

Introduction to Information Assurance

Module 1

Systems Security Management

Eller/ MIS
Copyright © 2015, Arizona Board of Regents

Module Objectives



- Information Assurance (IA)
- CIA Triangle
- IA Pillars
- National Security Directive #42
- Systems
- System Administration
- System Administrator's Role
- System Administrator's Day
- Next Module...

Systems Security Management



Eller/ MIS 
Copyright © 2015, Arizona Board of Regents

By the end of this module, you should have a clear understanding of:

- What Information Assurance is and why it is important.
- What the three focus areas of Information Assurance are.
- What the five pillars of IA are and why they are important.
- What National Security Directive #42 is and how it affects IA.
- What a system is and how systems are used.
- What a system administrator is and what their role is in Information Security.
- When to celebrate System Administrator's Day!


Information Assurance (IA)

- What is Information Assurance?
- National Security Agency
 - Central Security Service
 - NSA/CSS
- IA Directorate

Systems Security Management

Directorate of Information Assurance
Copyright © 2015, Arizona Board of Regents

Eller/ MIS 

What is Information Assurance (IA)?

Information Assurance is defined as the set of measures intended to protect and defend information and information systems by ensuring their confidentiality, integrity, availability, authentication, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. These measures are planned and executed by the Information Assurance Directorate (IAD) of the National Security Agency/Central Security Service (NSA/CSS).

The Central Security Service


The Central Security Service (CSS) is an agency of the U.S. Department of Defense, established in 1972 by a Presidential Directive to promote full partnership between the National Security Agency (NSA) and the Service Cryptologic Elements (SCE) of the United States Armed Forces. The CSS was created to provide timely and accurate cryptologic support, knowledge, and assistance to the military cryptologic community. The day-to-day work of the CSS is to capture enemy signals (radar, telemetry, radio/satellite communications) using the means of the involved service. For example, the Navy has special submarines for tapping undersea cables; the Air Force operates aircraft with sophisticated antennas and processing gear to listen to enemy radar and radio; and on the ground, the Army operates similar eavesdropping equipment.

The Information Assurance Directorate


The Information Assurance Directorate is a department within the NSA/CSS and is tasked with defining IA policy and implementation strategy.

Information Assurance (IA)

- Why is IA Important?
 - Why Should We Care?
 - Privacy
 - Theft
 - Identity
 - Espionage
 - Government
 - Corporate
 - Loss of Revenue
 - Malicious Intent
 - You Could Lose Your Job!



Systems Security Management

Eller/ MIS 

Copyright © 2015, Arizona Board of Regents

Why is Information Assurance Important?

Information Assurance is extremely important in the digital age. Just a quick search on the Internet will allow you to discover a tremendous amount of information about specific people, places, projects, or just about any topic you could conceive. The U.S. Government started their IA program to define Information Security as a priority. Agencies of the U.S. Government who handle sensitive information must follow strict guidelines in order to ensure this information remains secure. The risk of general data loss or the risk of losing sensitive information is far too great to not have plans in place to help mitigate the risks. While the Government has adopted this philosophy, corporations and other organizations are beginning to see the wisdom in adopting Information Assurance programs. According to the 2014 Verizon Wireless Data Breach Information Report there were 1,367 confirmed data breaches and over 63,000 security incidents in 2013 alone (Verizon, 2014, pg. 2). Information Assurance should now be considered a vital component of an organization's Information Security process, and here are some reasons why we should all care about IA:

Privacy: Most of us have likely seen at least one privacy policy in our lives. Credit card companies, hospitals, universities, and many other groups all provide privacy policy documents to those who use their services, so we, as consumers, understand how our personal information will be used and who it will or will not be shared with. So, how then do those organizations ensure the privacy of their customer's information? Adopting an Information Assurance program can significantly improve an organization's information security stance and help ensure the privacy of customer data.

