentiality, integrity or availability of information. They may be purposefully included features or simple bugs in an otherwise functional design.

There are three main types of vulnerabilities: physical, human, and system (software or hardware). Physical vulnerabilities can range from susceptibility to Acts of God to poor security at server facilities. People likewise pose a vulnerability to information assurance, either through willful acts as "malicious insiders" or simple ignorance of security precautions (e.g., by clicking on attachments). There are varying controls that can be put in place to address these issues.

In software, vulnerabilities don't impede system operation. Instead, they act as a narrow window through which an exploit may be written. For example, a program that expects to retrieve a static image file but fails to check the supplied file type might return an executable software program instead. Retrieving the image was intentional, but failing to check the file type allows a third party to execute malicious software. The Love Letter virus of 2000 relied on the fact that Windows 2000 and XP hid known file extensions when parsing file names from the right to the left. The virus, an executable program, thus appeared to be a .txt file, while it actually was a visual basic script (LOVE-LETTER-FOR-YOU.TXT.vbs).[14] While this design convention didn't constitute a "flaw" per se, it was used by third parties to effect unintended operations in the software. Vulnerabilities may also be introduced directly to hardware through compromises in chip design or manufacture somewhere along a supply chain.[15]

While software developers have incorporated security into their development processes, thousands of vulnerabilities are still found in software every year. Many of these software-based vulnerabilities can be found on NIST's National Vulnerability Database. In 2014, over 7,900 vulnerabilities were published on the site.[16]

But despite the high number of vulnerabilities discovered each year, several of which have been rated as having a "Critical" impact to security, many organizations still do not view addressing vulnerabilities on a regular basis as part of their cybersecurity program to prevent breaches. In the Cisco 2015 Annual Security Report, 90% of respondents said they feel, "…confident about their security policies, processes, and procedures."[17] However, less than 50% of those polled stated that they utilized vulnerability scanning or patch and configuration management as part of their security programs.[18]

This is concerning, given data from Hewlett-Packard's Cyber Risk Report 2015 that states that the top 10 vulnerabilities they saw targeted in 2014, accounting for 78% of the total observed, were discovered between 2009 and April 2013.[19] When considering the lack of emphasis placed on vulnerability scanning or patch and configuration management, it's not a surprise that 54% of Cisco respondents reported they needed, "…to manage public scrutiny following a security breach."[20]

Due to the complexities of software interaction, both with other programs and hardware, it is impossible to detect all vulnerabilities prior to a piece of software being published. Thus, maintaining a community of vulnerabilities researchers who responsibly disclose data to vendors, and having vendors issue patches in a timely fashion, must continue.

Information Sharing

Information sharing has been a vociferously debated topic within policy circles for the past several years, a debate that has been driven largely by several versions of the Cyber Intelligence Sharing and Protection Act. There are three possible uses for such a law. The first is to encourage information flow from the government to private sector actors. In this 'information down' scenario, Federal intelligence collection and analysis capabilities are made available in some limited fashion to the private sector to improve the latter's ability to understand and defend against threats. A second function of the law would be to encourage information sharing between private actors, while a third would be to encourage 'information up' from private actors to the government. In this situation, the government acts to improve its own situational awareness of civilian networks by incentivizing private groups and firms to share their respective network activity and suspected malicious traffic.

Information sharing "up" may provide the government with an information assurance advantage, but it is not clear what benefit will be gained by the private sector. Information sharing "down" may reinforce firm's security capabilities and awareness, but is complicated by the need for clearances to share classified information with companies outside of limited pilot programs like the Defense Industrial Base Cyber Security and Information Assurance activity.[21]

Sharing threat information is already common practice in parts of the private sector. One example is the "signatures", or defining characteristic of new attacks, shared by vendors with users of their anti-virus and intrusion detection systems. In early 2015, Facebook announced ThreatExchange, a platform for sharing signatures, URLs, and contextual information about threats with other firms.[22] What began as an ad-hoc collaboration between companies to help stop sizable distributed denial of service (DDOS) attacks, the service will combine proprietary and open source information feeds into a single data format accessible to members.[23] Yet many information assurance experts criticize the focus on information sharing as it provides little direct information assurance benefit; "information sharing allows better and faster bandaids but doesn't address the core problem" says Jeff Moss, founder of the DEF CON and Black Hat information security conferences.[24]

