Due Care vs. Due Diligence in Cybersecurity

- Due Care: Actions taken to mitigate a vulnerability (after an incident).
- Due Diligence: Steps taken to protect assets and prevent future exploits.
- Due Care is reactive; Due Diligence is proactive.
- Both are essential components of a comprehensive cybersecurity strategy.

Boldi AG’s Cybersecurity Shortcomings

- **Last Information Risk Analysis in 2014:** The company's failure to conduct an information risk analysis since 2014 demonstrates a lack of proactive cybersecurity measures. This is a critical oversight, as regular risk assessments are essential for identifying and addressing vulnerabilities before they can be exploited.

- **Physical Security Gaps:**Physical Security Gaps: Storing backup systems and databases in an offsite facility without 24/7 monitoring is a significant security risk. This indicates a failure to implement basic physical security controls to protect critical assets.

Consequences of Inadequate Cybersecurity

Increased Vulnerability to Attacks: The absence of regular risk assessments and inadequate physical security measures leave Boldi AG highly susceptible to cyberattacks, including ransomware attacks like the one that recently affected their competitor.

Potential for Data Breaches: The lack of proper access controls and physical security could lead to unauthorized access to sensitive data, resulting in data breaches and significant financial and

Regulatory and Legal Risks: Failure to comply with information security best practices could expose Boldi AG to legal and regulatory penalties.

Recommendations for Boldi AG

- **Implement a Risk Management Framework:** Adopt a proactive approach to cybersecurity by establishing a risk management framework that includes regular risk assessments, vulnerability management, and incident response planning.

- **Enhance Physical Security:** Immediately address the security gaps at the offsite storage facility by implementing 24/7 monitoring, access controls, and other appropriate physical security measures.

Recommendations for Boldi AG (cont.)

- **Enforce Information Security Best Practices:** Prioritize the implementation of essential controls, including access management, user training, and data encryption, to protect critical assets and reduce the risk of cyber attacks.

- **Regular Staff Training:** Conduct regular cybersecurity training for all employees to raise awareness and ensure compliance with security policies and procedures.

Defense options for Boldi AG

Deter:

- Deter or discourage unauthorised people from attempting to gain unauthorised access to the facility. Implement measures that unauthorised people perceive as too difficult or needing special tools and training to defeat.
- Have IDS/IPS to monitor and detect malicious traffics.
- Implement firewalls and separate networks so outsiders don’t get access.

Detect:

- Detect unauthorised access as early as possible. Implement measures to work out whether an unauthorised action is occurring or has occurred.

Defense options for Boldi AG (cont.)

Respond:

- An effective response counters the anticipated activity of an unauthorised person within a time appropriate to the delay measures. Prepare measures to prevent, resist, or mitigate the impact of an attack or event.

Recovery:

- Take the steps required to recover from a security incident. Plan to restore operations to as near normal as possible in a timely manner following an incident.