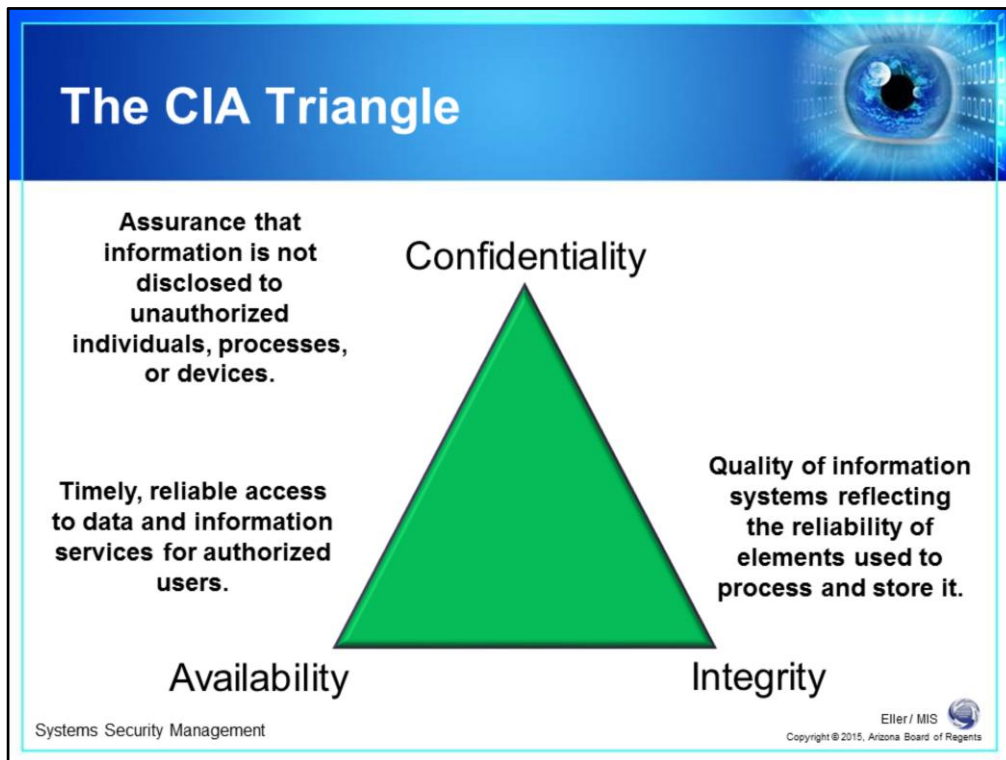
Theft: Information theft should be a major concern of everyone. According to the FTC's Consumer Sentinel Network Data Book for 2013, the CSN received over 280,000 consumer complaints related to identity theft in 2013 (Federal Trade Commission, 2014, pg. 4). Many criminal organizations are running identity theft rings, where they use hackers to breach networked computer systems so they can steal personal information and sell it on the black market. Often they sell this information multiple times in order to realize greater illicit revenues. Identity theft has become a billion-dollar a year business for these criminal organizations, and we need to find ways to prevent them from obtaining the personal information they need.

Theft of information is not limited to for-profit organized crime syndicates. Information espionage is also a very real threat to our information security. Governments on less-than-friendly terms with the United States likely all have covert actions underway to try and steal government secrets. Corporate espionage is also something to be concerned with as an employee at a competing corporation might be misguidedly and might try to obtain information from the competition to help his or her company move into a better position in the market. In the previously mentioned 1,367 data breaches during 2013, approximately 300 were directly related to cyber-espionage (Verizon, 2014, pg. 16).

