Question	Answer	Additional Link
What is Information Security?	**Information security** means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.[1] The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms. Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer.	http://csrc.nist.gov/groups/SMA/ate/index.html http://csrc.nist.gov/groups/SMA/sbc/workshops.html#03 http://en.wikipedia.org/wiki/File:Information_security_components_JMK.png
What is a bot or a botnet?	A 'bot' is a type of malware which allows an attacker to gain complete control over the affected computer. Computers that are infected with a 'bot' are generally referred to as 'zombies'. There are literally tens of thousands of computers on the Internet which are infected with some type of 'bot' and don't even realize it. Attackers are able to access lists of 'zombie' PC's and activate them to help execute DoS (denial-of-service) attacks against Web sites, host phishing attack Web sites or send out thousands of spam email messages. Should anyone trace the attack back to its source, they will find an unwitting victim rather than the true attacker. **Botnet** is a jargon term for a collection of software robots, or bots, that run autonomously and automatically. The term is often associated with malicious software but it can also refer to the network	http://en.wikipedia.org/wiki/Botnet http://csrc.nist.gov/groups/SMA/sbc/workshops.html#03 http://www.honeynet.org/papers/bots/ http://gcn.com:80/articles/2009/08/31/security-threats-invasion-of-botnets.aspx

	of computers using distributed computing software. While botnets are often named after their malicious software name, there are typically multiple botnets in operation using the same malicious software families, but operated by different criminal entities.[1] While the term "botnet" can be used to refer to any group of bots, such as IRC bots, this word is generally used to refer to a collection of compromised computers (called Zombie computers) running software, usually installed via drive-by downloads exploiting Web browser vulnerabilities, worms, Trojan horses, or backdoors, under a common command-and-control infrastructure.	http://www.honeynet.org/node/54
What is malware?	Malware, or Malicious Code, is a catch-all term used to refer to various types of software that can cause problems or damage your computer. The more common classes of program referred to as malicious code are viruses, worms, Trojan horses, macro viruses, and backdoors.	http://technet.microsoft.com/en-us/library/dd632948.aspx
What is a denial of service?	A denial of service (DoS) attack floods a network with an overwhelming amount of traffic, slowing its response time for legitimate traffic or grinding it to a halt completely. The more common attacks use built-in "features" of the TCP/IP protocol to create exponential amounts of network traffic.	http://csrc.nist.gov/publications/nistbul/itl99-05.txt http://csrc.nist.gov/groups/SNS/security-risk-analysis-enterprise-networks/
What is Phishing?	Phishing is a type of attack aimed at obtaining a user's personal or confidential information. It typically involves some sort of spam email designed to lure a user to a spoofed web site.	http://netsecurity.about.com/od/p/g/def_phishing.htm http://lp.tippingpoint.com/phishing1.html?gclid=CNvi6uym5ZwCFeNB5godu0mzGQ
What is Spam?	Spam is the term used to describe unwanted or unsolicited email. It is generally sent in bulk to millions of email addresses at once and frequently contains other security concerns such as viruses, worms or phishing attacks.	http://netsecurity.about.com/od/s/g/def_spam.htm http://en.wikipedia.org/wiki/Spam_(email)

