## Sources of Information Security Threats

### Case Assignment

Based on the required reading materials and your own research, prepare a **4- to 7-dbl spaced** page paper to discuss various threats to information security. You are to address the following questions in the paper:

1. Why is information security an important issue?
2. What are the sources of information threats? Discuss them in the categories of human, nature, and technology.
3. Discuss the role of ethical hacking and the potential legal issues involved.

### Assignment Expectations

Your paper should provide a summary of your findings from the assigned materials and any quality resources you can find. Cite all sources and provide a reference list at the end of your paper. The following items will be assessed in particular:

1. Ability to consolidate ideas from the reading materials.
2. Demonstration of your understanding of information security from different perspectives.
3. All questions raised in this assignment have been addressed.
4. The report is written succinctly.

**Use at least 1 reference from each of the 3 sections. Total at least 3**

There are many sources of threats to information security. They can come from:

* **Human aspects:** unintended errors made by an authorized user, information espionage, deliberate vandalism and hacking, deliberate attacks, etc.
* **Natural disasters:** earthquakes, tornadoes, floods, landslides, etc.
* **Technology factor:** system failures, obsolescence, etc. The following readings will explore them one by one.

**Human Factor**

Cliff Edwards, Olga Kharif, and Michael Riley (2011). [Human Errors Fuel Hacking as Test Shows Nothing Stops Idiocy](http://www.bloomberg.com/news/2011-06-27/human-errors-fuel-hacking-as-test-shows-nothing-prevents-idiocy.html" \t "_blank)

Homeland Security Test Shows Human Errors Fuel Hacking: [https://www.youtube.com/watch?v=rvVzHK29MK4](https://www.youtube.com/watch?v=rvVzHK29MK4" \t "_blank)

Failure to update software behind federal data breach: [https://www.youtube.com/watch?v=0X7QylrAnnA](https://www.youtube.com/watch?v=0X7QylrAnnA" \t "_blank)

Nonverbal human hacking: [https://www.youtube.com/watch?v=SZ8kJNojrzI](https://www.youtube.com/watch?v=SZ8kJNojrzI" \t "_blank)

Pesante, L. (2008). Introduction to information security. Retrieved from [https://www.us-cert.gov/sites/default/files/publications/infosecuritybasics.pdf](https://www.us-cert.gov/sites/default/files/publications/infosecuritybasics.pdf" \t "_blank)

Paul Rubens (2011). [Stop Software Attacks From Destroying Your Servers](http://www.serverwatch.com/tutorials/article.php/3936741/Stop-Software-Attacks-From-Destroying-Your-Servers.htm" \t "_blank)

Infosec Institute ([Physical security: Managing the intruder](http://resources.infosecinstitute.com/physical-security-managing-intruder/" \t "_blank))

United States Government Accountability Office (2009). “[Information Security: Cyber threats and vulnerabilities place federal systems at risk.”](http://www.gao.gov/new.items/d09661t.pdf" \t "_blank)

Brian Krebs (2011). [Cyber Intrusion Blamed for Hardware Failure at Water Utility](http://krebsonsecurity.com/2011/11/cyber-strike-on-city-water-system/" \t "_blank)

Perrow, Charles (2008). [Software failure, security and Cyber attack.](http://www.cl.cam.ac.uk/%7Erja14/shb08/perrow.pdf" \t "_blank)

**Natural and Man-made disasters**

Defending Your Business Against Natural Disasters: A Look at Data Protection Solutions from [http://www.stratech.com/solutions/data-protection-solutions/data-protection-and-natural-disasters.php](http://www.stratech.com/solutions/data-protection-solutions/data-protection-and-natural-disasters.php" \t "_blank)

**Optional Reading**

U.S. Air Force hands out cyber security contracts worth up to $300 million (July 11, 2012) from [http://www.infosecurity-magazine.com](http://www.infosecurity-magazine.com/" \t "_blank)

Security strategies, retrieved from [http://technet.microsoft.com/en-us/library/cc723506.aspx](http://technet.microsoft.com/en-us/library/cc723506.aspx" \t "_blank)

**Section B: Attacks**

There are various forms of attacks that aim to compromise a system: social engineering, viruses, worms, Trojan horses, back doors, denial of service attacks, spoofing, spams, sniffers, phishing, etc. Next, we will study how they work.