Critical Infrastructure Protection

Critical Infrastructure Protection (CIP) is the protection of hardware and the specialized software that controls it, as well as of information systems that are deemed to be of national importance (like those used in the financial sector). CIP falls under Information Assurance as well. For all of its specialized challenges, the basic steps are similar: to isolate and protect key applications from the Internet, to remove or patch vulnerabilities in software, and to make sure users don't break anything. There are differences between the software in your laptop and that used to control industrial systems, but the distinction is only a fraction of what it was a decade ago, and it is one that continues to shrink. For some sectors, standards of protection and practice already exist. For example, companies involved in electrical power generation and transmission operate under security standards developed by the North American Electric Reliability Corporation (NERC).[25] For others, like financial services, they are still evolving.

Presidential Policy Directive 21 (PPD-21) identifies sixteen critical infrastructure sectors including chemical manufactur'ing, the financial services industry, and electricity generation. Each of these has been highlighted as, "essential services that underpin American society."[26] There are many challenges in securing each of these diverse sectors, but two particular issues predominate.

First, the vast majority of information system assets in each of the sixteen sectors are in private hands, which translates into a diversity of standards and security approaches and resistance to the various Federally-mandated approaches that have been put forth since the late 1990s.

Second, many of these critical infrastructure sectors must secure both traditional information technology (IT) systems and operational technology (OT) or industrial control systems. IT systems typically function with widely-used software like Adobe Reader or Mozilla's Firefox browser. Even where more enterprise (organization-wide) applications like email or network print services are required, the software employed generally has a wide user base. One of the most challenging aspects of information assurance is that this software contains vulnerabilities – flaws or features that could enable a third party to take control of the software and the computer system it runs on. This is the entry point for an intrusion; threat actors need to be able to run malicious code on a computer in order to execute an attack. A vulnerability, if discovered by defenders, can be modified or slightly rewritten in order to render it harmless.

For complex software like that associated with industrial control systems (ICS), the design and testing process associated with such "patches" can be cumbersome. The embedded nature of ICS makes them difficult to access and modify while the user base for ICS application is generally much smaller than that of IT systems, leading to niche products with software that is esoteric and difficult to change. Industrial activities often require nearly continuous operation, so taking ICS equipment offline for regular updates and patching is challenging at best.[27] ICS software also tends to be designed for long run use, with equipment lifetimes of 15 years or more as opposed to IT software which can change substantially in far shorter cycles. Indeed, in its first decade of existence, the Firefox browser evolved through 30 commercial versions. In addition, while the software development community in the commercial IT sector has largely moved to embrace the process of regular patching, along with the responsibilities and overhead costs associated with it, ICS developers and operators still lag behind. This means that patching is not yet a standard feature of ICS software development and use, even though vulnerabilities continue to be discovered in ICS software.[28]

Workforce Training and Certification

Dealing with these problems requires implementing technical and policy solutions. That, in turn, requires a trained and certified workforce. Developing the skills and education applicable to the field can be a challenge, however. There is a shortage of skilled information assurance professionals, especially for Federal work, and disagreements over how to encourage more to enter the workforce as the continually evolving problem area has forced trade-offs between practical experience and technical expertise.[29]

A 2011 paper from the Cyber Security and Policy Research Institute at George Washington University found that, "the university model does not completely satisfy all cyber security education and training needs [as] traditional undergraduate and graduate programs tend to take several years to complete and… [these programs] face difficulties educating students about a rapidly changing field… Academic silos prevent collaboration and integration… [as] most academic programs have tended to build their own tools rather than exchange resources with others, and they tend to hold firm ownership over whatever they create."[30] This need for both skills and experience raises the question of whether to emphasize practical experience and "on the job" training (like airline pilots, who obtain thousands of hours of flight time in progressively larger aircraft) or to treat Information Assurance as a certified profession like medicine, where professional credibility comes from grueling coursework and testing.