What is a Risk Assessment?	IT Security Compliance regulations and guidelines (GLBA, NCUA, FFIEC, HIPAA, etc.) require an organization to conduct a Risk Assessment. The Risk Assessment should identify reasonably foreseeable risks that could result in service interruption or unauthorized disclosure, misuse, alteration, or destruction of confidential information. The Risk Assessment process evaluates the likelihood and potential damage of the identified threats and assesses the sufficiency of safeguards in place, to control the identified risks.	http://www.risk-management-basics.com/risk-management-probability-versus-total-cost-graph.shtml http://csrc.nist.gov/groups/SMA/sbc/workshops.html#03
What is Outsourcing?	**Outsourcing** is subcontracting a process, such as product design or manufacturing, to a third-party company.[1] The decision to outsource is often made in the interest of lowering cost or making better use of time and energy costs, redirecting or conserving energy directed at the competencies of a particular business, or to make more efficient use of land, labor, capital, (information) technology and resources[*citation needed*]. Outsourcing became part of the business lexicon during the 1980s. It is essentially a division of labor. Out sourcing in the information technology field has two meanings [2] One is to commission the development of an application to another organization, usually a company that specializes in the development of this type of application. The other is to hire the services of another company to manage all or parts of the services that otherwise would be rendered by an IT unit of the organization. The latter concept might not include development of new applications	http://en.wikipedia.org/wiki/Outsourcing http://csrc.nist.gov/organizations/fissea/2008-conference/presentations/Wednesday/Wednesday-Oleary_InfoSecurityFlatWorld.pdf
What do I need to do to secure my business?	Information is one of the most valuable assets of any organization, public or private, and the protection of that information is critical. Information security is the protection of information from a wide range of threats and vulnerabilities to ensure business continuity. The vulnerability of any one small business may not seem significant to many other than the owner and employees. However, 95 percent of all US businesses are small and medium-sized businesses (SMBs), of	http://csrc.nist.gov/groups/SMA/sbc/workshops.html#03 http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf http://www.score.org/index.html

	500 employees or less. Therefore a vulnerability common to a large percentage of all SMBs could pose a threat to the Nation's economic base. In the special arena of information security, vulnerable SMBs also run the risk of being compromised for use in crimes against governmental or large industrial systems upon which everyone relies. SMBs cannot always justify an extensive security program, or often a single full time expert. Nonetheless, they confront serious security challenges and must address security requirements based on identified needs. The difficulty for these organizations is to identify needed/cost-effective security mechanisms and obtain training that is practical and cost effective. Such organizations also need to become more educated consumers in terms of security, so that their limited security resources are well applied to meet the most obvious and serious threats.	
Where can I go for training on cyber security issues?	Information is one of the most valuable assets of any organization, public or private, and the protection of that information is critical. Information security is the protection of information from a wide range of threats and vulnerabilities to ensure business continuity. The difficulty for these organizations is to identify needed/cost-effective security mechanisms and obtain training that is practical and cost effective. Such organizations also need to become more educated consumers in terms of security, so that their limited security resources are well applied to meet the most obvious and serious threats.	http://csrc.nist.gov/groups/SMA/sbc/overview.html http://www.smallbusiness3.com/welcome http://www.score.org/index.html
Is there a checklist of Do's and Don'ts for Cyber Security?	A general SDLC includes five phases: initiation, acquisition/development, implementation/assessment, operations/maintenance, and sunset (disposition). Each of the five phases includes a minimum set of security tasks needed to effectively incorporate security in the system development process. Including security early in the information SDLC will usually result in less expensive and more effective security	http://csrc.nist.gov/groups/SMA/sdlc/documents/SDLC_brochure_Aug04.pdf http://www.smallbusiness3.com/welcome

	than adding it to an operational system. The following questions should be addressed in determining the security controls that will be required for a system: • How critical is the system in meeting the organization's mission? • What are the security objectives required by the system, e.g., integrity, confidentiality, and availability? • What regulations and policies are applicable in determining what is to be protected? • What are the threats that are applicable in the environment where the system will be operational?	
How can I stay current on Cyber Security issues?	There are many sources for updates on the Cyber Security and information security issues. The NIST Computer Security website has updates as well as publications that refer to security applications. Other sources are the SBA website, FBI website, University websites, and magazines and other publications.	http://web.jhu.edu/clips http;//www.2600.com http://www.gnc.com/Articles/2009/03/03/WH-cyber-review-updates.aspx
Where can I go to get information on training?	What makes an effective information security program for a small organization? This educational presentation is intended to promote: • Awareness of the importance of need for IT security • Understanding of IT security vulnerabilities and corrective measures The interactive discussion will focus on those information security risks facing all small organizations and how those risks can be identified and managed. Topics will include: • How your data is vulnerable • What you can lose through an information security breach • Practical steps to protect your operations	http://csrc.nist.gov/groups/SMA/sbc/workshops.html#03 http://web.sba.gov/faqs/

