Never to Early to Learn
Careers in Information Assurance/Information Security and Digital Forensics

What is Information Assurance?

Nearly every aspect of society today depends on computer systems: transportation, communication, banking, and manufacturing, to name a few. However, this infrastructure of computerized systems is increasingly under threat of attack from viruses, worms, hackers, and information thieves. Every business wants to be assured that their information is safe.

Businesses and government agencies need to protect their systems. A computer worm or virus can cause delays and cost money, but information theft can be disastrous. Business information that is stolen from computers can be used to steal money from private accounts or reveal trade secrets. It has even been used to blackmail businesses and individuals. If information is obtained from government sites, the results can have even more dire consequences.

Information assurance refers to the people, hardware, software, policies, and procedures that protect information systems. Definitions of information assurance list five elements it is meant to protect:

- that the information is available when needed
- that the integrity of the information is sound
- that its authenticity can be verified
- that it is kept confidential
- that proof of the integrity and the origin of the data can be provided

One of the fastest growing fields in computer technology is in information assurance. Although the mission of information assurance has been around for more than 50 years, the development of the computer and, more recently, the ever-increasing use of computer systems for the transfer and storage of information have changed the environment and the necessity for improving the protection of sensitive information.

What Does an Information Assurance Graduate Do?

Information Assurance is the process of protecting data from misuse by people inside or outside a business or organization. This misuse might come from a hacker or corporate spy, but it can also come from a current or former employee who might want to sabotage a computer database. It is the job of the information assurance professional to create a system designed to prevent this from happening.

Because no system is perfectly secure, it is also the role of the information assurance professional to help create a system of checks and quality controls that allows an organization to trace transgressors. Technology constantly changes, and with any online transaction there is always a risk of a security breach. Therefore, the job of information assurance is never-ending.

The information assurance professional must be knowledgeable in several aspects of computer technology. One of the most fundamental areas of expertise is computer network design and infrastructure. In creating or working with a network design, the professional must understand the needs and business objectives of the client. Some networks are local, to be used only within the organization itself. Other networks are widespread, used by customers across the country or around the world. With this in mind, the network is designed to accomplish the goals of the organization while protecting the core information.

Cryptography is included as a part of this security design. Cryptography has long been used as a means to translate data to a form that is nearly impossible to read without the correct key. This process typically uses mathematical

algorithms to encrypt the data. Cryptographic mechanisms are regularly used to control access to such things as a shared disk drive or even pay-per-view television channels.

Information assurance professionals must also be knowledgeable in ***intrusion detection and control***, which is the art of discovering if an inappropriate activity has occurred. Intrusion detection is not a security system. Instead, it inspects all inbound and outbound network activity to identify suspicious patterns that may indicate someone is attempting to break into or compromise a computer system.

Another aspect of the information assurance process involves creating a system that provides user ***authorization and authentication.*** This is granting or denying access to a network resource. Authentication makes certain that users are who they claim to be. Authorization allows the user access to various resources based upon proof the user's identity.

If an organization's data center is compromised, the information assurance process is responsible for data integrity and recovery. The data can be compromised by human error, system crashes, software bugs or viruses, and even natural disasters such floods or fires. Regardless of the size of the organization, the information is valuable and must be recovered whenever possible. This can be accomplished through backup systems, or with special software products designed to help salvage data or damaged disks and tapes.

The ***information assurance specialist*** is involved with all these technical aspects, but they are involved in the organizational functions of creating a security policy for the organization and making sure that people within the organization adhere to it. They must be familiar with national and state laws that regulate privacy concerns and electronic commerce.

Trends in Information Assurance Careers

The federal government and the Department of Homeland Security have made information protection a matter of national security, and that is not limited to just the government information. Access to private data and sensitive business details could create security problems. Therefore, despite any downturns in the information technology economy, the market for information assurance and other computer security personnel is likely to remain strong. A shortage of qualified people to take on the roles of information assurance has led several colleges to create new programs or specialties dedicated to helping meet the demand.

Career Education in Information Assurance

Undergraduate and Graduate Degree and Certificate Programs

Anyone with an interest in computer technology may want to look into a college computer science program, or engineering degree or even the specific cybersecurity/IS/IA degree programs that are currently. These programs may have a grade point average or SAT score requirement. Programs that offer a master's degree generally want students who have completed an undergraduate degree in computer science/engineering/IA/IS/cybersecurity or something similar.

A broad knowledge of computer hardware and software is important, so high school students should take as many computer classes as possible. Mathematical and analytical skills are useful traits in information assurance. Problem-solving courses that include math and algebra will be beneficial, as will classes that emphasize communication skills such as writing and public speaking because of the need to pass along vital information to others.

Is an Advanced Degree Needed to Work in Information Assurance?

The current demand for specialists with information assurance skills means graduates with a bachelor's degree in computer science and experience can find employment. However, information assurance jobs typically demand

knowledge above and beyond a general computer background. Some programs offer certificates in the specialty, which is helpful. However, more schools are offering programs at the master's degree level.

What can you do with a College Degree in Information Assurance?