1. Milan Rajbhandari: [Social engineering](https://www.youtube.com/watch?v=D7BZkubZOFY" \t "_blank)
2. Trojan horse: [https://www.youtube.com/watch?v=ssckV79mNLs](https://www.youtube.com/watch?v=ssckV79mNLs" \t "_blank)
3. Benjamin Gottlieb, all you need to know about the virus: [http://www.washingtonpost.com/blogs/blogpost/post/flame-faq-all-you-need-to-know-about-the-virus/2012/06/20/gJQAAlrTqV\_blog.html](http://www.washingtonpost.com/blogs/blogpost/post/flame-faq-all-you-need-to-know-about-the-virus/2012/06/20/gJQAAlrTqV_blog.html" \t "_blank)
4. Viruses, Trojans, Malware, and other aspects of Internet Security: [https://discussions.apple.com/docs/DOC-2435](https://discussions.apple.com/docs/DOC-2435" \t "_blank)
5. Viruses, trojans, worms, phishing, spyware, spam, [https://www.youtube.com/watch?v=nBMq3Am3gKg](https://www.youtube.com/watch?v=nBMq3Am3gKg" \t "_blank)

Back doors—Ways of accessing a computer without the security and authentication procedures that are normally required.

1. Sniffer and how to detect sniffer in a computer network: [http://www.aboutonlinetips.com/sniffer-types-and-protecting-against-sniffing/](http://www.aboutonlinetips.com/sniffer-types-and-protecting-against-sniffing/" \t "_blank)
2. Denial of service attack: [https://www.us-cert.gov/ncas/tips/ST04-015](https://www.us-cert.gov/ncas/tips/ST04-015" \t "_blank)
3. Stephen M. Specht, Ruby B. Lee. Distributed Denial of service: taxonomies of attacks, tools, and countermeasures. [Proceedings of the 17th International Conference on Parallel and Distributed Computer Systems](http://palms.ee.princeton.edu/PALMSopen/DDoS%20Final%20PDCS%20Paper.pdf" \t "_blank), 2004 International workshop on Security in Parallel and Distributed Systems, pp. 543-550, September 2004

**Section C: Ethical Hacking**

An ethical hacker—penetration tester—must be familiar with laws involving computer technology. The laws related to IT change quickly, and tests that are legal in one state might not be in another one. For example, in Hawaii, the state needs to prove that the person who is charged with crime on a computer had the **intention** to create damage, and the computer he uses is used by himself/herself only. Before starting security testing, it is important to have a clear written contract that specifies the scope of the tasks; going beyond the scope of tests can be troublesome and might incur a lawsuit from the employer. Read the following materials for more information:

1. Computer Crime Statutes [http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx](http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx" \t "_blank)
2. Legal issues in hacking. [https://www.youtube.com/watch?v=4Xh8fBV7AOo](https://www.youtube.com/watch?v=4Xh8fBV7AOo" \t "_blank) (Embed this link directly).
3. Ethical hacking [https://www.youtube.com/watch?v=1Ae4TlwlJ7c&list=PL7134FC0815ADB8EB&index=1](https://www.youtube.com/watch?v=1Ae4TlwlJ7c&list=PL7134FC0815ADB8EB&index=1" \t "_blank)

Note: As a security tester, it is important to make sure your program will not use so many computer resources that employees will not able to get access to the network. The situation would create a denial of service problem, and you might end up violating state law.

**Check the following sites for malware attacks:**

1. [http://www.us-cert.gov](http://www.us-cert.gov" \t "_blank)
2. [http://www.symantec.com](http://www.symantec.com" \t "_blank) (Look for View All Viruses and Risks link. You can find the most recent viruses or worms, and solutions to remove them.)

Note: New viruses are created daily; antivirus software can only deal with the known ones. Hence, keeping antivirus software up to date is very important. To learn more about viruses and worms, and how to prevent infection, check the above two links.

To beat hackers, it helps to understand what they do and how they think. There are many online resources that teach you how to create viruses. Accessing them is dangerous, though, since many of these sites have Trojan horses and viruses that might infect your machine.

**To get certificated as an ethical tester, here are a few popular options:**

1. [Certified ethical hacker](http://www.eccouncil.org/Certification/certified-ethical-hacker" \t "_blank) (CEH)
2. [Certified information security systems professional](https://www.isc2.org/cissp/default.aspx" \t "_blank) (CISSP)
3. [OSSTMM Professional Security Tester Accredited Certification](http://www.isecom.org/certification/opst.html" \t "_blank) (OPST)

[Privacy Policy](http://www.trident.edu/privacy-policy" \t "_blank) | [C](http://www.trident.edu/university-information/contact-us" \t "_blank)