A popular approach, which tempers but does not resolve this debate, is the use of certifications. Short class sequences and testing are used in lieu of university-based programs, but often require work experience and annual continuing education as well. Many "purists" in information assurance feel that certifications don't genuinely show skill level, only that the applicant can pass a test.[31] After all, certifications are a business and organizations have a vested interest in making them mandatory for specific jobs. A well-known example, DoD 8570, requires particular certifications in order for individuals to hold positions like an Information Assurance Manager or an Incident Handler.[32] Without these certifications in hand, individuals would be unable to work in any of the identified positions, regardless of previous experience.

But while certifications don't necessarily prove one's ability to perform a given task, they do at least show a standardized understanding of the issues covered by the certificate program and so provide an opportunity for non-profits and many commercial firms, like the SANS Institute (www.sans.org), to establish common bases of knowledge. This helps create expectations within the information assurance community and can, for better or worse, provide a rapid means for employers to screen potential candidates.

While there is a hiring crunch for information assurance professionals in the Federal workforce, it is possible that the problem will resolve itself. A 2014 RAND study concluded that much of the labor market shortfall could be explained by the natural lag time for educational institutions to respond to particular market demand. In the case of information assurance, the study suggests that, "The difficulty in finding qualified cybersecurity candidates is likely to solve itself, as the supply of [qualified individuals] currently in the educational pipeline increases, and the market reaches a stable, long-run equilibrium."[33] This would be further helped by continued growth in the commercial information assurance labor market.

The Role for Congress

Information Assurance focuses on ensuring the confidentiality, integrity and availability of information. It encompasses a cluster of topics, including the defense of information systems and networks against compromise, design of secure software, protection of critical infrastructure, and the challenge of educating and hiring qualified professionals. While not the most headline grabbing, these are bread and butter topics for security professionals and constitute the majority of defensive "cybersecurity" activity in organizations on any given day.

The challenge for policymakers is that there is little opportunity for direct intervention. The standards and techniques of network and system security are continually evolving. Federal requirements, like FISMA, can help to create consistent practices, but risk lowering the bar of "minimum acceptable" behavior and may embed inflexible requirements that are quickly outpaced by events. In information assurance, ameliorating vulnerabilities is largely a software design and patch management problem. There may be some opportunity for policy changes to better incentivize investment in secure software, but the response of vendors is driven by the reaction of their customers so a functioning marketplace already exists.

Critical Infrastructure Protection has benefited from the government's role as a trusted intermediary, and while it faces many of the same rapidly evolving threats as more conventional IT security, the operational technology space lags some years behind. As such, it is more likely to benefit from established standards for security behavior. One way to approach the problem, as the sixteen sectors identified as critical infrastructure are relatively varied, would be to take an existing risk mitigation strategy like the NIST Risk Management Framework, now being integrated by the Department of Defense, and to use this as a model to develop varied individual sector standards.[34] This could be done in conjunction with existing non-governmental organizations, a model of which exists with the North American Energy Reliability Corporation (NERC).

Workforce training and certification presents a more intriguing opportunity for lawmakers. The Federal workforce embodies a vast set of standards for education and training. Better defining the information assurance roles required by public sector organizations, and the accompanying knowledge, skills, and abilities that these positions require, could help standardize many training and certification pipelines. Either by using a single organization's workforce as a model or through some comprehensive review process, standardized roles would serve as a powerful voice in the discussion of how to constitute a professional information assurance labor pool.

At the end of the day, there are a variety of strategies for securing systems and networks in use by both public and private organizations. Developing and deploying software free from vulnerabilities, meanwhile, remains an ongoing and still largely unsuccessful struggle. Much of the difficulty in securing Critical Infrastructure systems is the diversity of private actors who own them and the challenge of patching software used in complex machinery and other operational technology. Finally, the workforce required to support all of these varied tasks and missions is still smaller than is necessary, in part because of a range of opinions on the best way to train and educate professionals in the field. Information Assurance is a highly technical cluster of topics within cybersecurity and an area where many traditional policy tools are likely to have little positive effect. It is important to understanding the larger issue space however and so comes as the first topic specific paper in our series.

This paper serves as the second in a five part series developed to explain cybersecurity and the four large topic clusters it covers.