Career options for aspiring information assurance professionals

Information assurance positions are among the most demanding of the computer specialties. Employers prefer people who have at least a bachelor's degree, possibly with a concentration in information assurance. In addition, a broad background and extensive experience is generally helpful. Some employers ask for a graduate degree as well.

Individuals interested in information assurance jobs must be able to communicate effectively with team members, other staff, and customers. They can be involved with a number of tasks simultaneously, so they need the ability to concentrate and pay attention to detail. Some employers, especially government agencies, might require a security clearance before hiring someone for such a sensitive position. A background check is required in such circumstances, so it is important to have a clean record.

Information assurance jobs at major firms are rarely entry-level positions. Often, the people who fill these jobs will have years of computer experience and advance into the position or take classes to become more familiar with the requirements. As education catches up with demand, students might have more of an opportunity to move into these positions at smaller companies. As they gain experience, they can move into the more demanding and higher-paid positions.

Since the late 1990s, the federal government and private industry have worked together to fight attacks on the nation's computer infrastructure, including its financial infrastructure. Computer security has only become more important in recent years as more institutions and government agencies pay even more attention to security issues. Federal and state governments are employing more people in information assurance capacities. Here are just a few of the major U.S. agencies.

Department of Defense

- Defense Department controls all branches of the U.S. military. It operates the Computer Network Defense whose function is to protect, monitor, analyze, detect, and respond to unauthorized activity within the department's information systems and computer networks. It employs information assurance principles and that includes a plan of action against an information threat.

- The department established the Defense-wide Information Assurance Program (DIAP) in January 1998 to plan, monitor, coordinate, and integrate information assurance activities across the DoD. The agency serves as a facilitator for program execution by the combatant commanders, the various branches of the military all defense agencies. DIAP's objective is to provide a "big picture" that identifies redundancies, incompatibilities, and general deficiencies in informational assurance capabilities.

National Security Agency

- The National Security Agency/Central Security Service coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produce foreign intelligence information. The high technology organization bills itself as "America's cryptologic organization." As a leader in the fast-changing world of communications and data processing technology, the NSA Information Assurance Directorate is charged with providing solutions to keep U.S. information systems safe.

- The directorate's mission is to detect, report, and respond to cyber threats; make encryption codes to pass information securely between computer systems; and embed information assurance measures into the Global Information Grid. This challenge involves building secure audio and video communications

equipment, making tamper protection products, and providing trusted microelectronics solutions. The NSA often teams with other agencies across government, industry, and academia.

Department of Commerce

- U.S. Department of Commerce oversees nearly everything connected with promoting economic growth. It has several offices related to the regulation, development, and promotion of domestic and international trade. Its many tasks include gathering economic and demographic data for business and government decision-making, issuing patents and trademarks, and helping to set industrial standards.

- The department has implemented an Information Technology Security Program whose role is to assure that unclassified and classified national security IT systems are performing as specified; that unclassified and classified information is adequately protected; that the integrity of data and software is maintained; and, that unplanned disruptions of processing will not seriously affect the department's many functions.

Department of Energy

- The DOE is responsible not only for the nation's energy policy, but it also oversees our nuclear safety. This includes the nation's nuclear weapons program, nuclear reactor production for the United States Navy. The department has established a cyber-security program to protect the information and systems as the department increasingly relies upon new technology.

Department of Homeland Security

- This Cabinet department was created soon after the terrorist attacks of September 11, 2001, and is charged with preventing any further attacks on the domestic front. It has been a chief sponsor of many information assurance programs around the country through its university and fellowships program.

Government service is but one direction for information assurance specialists. A survey indicated that 85% of the firms and agencies surveyed had detected computer security breaches during the previous year. Of the more than 500 firms, government agencies, financial institutions, medical institutions, and universities surveyed, $455 million was lost because of computer crime in that year. Because of all this activity, businesses of all types need computer specialists.

Information assurance professionals might start in other computer-related careers before advancing up the later. Other jobs require similar skills, and some simply provide a solid background in computer protection. A few of these job titles and responsibilities include:

- **Computer security specialist.** Many basic duties of a computer security specialist might overlap with those of an information assurance specialist. Security specialists in some organizations plan, coordinate, and implement the organization's information security. Their responsibilities could include educating users on computer security, installing security software, monitoring the network for security breaches, and responding to hacker attacks. Security specialists might also be asked to gather data and evidence for prosecuting a crime. They might work for smaller companies.

- **Database administrators** set up computer databases, organize and store data, and test and coordinate changes to the databases. If they are responsible for the design and implementation of the database, they might also be asked to plan and coordinate its security measures.

- **Computer and information scientists** apply their expertise and innovative techniques to more complex problems of computer software and hardware. They most often work as theorists, researchers, or inventors. They apply a higher level of theoretical expertise and innovation and develop solutions to complex problems relating to computer hardware and software. Those with backgrounds in security might work as security specialists for data recovery situations or in installing custom security software.

- **Computer support specialists** do not generally have the training and background needed for information assurance. However, it can be a good launching pad for future specialists. Working in technical support or as help-desk technicians provides outstanding experience in learning various hardware, software, and systems. Support specialists often work as troubleshooters in a business or other organization.

