60/60

Kenneth Jahnke

Assignment 1 – 18 Jan 2025

CSCI 389 (Online) - Spring ‘25

1.1. Confidentiality requirements. 1) The PIN (high importance): The PIN is private information. It is used to authenticate with the bank that only the intended user is at the ATM. The user is required to not disclose it to anyone. 2) The physical ATM card (high importance): Maintaining confidentiality is primarily the responsibility of the card owner. To do this, the card owner is required to physically safeguard the card, so unauthorized individuals do not acquire it and utilize it. This is addressing only the physical card. Information on the card may exist elsewhere, which comes with its own vulnerabilities, but the physical card is what's being addressed in this scenario.

Integrity requirement. Secure ATM and banking system (high importance): It is the bank's responsibility to ensure data confidentiality by ensuring the ATM and the banking system it is connected to are secure and that data traverses the system securely. The bank is required to ensure the hardware, software, procedures, and trained personnel

Availability requirement. Cyber defense and attack response (high importance): The bank is required to have in place a robust cyber defense apparatus. This counters the possibility of services going down in the event of attack. The bank is also required to have in place plans and procedures to execute in the event of attack to expediently restore services.

1.2. The requirements apply to Confidentiality, Integrity, and Availability and they are all of high importance. The switching system is required to be up-to-date and meet industry standards and protocols. It is required to be maintained on a regular basis and have sufficient support systems (housing, electrical, network access, etc.). It is required to be overlooked by a cyberescurity team that monitors the system for anomalies, frequently updates software and firmware, updates hardware as necessary to meet standards, is sufficiently trained on matters of security with emphasis on switching network security, is trained on the ethics of privacy, is aware of the threat environment, and has reaction plans ready to deploy in the event of attack to expediently restore services.

1.3.a. Types of publications where confidentiality of stored data is important:

- Financial reports
- Military reports, particularly if the data is classified
- Medical reports
- Legal proceedings

1.3.b. Types of publications where integrity is important:

- Scientific reports and journals
- Public health reports
- Newspapers and journalism articles covering topics where accuracy is key to the adherence of ethical standards and the mitigation of misinformation
- Any publication where the use of the information drives key decisions

1.3.c. Types of publications where availability of stored data is important:

- Government reports
- News websites
- APIs
- Networking and technology statuses

1.4.a. Loss of confidentiality – low impact. The information is public; hence, confidentiality does not apply.

Loss of availability – high impact. Any number of decisions may depend on the utilization and analysis of this public information. Its loss impedes government, businesses, and personal lives.

Loss of integrity – high impact. The loss of integrity within this web server would turn it into a storehouse of misinformation.

1.4.b. Loss of confidentiality – high impact. If unauthorized personnel acquired access to such sensitive information, active investigations would very likely be compromised. This would severely harm judicial proceedings.

Loss of availability – high impact. Loss of access to evidence reports and legal analysis would very likely severely disrupt the legal proceedings. If this information was not lost, it would very likely take excessive amounts of time to reproduce or rediscover.

Loss of integrity – high impact. The judicial system aims to find the truth. If the integrity of the investigative information is negated, the judicial system cannot meet its aim.

1.4.c. Loss of confidentiality, availability, or integrity – all high impact. Just because the information is not privacy-related does not mean the unauthorized disclosure of this information, the loss of its access, or its degradation or undue modification would not have negative impacts on the financial organization and how it operates. Given the interconnectedness between financial institutions and efficiency of modern global life, it is critical that the institutions maintain operational and administrative continuity.

1.4.e. SENSITIVE, PRE-SOLICITATION PHASE CONTRACT INFORMATION

Loss of confidentiality - high impact. As stated, the information is sensitive.

Loss of availability - moderate impact. A loss of access would require the information to be refiled, redrafted, or retransmitted. If a project is already underway, a loss would likely create a significant delay.

Loss of integrity - moderate impact. Unintended modification of details of a contract would likely mean the deliverable does not meet specification. This would result in a loss of confidence and possible legal ramifications.

ROUTINE ADMINISTRATIVE INFORMATION

Note: Because “routine administrative information” is an extremely vague term, I felt at liberty to go hog wild in these doomsday scenarios.

Loss of confidentiality - high impact. The payroll department gets hacked. Everyone’s banking information gets stolen. A class action lawsuit is filed against the company for negligence. They lose. Millions in legal and restitution fees. The company goes under.

Loss of availability – high impact. The company switched to all digital years ago. The company’s servers got hacked. Literally everything was wiped. Contract information, human resource information, marketing materials, even the plans for the holiday party - all of it is gone. There are no internal or off-site backups of anything due to the prior year’s budget cuts in the IT department. The company is a shell. They shudder.

Loss of integrity – high impact. The company's website gets hacked. The attackers fill every page with lewd, vulgar, and offensive materials. The media takes notice and runs stories on the incident. The company's public image is tarnished. Sales numbers plummet. The company files for bankruptcy within the year.

SYSTEM AS A WHOLE

Due to the mishandling of “routine system information”, the contracting organization has been disbanded.

1.4.e. REAL-TIME SENSOR DATA

Loss of confidentiality – moderate impact. If this information were being gleaned to gather expose potential vulnerabilities, it may expose potent attack vectors to would-be adversaries. On the other hand, if the data is not sensitive and consists of low-grade technical or non-propriety information, its disclosure may be a moot point.

Loss of availability – high impact. Loss of access to this data stream will almost certainly negatively impact personnel's ability to monitor and control the system's function.

Loss of integrity - Inaccurate information passing through the SCADA indicates a fault in the system.

ROUTINE ADMINISTRATIVE INFORMATION

Note: My only assessment on the meaning of “routine administrative information” in the context of a SCADA is control signals (on, off, half power, what have you), so that’s how I’m framing this question. Yes, these are the same answers as in the previous section. But, sensor data drives control decisions, thus making the two data sets symbiotic.

Loss of confidentiality – moderate impact. If this information were being gleaned to gather expose potential vulnerabilities, it may expose potent attack vectors to would-be adversaries. On the other hand, if the data is not sensitive and consists of low-grade technical or non-propriety information, its disclosure may be a moot point.

Loss of availability – high impact. Loss of access to this data stream will almost certainly negatively impact personnel's ability to monitor and control the system's function.

Loss of integrity - Inaccurate information passing through the SCADA indicates a fault in the system.

SYSTEM AS A WHOLE

Loss of confidentiality – high impact. Unauthorized access of this information could feasibly be the effect of a nation-state cyber-attack. Given the SCADA controls distribution to the military installation, a loss of confidentiality becomes a matter of national security as the access may be an indication of attack intention and/or plans.

Loss of availability or integrity – high impact. Like the reasoning outlined in the previous statement, a loss of access to the data, or its destruction, deletion, or degradation may indicate a nation-state attack on the military base is occurring or is imminent.

P1.4 For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers.

a. An organization managing public information on its Web server.
b. A law enforcement organization managing extremely sensitive investigative information.
c. A financial organization managing routine administrative information (not privacy-related information).
d. An information system used for large acquisitions in a contracting organization contains both sensitive, pre-solicitation phase contract information and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.
e. A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.