Loss of Revenue: One major risk to a company could be a loss in revenues over a period of time. In late 2013 Target Corporation experienced a massive data breach that compromised 40 million credit and debit card accounts. This information was disclosed to customers on Dec. 19 and then on Jan. 10 they released news that hackers had also stolen personally identifiable information (PII) on as many as 70 million customers. Security experts estimated that the breach cost between \$400 million and \$450 million, which included expenses for fines from credit card companies and services for its customers like free credit monitoring ("Data-breach costs," 2014). This data breach was caused by malware infecting their Point of Sale systems and then exfiltrating the stolen information through their own networks to outside actors. The malware was defined later as BlackPOS, a variant that had been identified as early as January of that year (Krebs, 2014). As 2013 gave way to 2014 many, many more retailers reported breaches where customer information was compromised through malware affecting their Point of Sale systems: Home Depot (56 million records) (Krebs, 2014), Jimmy John's (Krebs, 2014), Michael's/Aaron Brothers (3 million records) (Anonymous, 2014), Neiman Marcus (Krebs, 2014), among others.

Malicious Intent: In April of 2013 the Syrian Electronic Army (SEA) claimed responsibility for hacking into the Twitter account for the Associated Press and reporting that there had been two explosions at the White House and that the President of the United States had been injured. Within three minutes of that tweet, the Dow Jones dropped about 150 points, resulting in a \$136 billion drop in equity market value. The market subsequently stabilized, but this shows that malicious intent can have some unforeseen consequences depending on reactions to erroneous information (Fisher, 2013).

As a System Administrator, System Manager, or even as high as a Chief Information (or Security) Officer, should a system (or multiple systems) be breached and sensitive data is lost, one or more people with the responsibility of making sure this type of event would not happen could find himself or herself without a job. Obviously the exact circumstances would need to be examined; however, it is not implausible if the breach is severe enough that at least one person in the chain might find themselves unemployed. Therefore it is in the best interest of the System Administrator to ensure his or her systems are as secure as possible to mitigate any potential risks of a breach.



The CIA Triangle

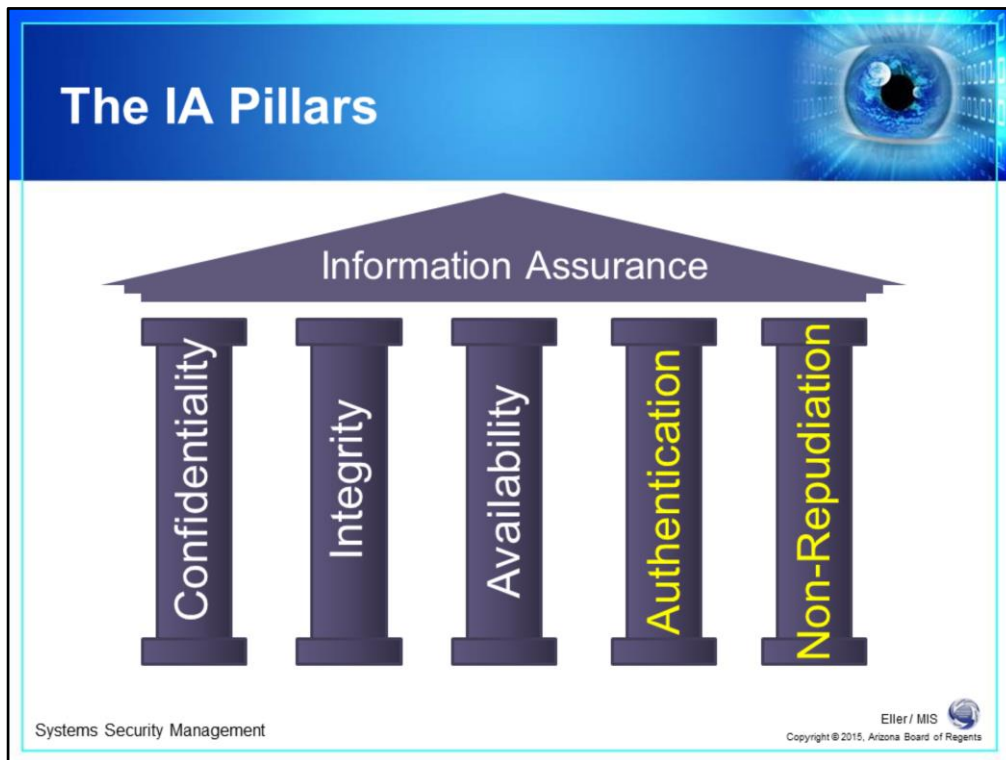
The CIA Triangle is comprised of three main areas: Confidentiality, Integrity, and Availability.