	• How to use information security vendors and consultants • How to evaluate tools and techniques based on your needs	
Where do I find the regulation who should be trained?	Please review the attached links for more information on this question.	http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf
Q: Where can I get current information on security issues?	A: Briefings, Articles, Newsletters, and Magazines	http://csrc.nist.gov/groups/SMA/ate/materials.html#05 http://csrc.nist.gov/publications/drafts/ir-7621/draft-nistir-7621.pdf https://www.honeynet.org/aggregator http://old.honeynet.org/papers/profiles/cc-fraud.pdf
What exactly is a virus? Is a "worm" also a virus?	Viruses are computer programs or scripts that attempt to spread from one file to another on a single computer and/or from one computer to another, using a variety of methods, without the knowledge and consent of the computer user. A worm is a specific type of virus that propagates itself across many computers, usually by creating copies of itself in each computer's memory. Many users define viruses simply as trick programs designed to delete or move hard drive data, which, strictly speaking, is not correct. From a technical viewpoint, what makes a virus a virus is that it spreads itself. The damage it does is often incidental when making a diagnosis. Obviously, any incidental damage is important, even when authors do not intend to create problems with their viruses; they can still cause harm unintentionally because the author did not anticipate the full effect or	http://technet.microsoft.com/en-us/library/dd632948.aspx http://csrc.nist.gov/archive/virus/

	unintentional side effects. The most common method used for spreading a virus is through e-mail attachment. Sending a virus, even if designed to be harmless, can cause unforeseen damage.	
What is a "Trojan Horse"?	A Trojan Horse meets the definition of virus that most people use, in the sense that it attempts to infiltrate a computer without the user's knowledge or consent. A Trojan Horse, similar to its Greek mythological counterpart, often presents itself as one form while it is actually another. A recent example of malware acting as a Trojan horse is the recent e-mail version of the "Swen" virus, which falsely claimed to be a Microsoft update application.	http://technet.microsoft.com/en-us/library/dd632948.aspx http://en.wikipedia.org/wiki/Trojan_horse_(computing)
What is computer Forensics	**Computer forensics** is a branch of forensic science pertaining to legal evidence found in computers and digital storage mediums. Computer forensics is also known as *digital forensics.* The goal of computer forensics is to explain the current state of a *digital artifact.* The term digital artifact can include a computer system, a storage medium (such as a hard disk or CD-ROM), an electronic document (e.g. an email message or JPEG image) or even a sequence of packets moving over a computer network. The explanation can be as straightforward as "what information is here?" and as detailed as "what is the sequence of events responsible for the present situation?"	http://www.forensics-intl.com/def2.html http://csrc.nist.gov/staff/rolodex/scarfone_karen.html
`		
What is the Honeynet Project?	About The Honeynet ProjectFounded in 1999, The Honeynet Project is an international, non-profit (501c3) research organization dedicated to improving the security of the Internet at no cost to the public. With Chapters around the world, our volunteers are firmly committed to the ideals of OpenSource. Our goal, simply put, is to make a difference. We accomplish this goal in the following three ways.	https://projects.honeynet.org/honeysnap/
What are Hackers?	In common usage, a hacker is a person who breaks into computers, usually by gaining access to administrative controls.[1] The subculture that has	http://www.2600.com/ http://en.wikipedia.org/wiki/Hac

	evolved around hackers is often referred to as the computer underground. Proponents claim to be motivated by artistic and political ends, and are often unconcerned about the use of illegal means to achieve them.[2]	ker_(computer_security) http://csrc.nist.gov/publications/nistir/threats/subsection3_4_2.html