

# COMP3441/9441 Tutorial Week 11

## Enterprise Security

1. A new vulnerability has been announced in the public domain. It exists in a service used in a popular and broadly used computer application. The manufacturer has made a patch available for download and installation.

You are a security practitioner working for a large global corporation with a very complex IT infrastructure. Your role is to search for new security vulnerabilities and determine if they do or may concern your business. You also need to identify their potential impact and severity to the business. Finally, you formulate recommendations on what actions should be taken, how quickly, and why.

- (a) How do you determine whether the vulnerability will affect your business?
  - (b) If the vulnerability does affect your business, how do you identify the potential impact it might have?
  - (c) What kind of factors might affect your business's ability to close the exposure?
  - (d) What recommendations might you make on actions your business should take to minimize the risks of this vulnerability?
  - (e) Your manager asks you to identify the impact and costs of implementing your recommendations across the enterprise. How do you estimate this?
2. What are the general categories of security risks? Give some specific examples of risk from each category.
  3. What are the four stages in the information risk management model? Give some examples of the actions that are taken in each of the stages.

Question 1 is from K. Valios, *Security Management Issues*, UNSW COMP3441/9441 Seminar Slides, Week 10, Oct. 2003.