Confidentiality: Provides assurance that information is not disclosed to unauthorized individuals, processes, or devices. Anyone needing to secure information systems needs to make certain that access to sensitive information is only granted to those who specifically need access for their job function.

Integrity: Describes the quality of information systems, reflecting the reliability of elements used to process and store it. System Administrators must provide assurances that any information stored or transmitted has not been altered throughout the entire process of requesting, retrieving, and storing said information. Safeguards could include file-level security, encryption, digital signatures, or other means of validating the information has not been accessed or modified in any way as it moves from storage to the user and back to storage.

Availability: Providing timely and reliable access to data and information services for authorized users. People who need to access specific information systems or data need to access it when they need the information, not sometime in the future. System Administrators need to ensure information systems and data is available to users whenever they might need it.

At a bare minimum, anyone needing to secure information systems needs to ensure the CIA triangle is taken into consideration and appropriate safeguards are put in-place. These three areas also form part of the overall foundation of Information Assurance. These components are further defined as part of the IA Pillars.



The Information Assurance Pillars

There are five pillars designed to provide a solid foundation for Information Assurance. The first three comprise the CIA Triangle and the latter two work along side the triangle to further define IA.

Confidentiality – Simply put, confidentiality is just what you think it means. How do we keep personal information and other confidential data private?

Integrity – The term information integrity describes the trustworthiness and dependability of the information transmitted to users over a network.

Availability – How do we ensure data and specific information is available to those who need it, when they need it, without granting access to those who are not authorized to access it?

Authentication – Used to verify the identity of those users requesting access to specific data or information. Through authentication techniques, system administrators can ensure the proper users are granted access to what they need.

Non-Repudiation – This is the concept of ensuring that a party in a dispute cannot refute the validity of a statement or contract. In information security terms, non-repudiation is the act of including trusted digital signatures into data or information as it is transmitted over a network as a means of ensuring the data or information has not been altered in any way, and to verify that it was sent by the person claiming to have sent it. This concept will be discussed more in Module 8 – Authentication and Encryption.

Each of the pillars (confidentiality, integrity, availability, authentication, and non-repudiation) are designed to work together in order to create a solid foundation for Information Assurance.

National Security Directive #42



- Signed by the President on July 5, 1990
- Created the NSTISSC
 - Provide System Security Guidelines
 - Two Committees
 - Telecommunications Security
 - Information Security
 - Cryptography
 - Recommends Implementation of Protective Measures



Systems Security Management

Eller/ MIS
Copyright © 2015, Arizona Board of Regents

National Security Directive #42

National Security Directive #42 was signed by President George Bush Sr. on July 5, 1990. The directive “established initial national objectives, policies, and an organizational structure to guide the conduct of national activities directed toward safeguarding from exploitation, systems that process or communicate national security information; established a mechanism for policy development; and assigned responsibilities for implementation” (Center for National Security Systems, 2004). This directive officially created the National Security Telecommunications and Information Systems Security Committee (NSTISSC).

The National Security Telecommunications and Information Systems Security Committee

The NSTISSC was tasked with providing System Security guidelines to be used by the Federal Government’s various agencies. In order to accomplish this, the committee formed two additional, specific committees, each working on a different aspect of system security. One committee would focus on creating guidelines for telecommunications security and the other would focus on information security. In addition, the directive covered the use of cryptography as a means of helping to secure information as it is transmitted and stored. Finally, the committee was instructed to recommend the implementation of protective security measures as a means of further reducing the risk of system breaches.