- **Network systems and data communications analysts** design and evaluate network systems. Working day to day with network modeling, analysis and planning offers some of the fundamental background needed for advancement into information assurance. They might also be responsible for web site design and creation, including security issues.

- **The computer systems administrator** installs and manages an organization's network or Internet system. They are responsible for maintaining network hardware and software, analyzing problems, and monitoring to make certain it is available to the system when needed. This person is often asked to plan and implement the organization's network security measures. In some organizations, computer security specialists are responsible for the information security.

- **Computer and information systems managers** are more directly involved in overseeing others who work in the system such as network analysts and computer programmers. This means they must determine the personnel and equipment needs of the organization. They are usually in charge of coordinating such activities as upgrading the hardware and software, developing computer networks, and programming the system.

- **Management information systems directors** manage the information system, which includes applications, networks, personal computers, and hardware and software. This typically involves the planning, organizing and daily support of the system under the supervision of the chief information officer. They might oversee user services such as an organization's help desk.

- **Project managers** develop requirements, budgets, and schedules information technology projects. They work with internal and external clients, vendors, consultants, and computer specialists to coordinate projects from development through implementation. They have become more involved in projects to upgrade information security.

- **Local area network and wide area network managers** can be in charge of everything from setting up the network through managing and updating it. The configuration of the hardware and software used to create the connections falls under this job's function. The larger the network, the more security issues can become a problem. As is true with most of these positions, the job provides extensive knowledge of system setups and the hardware used to operate it. The managers know the network inside and out.

Although all businesses need some type of computer security protection, not all can afford, or need, to hire a full-time information assurance specialist. Therefore, consultants with a detailed knowledge of computer-security programs are in demand. Mid-size companies who deal with online transactions or handle confidential personal information might use these entrepreneurs.

Universities, which have huge amounts of sensitive information stored, are among the prime organizations in need of information assurance professionals. But, they also need professors and researchers to teach and perform research in this area, especially since programs and course offerings have expanded in recent years.

Did You Know?

- As many as 11 million people have victimized by identity theft in a given year
- Between 200 and 300 computer viruses are created each month
- Online thieves who have obtained credit card numbers and other personal information have netted about $500 million from victims in the United States

Licensing and Certification

A license is not needed for a career in information assurance. However, certifications in some technologies might be required. Vendors, some colleges, and others often provide these certifications. Many employers, especially government agencies or government contractors may require background checks. Some government agencies may also require a security clearance.

For more information about information assurance:

- The Department of Defense Information Assurance Support Environment http://en.wikipedia.org/wiki/Department_of_Defense_Information_Assurance_Certification_and_Accreditation_Process
- The National Security Agency/Central Security Service Information Assurance Technical Framework Forum http://www.nsa.gov/
- NSA Kids Page http://www.nsa.gov/kids/index.htm
- DISA http://www.disa.mil/

Computers & Information Technology
Cybersecurity Specialist
Source: http://www.geteducated.com/career-center/

Outlook & Growth
This career is expected to grow 27 percent—faster than average—through 2016. An increase in computer security jobs is expected as technology continues to advance and become more affordable. More businesses will add computers and will need specialists to make their networks secure.

In addition, use of the Internet by businesses should increase the demand for computer security specialists. Some specialists will work inside consulting firms dedicated exclusively to computer security issues.

Salary & Wages
Those in executive roles—with titles such as chief information security officer, chief security officer or security manager—earned $106,326 on average. Those in more technical roles (security engineer, security penetration tester or web security manager) earned an average of $75,275.

What is a Cybersecurity Specialist?
Computer security specialists work with companies to build secure computer systems. They question managers and staff about their current security methods. They find out what information the company wants to protect. Specialists also learn what information employees should be able to access. Computer security specialists use their findings to plan the security system. They regularly train staff on how to use security software and properly use computers to prevent any problems.

Some computer security specialists write rules and procedures for employees to follow. In some companies, specialists coordinate security for vendors and customers in addition to employees. Specialists evaluate security breaks and determine if there are problems or errors. If there is a problem, specialists track where the break came from and shut off the access point.

Education & Degree Path
There are many ways to become a computer security specialist. Many employers prefer to hire people with some formal college education. An AS or AAS or BS degree in computer science, engineering, or information systems are all excellent preparation for this occupation. Another route is to major in your area of interest and minor in one of these degrees.

Bachelor's degrees in computer security—some also refer to as cybersecurity or information assurance programs—are also available online.

An important part of preparing for this field is learning the latest technology. Some people learn through classes and others teach themselves.

Certification: As with other computer specialties, you can receive certification in certain products or groups of products, which can increase your appeal to employers.

Entering the Field: Many security specialists learn their skills on the job. They are paired with an experienced specialist who teaches them the job. This type of training can take between one and two years. The military has become a leading trainer in this specialty area. If you have skills and employment in any technical aspect of computers—repair, database and office systems—you can retrain to specialize in cybersecurity.

Career Changers: Many enter this field after working at a related computer specialty, such as programming or web mastering or network administration. You can re-tool quickly by earning a certificate or taking courses in cybersecurity or information assurance.