ITMD: 511 Application Development Methodologies

Chapter 14: Resilience Engineering

Exercises

1. Explain how the complementary strategies of resistance, recognition, recovery, and reinstate- ment may be used to provide system resilience.

2. What are the types of threats that have to be considered in resilience planning? Provide examples of the controls that organizations should put in place to counter those threats.

3. A hospital proposes to introduce a policy that any member of clinical staff (doctors or nurses) who takes or authorizes actions that leads to a patient being injured will be subject to criminal charges. Explain why this is a bad idea, which is unlikely to improve patient safety, and why it is likely to adversely affect the resilience of the organization.

4. What is survivable systems analysis and what are the key activities in each of the four stages involved in it as shown in Figure 14.8?

5. Explain why process inflexibility can inhibit the ability of a sociotechnical system to resist and recover from adverse events such as cyberattacks and software failure. If you have experience of

process inflexibility, illustrate your answer with examples from your experience.

6. Suggest how the approach to resilience engineering that is proposed in Figure 14.9 could be used in conjunction with an agile development process for the software in the system. What problems might arise in using agile development for systems where resilience is important?

7. A senior manager in a company is concerned about insider attacks from disaffected staff on the company's IT assets. As part of a resilience improvement program, she proposes that a logging system and data analysis software be introduced to capture and analyze all employee actions but that employees should not be told about this system. Discuss the ethics of both introducing a logging system and doing so without telling system users.

8. In Section 13.4.2, (1) an unauthorized user places malicious orders to move prices and (2) an intrusion corrupts the database of transactions that have taken place. For each of these cyber- attacks, identify resistance, recognition, and recovery strategies that might be used.