Exercise: Customer Records
March 16, 2017

Background
In this exercise, you’re once again the chief technology officer for that mobile-applications startup, working up a security framework for the startup’s network designed to protect the business’s documents and data.

The new feature today is that the sales and marketing people are starting to develop contacts with potential customers for your product and even to explore possible price structures (quantity discounts, site licenses, and so on). One of the programmers has designed a simple SQL database in which to store information about these potential customers—each company or division’s name and street address and the name, e-mail address, mobile phone number, and LinkedIn page of the contact person at that company or division.

The Proposal
Today’s assignment is to write up two new sections for the security-framework document:

4. A specification stating policies for access to customer information both within the startup itself and by business partners, representatives of the Securities and Exchange Commission and the Internal Revenue Service, and other potentially interested outside parties.

5. A proposal for implementing these policies, considering such questions as
   • whether to allow authorized users to access the database remotely, over the Internet (and, if so, by what mechanism and under what conditions);
   • whether the database should exist in one and only one copy, requiring sales and marketing people to access it directly each time they need to put information into it or read information out of it, or whether they should be allowed to make their own private copies;
   • whether it would be prudent to hire a new person to implement and manage the database securely or, alternatively, to outsource this function to another company that specializes in secure data management;
   • whether there is any role for encryption in the management of the database;
   • and what actions the company should take if personally identifiable information is somehow leaked from the database to potentially hostile parties (e.g., criminals who start sending phishing e-mails to the leaked e-mail addresses of customers).

This exercise will be due at the beginning of class on Thursday, April 6.