Endnotes

1) "What is Security Analysis?" Imperial College London, , http://www.doc.ic.ac.uk/~ajs300/security/CIA.htm.
2) "Email Attack on Vendor Set Up Breach at Target," *Krebs on Security*, February 14, 2014, http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/.
3) Andrew Schneiter, Harold F. Tipton and Steven Hernandez, *Official (ISC)2 guide to the CISSP CBK*, Third ed. (Auerbach Communications, 2013).
4) Ines Brosso and Alessandro La Neve, "Adaptive Security Policy Using User Behavior Analysis and Human Elements of Information Security," in Elmer P. Dadios, ed., *Fuzzy Logic – Emerging Technologies and Applications* (InTech, 2012), http://cdn.intechopen.com/pdfs-wm/32882.pdf.
5) Aarti Shahani, "Hygiene, Honey Pots, Espionage: 3 Approaches To Defying Hackers," NPR, February 16, 2015, http://www.npr.org/blogs/alltechconsidered/2015/02/16/386669799/hygiene-honeypots-espionage-3-approaches-to-defying-hackers.
6) See, for example, "The Problem with Security Through Obscurity," http://www.diablotin.com/librairie/networking/puis/ch02_05.htm.
7) Shahani, "Hygiene, Honey Pots, Espionage."
8) Kelly Jackson Higgins, "Hacking Tool Lets A VM Break Out And Attack Its Host," *Dark Reading*, June 4, 2009, http://www.darkreading.com/risk/hacking-tool-lets-a-vm-break-out-and-attack-its-host/d/d-id/1131254?; Fahmida Rashid, "VUPEN Method Breaks Out of Virtual Machine to Attack Hosts," *Security Week*, September 5, 2012, http://www.securityweek.com/vupen-method-breaks-out-virtual-machine-attack-hosts.
9) Daniel M. White, "The Federal Information Security Management Act of 2002: A Potemkin Village," *Fordam Law Review* 79, iss. 1 (2011), http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4687&context=flr.
10) *Cybersecurity Act of 2012*, S. 2105 (112th Congress, 2011-2013), https://www.govtrack.us/congress/bills/112/s2105/text.
11) Sean B. Hoar, "Congress Passes The Federal Information Security Modernization Act of 2014: Bringing Federal Agency Information Security into the New Millenium," *Privacy & Security Law Blog*, December 18, 2014, http://www.privsecblog.com/2014/12/articles/cyber-national-security/congress-passes-the-federal-information-security-modernization-act-of-2014-bringing-federal-agency-information-security-into-the-new-millennium/.
12) "Risk Management Framework (RMF) Overview," NIST Computer Security Division, http://csrc.nist.gov/groups/SMA/fisma/framework.html.
13) Cisco Corporation, *Cisco 2015 Annual Security Report*, http://www.cisco.com/web/offers/lp/2015-annual-security-report/index.html.
14) "Information About the VBS.LOVELETTER Worm Virus," Microsoft Corporation, http://support.microsoft.com/kb/282832.
15) Georg T. Becker et al., "Stealthy Dopant-Level Hardware Trojans," Paper presented at the Cryptographic Hardware and

Embedded Systems (CHES) 2013 conference, Santa Barbara, California, August 21, 2013, http://sharps.org/wp-content/uploads/BECKER-CHES.pdf.

16) "National Vulnerability Database," https://nvd.nist.gov/.

17) Cisco Corporation, *Cisco 2015 Annual Security Report*.

18) Ibid.

19) "National Vulnerability Database."

20) Cisco, *2015 Annual Security Report*.

21) "Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities," *Federal Register*, October 22, 2013, https://www.federalregister.gov/articles/2013/10/22/2013-24256/department-of-defense-dod-defense-industrial-base-dib-voluntary-cyber-security-and-information.

22) "Understanding Threats with ThreatData," *Facebook* post dated March 25, 2014, https://www.facebook.com/notes/protect-the-graph/understanding-online-threats-with-threatdata/1438165199756960.

23) Michael Mimoso, "Facebook Threat Exchange Platform Latest Hope for Information Sharing," Kaspersky, February 11, 2015, http://threatpost.com/facebook-threatexchange-platform-latest-hope-for-information-sharing/110993.

24) Sara Sorcher, "Influencers: Obama's Info-Sharing Plan Won't Significantly Reduce Security Breaches," *Christian Science Monitor*, February 25, 2015, http://www.csmonitor.com/World/Passcode/2015/0225/Influencers-Obama-s-info-sharing-plan-won-t-significantly-reduce-security-breaches.