Systems

- What is a System?

- Structure
- Behavior
- Interconnectivity

- IT Systems

- Servers
- Appliances
- Devices



Systems Security Management

Eller/ MIS
Copyright © 2015, Arizona Board of Regents

What is a System?

A system is something which performs a specific function. Systems can be something as simple as how a task is completed (mentally, physically, or technically) or systems can be technological in nature.

In general...

Systems have structure, defined by parts and their composition;

Systems have behavior, which involves inputs, processing and outputs of material, energy or information;

Systems have interconnectivity: the various parts of a system have functional as well as structural relationships between each other.

Notice that each attribute of a system can be seen as both technical or non-technical, meaning a system does not need to be related to Information Technology; however, for this course we will be focusing on IT systems.

There are several kinds of IT systems in use around the globe. Most commonly, when referring to IT systems one is likely referring to servers. Servers are used for a variety of purposes, but they all have one commonality: servers are used to serve one or more specific needs. Examples of servers would include e-mail servers, file servers, print servers, and web servers.

Appliances are another type of IT system. No, I am not talking about household appliances, but rather specific server hardware and software combinations sold together by a company in order to meet a specific need. For example, several vendors provide a Security Information Event Manager appliance that allows companies to aggregate event logs from various, disparate systems (such as routers, firewalls, Windows Domain Controllers, web filtering solutions, etc.) into one place and allow a single pane of glass for security analysts to have visibility into what's going on in the environment. Some of these systems include actionable intelligence features where events can be correlated into threats by observing behavior, actors (internal or external, privileged or non-privileged), and activities that correspond to actions. For example, by tying in the Active Directory users, HR systems, and physical access systems like a badge-reader, a SIEM can observe through various events logged that an employee who should only access a building during a typical work day, has just entered a restricted building in the middle of the night. This is just one example of an appliance, others might include anti-spam scanners, intrusion detection systems, or specific network services such as domain naming servers. These are all topics we will cover in later modules.

Network devices are another type of IT system. Networked devices are also used to serve a specific purpose, and more often than not, they are designed to allow for network communication. This would include network hardware such as routers, switches, wireless access points, or firewalls. Each of these items is used to facilitate communication throughout a corporate network; however, none are typically accessed directly by users. Think of network devices as similar to an electrical junction box. They allow for the job at hand without anyone giving them a second thought unless they stop working.

System Administration



- What is Systems Administration?
 - Management of One or More Systems
- What Kind of Systems are Managed?
 - Servers
 - Windows, Linux, Mac OS X, etc.
 - Network Devices
 - Routers, Switches, Wireless, etc.
- Now this Function Includes Security

Systems Security Management

Eller/ MIS
Copyright © 2015, Arizona Board of Regents

What is Systems Administration?

Systems administration is the practice of managing one or more IT-related systems. This can include managing physical, logical, and virtual aspects of IT systems. Physical aspects might include the installation of new hardware into a rack-based server room environment, replacement of failed hardware, or physically moving equipment from one location to another. Logical aspects might include the configuration of operating systems or other applications or network infrastructure and server design. Virtual aspects might be the creation and management of Virtual LANs (vLANs), Virtual Private Networks (VPNs), or Virtual Machines (VMs). Each of these aspects will be examined (and some will be worked with in a hands-on lab environment) throughout this course.

What Kind of Systems are Managed?

Usually, a System Administrator will manage a number of different system types, including servers running Windows, Linux, or the Mac OS X operating systems, and network devices such as routers, switches, and wireless access points. In the past, this was typically all a System Administrator would be tasked with; however, over nearly the past two decades, security has become a major focus of System Administration.

System Administrator's Role



- A person employed to maintain and operate a computer system and/or network.
- May be members of an Information Technology department.
- Usually charged with installing, supporting, and maintaining servers or other computer systems, and planning for and responding to service outages and other problems.

