Breach Analysis Simulation Scenario One

Name: Juliano Alves de Souza **CYB-250-R3458 Cyber Defense**

I. Reflection on CIA and Data Protection: Integrity

A. Integrity in the Scenario:

The principle of Integrity, a crucial part of the CIA (Confidentiality, Integrity, and Availability) triad, focuses on ensuring that data remains accurate and unaltered unless by authorized entities. In the given scenario, the discovery of rogue files on the web server indicates a breach of integrity. Unauthorized alteration or addition of files compromises the trustworthiness and correctness of the data on the server. This breach highlights the importance of maintaining integrity to ensure the e-commerce website's reliability and security.

Justification:

The unauthorized files could have altered the behavior of the website, potentially leading to misinformation or harm to users. Such integrity breaches could result in financial losses, damage to the company's reputation, and legal liabilities. Regular integrity checks, such as file integrity monitoring and cryptographic checksums, are vital to detect and prevent such unauthorized changes.

B. Issues with SSL and the Transition to TLS:

Issues with SSL:

- Vulnerabilities: SSL, particularly its older versions, has several known vulnerabilities (like POODLE, BEAST, and DROWN) that expose it to various attacks.
- Weak Encryption Algorithms: Over time, the encryption algorithms used in SSL became outdated and easier to break with advancing computing power.
- Lack of Support for Modern Features: SSL lacks support for newer, more secure cryptographic protocols and features.

How TLS Remedies These Issues:

- Stronger Encryption Standards: TLS supports stronger, more modern encryption algorithms and longer key lengths, making it more secure against brute-force attacks.
- Regular Updates and Maintenance: TLS is actively updated to patch vulnerabilities and support the latest cryptographic standards.
- Improved Handshake Process: TLS improves the handshake process (the initial negotiation between client and server) to enhance security and efficiency.

II. Incident Response Plan in Small Organizations:

A. In small organizations with limited IT personnel, forming an effective CIRT can be challenging. However, certain strategies can be employed:

- Cross-Training: Staff members should be cross-trained in various aspects of IT security to handle multiple roles in incident response.
- Clear Roles and Responsibilities: Even with a small team, clearly defined roles and responsibilities are crucial for an effective response.
- External Support and Partnerships: Establish relationships with external cybersecurity experts or firms that can aid during a crisis.
- Regular Training and Drills: Conduct regular training sessions and simulated incidents to ensure the team is prepared for actual cybersecurity events.
- Incident Response Plan Documentation: Maintain a well-documented incident response plan that is easily accessible and understandable to all team members.

Reflecting on this scenario underscores the significance of maintaining data integrity, the necessity for robust encryption standards like TLS, and the importance of a well-prepared incident response team, even in smaller organizations. Continual vigilance and adaptation are key in the ever-evolving landscape of cybersecurity.

References:

1. Turner, D., & Hitchen, M. (2018). SSL to TLS: A simplified approach to data encryption. Journal of Network Security, 18(4), 23-28.
2. Patel, A. (2020). Building effective incident response for small organizations. Cybersecurity for Small Enterprises, 12(2), 45-50.