25) "CIP Standards," North American Electric Reliability Corporation, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

26) White House, Office of the Press Secretary, "Presidential Policy Directive – Critical Infrastructure Security and Resilience," February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

27) Bonnie Zu, Anthony Joseph, and Shankar Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems," *IEEE Conferences on Internet of Things, and Cyber, Physical and Social Computing*, 2011, http://bnrg.cs.berkeley.edu/~adj/publications/paper-files/ZhuJosephSastry_SCADA_Attack_Taxonomy_FinalV.pdf.

28) Brian Donohue, "Bug Hunters Find 25 ICS, SCADA Vulnerabilities," *Threat Post*, October 16, 2013, http://threatpost.com/bug-hunters-find-25-ics-scada-vulnerabilities.

29) Amber Corrin, "Is there a cybersecurity workforce crisis?" *FCW*, October 15, 2013, http://fcw.com/articles/2013/10/15/cybersecurity-workforce-crisis.aspx.

30) http://static1.squarespace.com/static/53b2efd7e4b0018990a073c4/t/54203f2de4b09a2902bc6f8a/1411399469318/costis_-_cybersecurity_workforce_development_directions.pdf

31) Jeff Atwood, "Do Certifications Matter?" *Coding Horror*, January 17, 2007, http://blog.codinghorror.com/do-certifications-matter/.

32) "DoD Approved 8570 Baseline Certifications," Information Assurance Support Environment, n.d., http://iase.disa.mil/iawip/Pages/iabaseline.aspx.

33) Martin Libicki, David Senty and Julia Pollak, *Hackers Wanted: An Examination of the Cybersecurity Labor Market* (RAND, 2014), http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf.

34) Department of Defense, "Instruction Number 8510.01: Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf.

UNDERSTANDING INFORMATION ASSURANCE

About The Defense Technology Program

A revolution is taking place in the nature of warfare. The proliferation of ballistic missiles and weapons of mass destruction has given rogue states and terrorist groups unprecedented access to potentially devastating capabilities, while space and cyberspace have emerged as distinct new arenas of strategic competition. The American Foreign Policy Council's (AFPC) work in these areas is aimed at helping U.S. offcials understand and respond to this new, and increasingly complex, threat environment.

For more information about the program, please contact Richard Harrison, Director of Operations and Defense Technology Programs at Harrison@afpc.org.

About AFPC

For over three decades, AFPC has played an essential role in the U.S. foreign policy debate. Founded in 1982, AFPC is a 501(c)(3) non-profit organization dedicated to bringing information to those who make or influence the foreign policy of the United States and to assisting world leaders with building democracies and market economies. AFPC is widely recognized as a source of timely, insightful analysis on issues of foreign policy, and works closely with members of Congress, the Executive Branch and the policymaking community. It is staffed by noted specialists in foreign and defense policy, and serves as a valuable resource to officials in the highest levels of government.

AFPC Mission Statement

The American Foreign Policy Council seeks to advance the security and prosperity of the United States by:

- providing primary source information, as well as policy options, to persons and organizations who make or influence the national security and foreign policies of the United States;
- arranging meetings and facilitating dialogue between American Statesmen and their counterparts in other countries; and
- fostering the acceptance and development of representative institutions and free market economies throughout the world in a manner consistent with the Constitution, the national interest, and the values of the United States.

AFPC STAFF

Mr. Herman Pirchner, Jr.
President
Mr. Ilan Berman
Vice President
Mrs. Annie Swingen
Director for External Relations
Mr. Jeff M. Smith
Director of South Asia Programs and Kraemer Strategy Fellow
Mr. Richard Harrison
Director of Operations and Defense Technology Programs

BOARD OF ADVISORS

Amb. Paula J. Dobriansky
Mr. Stephen A. Fausel
Hon. Newt Gingrich
Amb. Robert G. Joseph
Hon. Robert "Bud" C. McFarlane
Gov. Tom Ridge
Dr. William Schneider, Jr.
Hon. R. James Woolsey
Hon. Dov Zakheim

CONTACT

509 C Street NE
Washington, D.C. 20002
Telephone: 202.543.1006
Fax: 202.543.1007
www.afpc.org