Class Project Assignment Two

NIST 800-30

Download and read the Risk Management Guide for Information Technology Systems from the National Institute for Standards and Technology (NIST Special Publication 800-30) [1]. Based on your reading, briefly answer the following questions.

Place an electronic version of your answers online and link them to our Google Group. This assignment will become part of your online class portfolio.

Questions

1. What is the purpose of NIST Special Publication 800-30?

2. What is the principal goal of an organization's risk management process?

3. According to NIST, what three processes compose risk management?

4. How does risk management relate to the System Development Life Cycle (SDLC)?

5. NIST 800-30 defines seven Information Assurance "key roles". Name and briefly describe each.

6. How does NIST 800-30 define the security primitives, threat, vulnerability, and risk?

7. How is a threat source defined? Name three common threat sources.

8. According to NIST, whose responsibility is IT Security? (technical or management)

9. What is a security control? Define: technical controls, management controls, and operational controls.

10. How should the adverse impact of a security event be described?

11. Describe the difference between quantitative and qualitative assessment?

12. Name and describe six risk mitigation options.

13. What is residual risk?

[1] http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Journal Assignment Two

For your journal (blog), you need to identify a current online news article that deals with cyberwarfare. The focus of the article may be a specific cyberwarfare incident, a specific tactic, or other related issue.

For your journal, post a brief (one to three paragraphs) essay that explains why you selected that article. How the article relates to the class and why the article is important.

Your essay should include a link to the selected article. Note that your essay should not summarize the article. Be sure to post a link to your journal article in the Discussion Section of our Google Group.

Note that cyberwarefare can be defined several ways. Before you begin, you may want to examine cyberwarfare reference materials at:

http://staff.washington.edu/dittrich/cyberwarfare.html

You may also want to look at:
http://gcn.com/articles/2006/08/17/red-storm-rising.aspx

You may also want to look at the Estonia incident:
http://searchsecurity.techtarget.com/news/interview/0,289202,sid14_gci1265720,00.html
or
http://www.nytimes.com/2007/05/18/world/europe/18iht-estonia.4.5774234.html
or
http://www.csmonitor.com/2007/0517/p99s01-duts.html

Outside Reading Assignment Two

This week, your outside reading assignment is RFC 1135 "Helminthiasis of the Internet Worm". [1] RFC 1135 is about the first Internet malware infestation. Since this event is well documented, you may want to supplement this reading with one, or more, of the references listed below.

Based on your reading, briefly answer the following two questions.

1. What was the cause of the first Internet Worm? In specific, what vulnerabilities did the worm take advantage of in order to spread through the Internet?

2. Are those vulnerabilities still present?

References

http://tools.ietf.org/rfc/rfc1135.txt

http://www.faqs.org/rfcs/rfc1135.html

http://snowplow.org/tom/worm/worm.html

http://homes.cerias.purdue.edu/~spaf/tech-reps/823.pdf