

MICROS, GEORGE

Assignment # 1

CS 565: INTRODUCTION TO INFORMATION ASSURANCE  
INSTRUCTOR: RAVI MUKKAMALA, PH.D  
SPRING 2015

# 1 QUESTION 1

## 1.1 The Question

List four (or more) issues addressed by Information Assurance that are often not addressed by Information Security.

## 1.2 The Answer

Information assurance is the collections measures and methods that protect information and information systems from the risk of comprising the availability and integrity of information. Information security refers specifically to the protection of information. Therefore, information assurance supersedes information security and can be thought of as an abstraction and container for it. Some of the issues addressed by information assurance, but not by information security are:

- Risk and threat assessment:  
The overall assessment of systems vulnerabilities and the resources available for attacks as well as the systematic testing for unexpected dangers. The assessment of risks associated with a particular security strategy and the threats of new attacks being developed.
- Management and strategy of security:  
The organization and mitigation of security procedures that will provide the best possible security protection against attacks. The prioritization of the risks and vulnerabilities that need to be addressed
- Standards and policies:  
Providing security compliant with standards and laws. Also, establishing policies that will help prevent attack trends and provide uniform security across different modalities, i.e. desktop, laptop, mobile, web-based.
- Training and education:  
The development of training programs and the dissemination of the resources necessary to provide knowledge and information of the subject matter of security. This may include but is not limited to the vulnerabilities of new hardware, attack strategies and attack resources.
- Security system development  
The design and review of plan to create hardware and software provides a higher level of security. Developing systems that reduce the number of innate vulnerabilities and access points and can provide resistance to a broad range of threats and attacks.
- Operational mediation:  
Overseeing security procedures and tasks continually to provide long term security against potential vulnerabilities that develop over time. The human factor is especially important. Maintaining a schedule of updates and changes that can prevent against the vulnerabilities of human users.

## 2 QUESTION 2

### 2.1 The Question

List four (or more) conditions that warrant methodologies for enforcing information assurance at both corporate and governmental organizations.

### 2.2 The Answer

The necessity for information assurance is ever-present. In both a corporate and government setting it is necessary to maintain a certain level of security. However there are situations that merit specific methodologies and plans for enforcing information assurance.

- National security:

The field of intelligence and counter-intelligence on a national setting is vital. Its importance is so great that it cannot rely on simply defending against attacks as they occur, but rather actively developing prevention systems for a broad spectrum of attacks.

- Financial information:

The introduction of technology has made financial transaction extremely easy, but also vulnerable to many attacks that users cannot protect against on their own. Online banking cannot afford to wait for attacks to occur and attempt to apprehend attackers. A prevention system that is real-time and dynamic must be in-place to detect false transaction swiftly.

- Product security:

Many of the products consumed today are in the form of software, i.e. mobile apps, software packages, widgets. Many of these use personal use information in their features that require protection. Any application vulnerability on cellphones can affect millions of users and cost a company its livelihood and public image. It is necessary for a corporation to have developed a set of policies that it will follow and adhere to across products to ensure that user information is secure.

- Medical records:

Along with financial records and personal information medical records are also electronics. Violation of medical records can have adverse consequences for patients.

- Corporate competition:

Some corporations may attempt to launch an attack on competitors to infiltrate their corporate secrets or make their software more vulnerable.

## 3 QUESTION 3

### 3.1 The Question

Briefly write about the perception of information warfare and its outcomes. You may use any web resource but make sure to list the reference.

## 3.2 The Answer

The art of deception has been used throughout history and has its place in warfare. In Operation Fortitude was one such military deception used during World War II to distract axis forces from the Normandy landings. the perception of information warfare can be a very useful tool in the information security where there are many different aspects of an attack to protect against. Creating the impression of a specific attack against an opponent will force them to increase their fortification of that part of their security system drawing resources and attention from other vulnerabilities that then have. In a defensive situation creating the perception that a security system is vulnerable to a specific type of attack will attract attackers towards it and force them to develop attack against it. In this situation resources are being used to develop a specific attack and the attackers can be tracked and identified based on their actions. This is a way to weed out attacks and detect attacker that may have been unknown previously. The perception of information warfare is very important in the strategy, planning and management of information assurance.

[http://en.wikipedia.org/wiki/Operation\\_Fortitude](http://en.wikipedia.org/wiki/Operation_Fortitude)

## 4 QUESTION 4

### 4.1 The Question

From the web, list five different job openings (with any job descriptions) relevant for information assurance professionals. Provide the URLs of the listings.

### 4.2 The Answer

- Information Assurance Specialist

Fabricates, installs, maintains, and repairs electronic, mechanical, and/or other types of components and equipment.

[http://www.resumeware.net/gdns\\_rw/gdns\\_web/job\\_detail.cfm?key=192161&referred\\_id=158](http://www.resumeware.net/gdns_rw/gdns_web/job_detail.cfm?key=192161&referred_id=158)

- Information Operations Specialist, Cyber Security

Contractor will assist Command Information Assurance Manager at Navy Munitions Command / Navy Munitions Command Pacific (NMC/NMCPAC), a shore command under the NMCI/NGEN/ONE-NET structure (without a network) with 45 locations worldwide. Contractor will assist with the Cyber Security Program of the Commands classified and unclassified systems, and will be responsible for ensuring Command compliance with all applicable DOD and DON program directives and requirements.

<https://ch.tbe.taleo.net/CH08/ats/careers/requisition.jsp?org=SYSTEK&cws=1&rid=447&source=Indeed>

- Information Assurance Analyst Job

Provide network security support for a large government client. Support the client in operational IA planning and contribute to the production and integration of IA compliant technologies in a network-centric environment. Provide overarching expertise for the C&A process, assist with the revision of the entire end-to-end C&A process, review C&A package submissions to ensure system and network architectures and technical and non-technical

operating features, adequately protect and defend against unauthorized access, conduct IA compliance and C&A documentation validation assessments for legacy applications, systems and networks, develop or expand existing, C&A, and IA documentation to ensure complete documentation exists in accordance with DoD C&A and IA policy, perform Certification Authority (CA) risk assessments to evaluate systems risks, and provide written risk assessment reports, including overall risk analysis reviews and recommendations to the client.

[http://careers.boozallen.com/job/Norfolk-Information-Assurance-Analyst-Job-VA-23501/243043700/?feedId=708&utm\\_source=Indeed](http://careers.boozallen.com/job/Norfolk-Information-Assurance-Analyst-Job-VA-23501/243043700/?feedId=708&utm_source=Indeed)

- Information Assurance Security Engineer

The Security Engineer (SE) reports to the Det-Chesapeake team lead and will independently lead and/or conduct enterprise and system-level ITSEC engineering tasks

<https://careers-goeis.icims.com/jobs/2302/information-assurance-security-engineer/job?mobile=false&width=930&height=500&bga=true&needsRedirect=false>

- Information Assurance Engineer

ManTech, a well-respected industry leader, is actively seeking talented professionals eager to support mission critical programs and solve some of the toughest problems critical to our great Nations security.

<https://sjobs.brassring.com/TGWEbHost/jobdetails.aspx?jobId=1216810&PartnerId=10696&SiteId=45&type=search&JobReqLang=1&recordstart=1&codes=INDD>