Differentiating Due Care vs. Due Diligence in Information Risk Management

Due Care:

- **Definition:** The effort made by an organization to protect its information assets from risk, based on established best practices and reasonable expectations.
- **Focus:** Ensuring that basic security measures are in place to avoid harm.

Due Diligence:

- **Definition:** The ongoing process of continuously evaluating and improving information security practices to identify and address new and evolving risks.
- **Focus:** Proactively managing and adjusting security measures to respond to changing risk environments.

Boldi AG Analysis:

- **What Went Wrong:** Boldi AG's issue lies in both due care and due diligence.
    - **Due Care:** They have taken basic steps (offsite storage) but failed to secure the facility with 24/7 monitoring, which is a fundamental practice for protecting backup systems.
    - **Due Diligence:** They did not regularly review or update their backup security practices, reflecting a lack of proactive risk management.

Conclusion: Boldi AG's approach lacked both due care (inadequate physical security) and due diligence (failure to continually assess and improve security measures).

Basic Options for Limiting or Containing Damage from Risk

1. Deter

- **Definition:** Implementing measures to discourage potential attackers from targeting the organization.
- **Example:** Using strong security policies, publicizing security investments, and employing deterrent technologies like firewalls and intrusion prevention systems.

2. Detect

- **Definition:** Identifying and monitoring signs of potential security breaches or attacks.
- **Example:** Deploying intrusion detection systems (IDS), monitoring network traffic, and analyzing logs for unusual activities.

3. Prevent

- **Definition:** Implementing controls to stop attacks from occurring in the first place.
- **Example:** Using antivirus software, ensuring secure coding practices, and applying security patches and updates regularly.

4. Avoid

- **Definition:** Changing practices or processes to avoid vulnerabilities or risky behaviors that could lead to attacks.
- **Example:** Avoiding the use of outdated software, implementing strong access controls, and avoiding risky behaviors like opening suspicious emails.

Reaction to Competitor Attack:

- **Understand Environment:** Identify and assess potential attack vectors.
- **Deter:** Strengthen security measures to make attacks more difficult.
- **Detect:** Implement monitoring systems to quickly identify signs of an attack.
- **Prevent:** Adopt best practices to minimize vulnerabilities.
- **Avoid:** Adjust strategies to avoid known risks and threats.
- **Deflect or Delay:** Use techniques to slow down or redirect attacks.
- **Degrade:** Employ methods to reduce the effectiveness of an attacker’s efforts.
- **Defeat:** Implement responses to neutralize and eliminate the attack.