Systems Security Management

Eller/ MIS 
Copyright © 2015, Arizona Board of Regents

A System Administrator is a person who is employed specifically to maintain and operate one or more specific computer systems and/or a computer network. Someone in this role may be a member of an Information Technology department; however, this may not always be the case. In most organizations the System Administrator will be associated with an official IT department; however, in settings similar to a University, individual departments may find themselves with a need for a System Administrator and might hire a student directly to perform this role.

In general, a System Administrator will usually be charged with installing, supporting, and maintaining servers or other computer systems. This person will also be responsible for planning for and responding to service outages or other problems.

System Administrator's Role



- AKA: SysAdmin or Systems Manager
- Other Duties May Include:
 - Scripting or Light Programming
 - Project Management
 - Supervising
 - Training
 - Consultation Services
- Must Demonstrate a Blend of Technical Skills & **Responsibility**.

Systems Security Management

Eller/ MIS
Copyright © 2015, Arizona Board of Regents

A System Administrator is also known as a SysAdmin or Systems Manager. Other duties generally performed by a SysAdmin may include:

Scripting or Light Programming: In general, most SysAdmins will need to write basic programs for various purposes, usually to automate some specific task. For example, a SysAdmin might write a small script which executes when you logon to your computer. This script might be used to provide access to specific network drives.

Project Management: While a SysAdmin typically is not an official "Project Manager," a SysAdmin can, in many cases, be responsible for managing system-related projects. Usually this occurs in organizations who do not have specific Project Managers defined in the IT department, and in these instances, the SysAdmin may also be the person performing the actual project work. For example, the installation and configuration of a new server for a specific purpose.

Supervising: Depending on the size of the organization, a SysAdmin may have one or more personnel working in IT specifically designated to systems work. In general, a primary SysAdmin or Systems Manager will be designated to manage the additional SysAdmins. While it is not a requirement (by any means) that the Manager be a SysAdmin himself, this does help with understanding the needs of his or her employees and this person can also understand very technical details.

Training: A SysAdmin should be one of the main people in an organization who thoroughly understands existing systems and applications. From a technical standpoint, this person is therefore the most qualified person to provide specific training to other SysAdmins or Users. Speaking in generalities, many IT workers (note, not all IT workers) may not be able to communicate effectively with non-technical people. For this reason, many organizations will hire someone with experience training others who will work with the SysAdmin to learn the specifics of a system or application in order to train others. In a pinch, however, the SysAdmin may fill this role.

Consultation Services: This is not to say the SysAdmin will be consulting with outside interests. More specifically, the SysAdmin will be required to consult with the organization's existing Help Desk support teams to diagnose systems, network, or other technical issues. There will be times where the Help Desk is simply unable to solve a user's problem and will need assistance from someone with more technical skill.

The bottom line is a SysAdmin must demonstrate a blend of technical skills and responsibility. Responsibility is extremely important, especially since it is a Systems Administrator who must work to ensure all of his or her systems provide Information Assurance for the organization.

System Administrator Day!

- Last Friday of July
 - July 31, 2015! 16th Annual SA Day!
- The SysAdmin's Price List



Systems Security Management

Eller/ MIS
Copyright © 2015, Arizona Board of Regents

System Administrator Appreciation Day is celebrated on the last Friday of July. According to the “official” SysAdmin Day website, “a SysAdmin is a professional, who plans, worries, hacks, fixes, pushes, advocates, protects and creates good computer networks, to get you your data, to help you do work -- to bring the potential of computing ever closer to reality” (System Administrator Appreciation Day, 2010).

This year on “Friday, July 31, 2015, is the 16th annual System Administrator Appreciation Day. Consider all the daunting tasks and long hours (weekends too.) Let's be honest, sometimes we don't know our System Administrators as well as they know us. Remember this is one day to recognize your System Administrator for their workplace contributions and to promote professional excellence. Thank them for all the things they do for you and your business” (System Administrator Appreciation Day, 2010).

