Background

Suppose that you’re the chief technology officer for a startup, producing mobile applications software, less than a year old, that has been funded by a group of venture capitalists but has not yet released any products. The team consists of six people—you and two other programmers, one of whom is the chief executive officer; a chief financial officer; a marketing and sales representative; and a factotum who combines the roles of purchasing officer, accountant, facilities scheduler, appointments secretary, and receptionist. You three programmers have known one another for six years and were friends in college; The CFO was appointed by the venture capitalists when the startup was formed; and the other two people were hired on the recommendation of a job placement service about six months ago. So far, there have been no personnel crises and no major disagreements about the direction of the company, and the personality conflicts have been minimal.

The work of the startup is being done on what used to be the home network of the CEO. It now comprises a gateway router, wired only, and two internal subnetworks, each with its own wireless router: one for the programmers, which has four well-equipped GNU/Linux workstations wired to it and also receives connections from half a dozen laptops, and one for the rest of the staff, handling four Windows workstations and three laptops. The gateway router has exactly four connections: outward to the company’s Internet service provider, and inward to the other two subnet routers and to another workstation, which is used as the company’s Web server. There is also a printer/scanner on each subnetwork. All of the hardware is standard stock from major suppliers (Dell, HP, Apple, Cisco).

The CEO’s main security concern has to do with the planning documents and implementation files of the applications that are under development. He’s worried, first, that some competitor will somehow find out your startup’s trade secrets and rush a similar product to market before your product can establish itself; and, second, that through some catastrophe or malicious attack the documents and files will be lost or corrupted. Part of your job is to provide a security framework that makes both of these possibilities unlikely.

The Proposal

Today’s assignment is to write up, in approximately a thousand words, the first three sections of the proposal that you will make to the other five people in the company, concerning the security framework that you think the company should implement:

1. The threat assessment: List and assess the security threats that you regard as most probable and consequential and the weaknesses that are most likely to be exploited.
2. Collecting information about users’ needs and current practices: Draw up a list of the questions relating to security that you most need to have answered in order to improve the company’s security.
3. Login and file-access controls: Propose rules for accessing the workstations, laptops, and routers that make up company network and the files stored on those devices that minimize the risk of prevent industrial espionage, vandalism, or accidental damage without obstructing the essential work of the current users of the network and any employees you subsequently hire.
In later assignments, we’ll add further sections on Web and e-mail use, use of social networks, procedures for backing up and restoring data, outsourcing and cloud-service policies, the use of encryption, protecting the privacy of users, business partners, and customers, and other security-related issues. For today, it is sufficient in section 3 of the report to deal with issues relating to login (local and remote) and file access.

This exercise will be due at the beginning of class on Thursday, February 16.