ITIS 3200
Ch 1 Activity

1. Gollman speaks of 4 epochs in computer security, ranging from the 1970s thru 2000s. Conspicuously missing from his analysis is the 2010s and beyond. Without needing too much research, what do you think would define or characterize the security needs of the last decade or so?

In 2010: McAfee failed to innovate during its 7 year under Intel.
In 2014: OPM devastated the intelligence capabilities of USA.
In 2014: Breach in SONY Pictures, they brought back James Franco, Seth Rogen for a movie.
In 2017: Eternal Blue confirms NSA is really good at developing exploits.
In 2020: Encryption and Multi-Factor Authentication are key.

2. How do you think end users' responsibilities for managing security have changed over that time?

End-users responsibility has changed drastically since the 1950's to the latest 21st century, when the users cant connect to the mainframe, now the user's can connect to the mainframe and identify the issue. Now in the 21st century users can collaborate with the tech experts and offer advice regarding information security, and IT departments..

3. The principle of full disclosure asks that all details of a security vulnerability to be disclosed. Does this lead to an increase or decrease in security? Why?

In my opinion disclosing information about the security vulnerabilities will decrease the security completely. Because if you know what makes it strong, and where are all the vulnerabilities are at, it will be a matter of time before someone is siphoning the data.

4. Applying your answer to #3 to the Log4j vulnerability, would your answer change? Why or why not?

Applying my answer to the log4j vulnerability, my answer would not change, because the job of 4j is to report any errors in the software, coupled with disclosing security information vulnerabilities, will make it the weaker system in the planet.