To help relieve some stress (and add some humor to the mix) check out the “Official SysAdmin’s Price List” (<http://home.chpc.utah.edu/~davidr/humor/pricelist.html>) and cartoon. Remember to sing a song to your SysAdmin(s) on their special day!

Next Module...



- Information Assurance in Government
 - NSTISSP #11
 - INFOSEC & COMSEC
 - Defense in Depth
 - Media Handling
 - EMSEC, TRANSEC, & TEMPEST
 - Information States
 - Rainbow Series

Systems Security Management

Eller/ MIS 
Copyright © 2015, Arizona Board of Regents

In the next module we will discuss the following:

- National Security Telecommunications and Information Systems Security Policy #11
- Information Security (INFOSEC) and Communication Security (COMSEC)
- Defense in Depth
- Media Handling
- Emission Security (EMSEC), Transmission Security (TRANSEC), and the TEMPEST Program
- Information States
- The Rainbow Series

References



- Anonymous Contributors. (2014, April 17). Michaels/Aaron Brothers breaches compromised 3 million records. *The State of Security: Tripwire*. Retrieved from <http://www.tripwire.com/state-of-security/top-security-stories/michaelsaaron-brothers-breaches-compromised-3-million-records/>.
- Center for National Security Systems. (2004, December 14). National Directive on Security of National Security Systems. Retrieved from <http://www.cnss.gov/Assets/pdf/CNSSD-502.pdf>.
- Data-breach costs take toll on Target profit. (2014, February). The Associated Press. Retrieved from <http://www.cbsnews.com/news/data-breach-costs-take-toll-on-target-profit/>.
- Federal Trade Commission. (2014, February). The Consumer Sentinel Network Data Book for January – December 2013. Retrieved from <http://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2013/sentinel-cy2013.pdf>.
- Filderman, E. (2000). SysAdmin Price List. Retrieved from <http://www.contrib.andrew.cmu.edu/~moose/sysadmin/pricelist.html>.
- Fisher, M. (2013, April 23). Syrian hackers claim AP hack that tipped stock market by \$136 billion. Is it terrorism?. *The Washington Post*. Retrieved from <http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/>.
- Joint Chiefs of Staff. (1999, August). Information Assurance: Legal, Regulatory, Policy and Organizational Considerations (4th Edition). Retrieved from <http://www.au.af.mil/au/awc/awcgate/c/s/ia.pdf>.
- Krebs, B. (2014, January). Hackers steal card data from Neiman Marcus. Retrieved from <http://krebsonsecurity.com/2014/01/hackers-steal-card-data-from-neiman-marcus/>.
- Krebs, B. (2014, February). These guys battled BlackPOS at a retailer. Retrieved from <http://krebsonsecurity.com/2014/02/these-guys-battled-blackpos-at-a-retailer/>.
- Krebs, B. (2014, July). Sandwich chain Jimmy John's investigating breach claims. Retrieved from <http://krebsonsecurity.com/2014/07/sandwich-chain-jimmy-johns-investigating-breach-claims/>.
- Krebs, B. (2014, September). Home Depot: 56M cards impacted, malware contained. Retrieved from <http://krebsonsecurity.com/tag/home-depot-breach/>.
- NSA Information Assurance FAQs. Retrieved from <http://www.iwar.org.uk/cip/resources/nsa/information-assurance-faq.htm>.
- SysAdmin (rm -rf /). (2008). What is a System Administrator? Retrieved from <http://www.zolty.eu/>.
- System Administrator Appreciation Day. (2010). Retrieved from <http://www.sysadminday.com>.
- Verizon. (2014). Verizon 2014 Data Breach Investigations Report. Retrieved from <http://www.verizonenterprise.com/DBIR/2014/>.
- White House, The. (1990). National Security Directive #42. Retrieved from <http://fas.org/rp/offdocs/nsd/nsd42.pdf>.