Pitch For Boldi AG

Part 1: Due Care vs Due Diligence and Boldi AG's Misstep

Due Care vs. Due Diligence:

- **Due care** refers to the ongoing actions an organization takes to maintain a reasonable and sufficient level of security for its information assets. This involves implementing and upholding security policies, procedures, and controls.
- **Due diligence** is the investigative process of identifying and understanding potential risks before engaging with a third party or taking on a new activity. It's about proactively assessing potential vulnerabilities.

Boldi AG's Mistake:

Boldi AG likely failed to perform **due diligence** when selecting their offsite storage facility. They didn't ensure the facility had adequate security measures like 24/7 monitoring, increasing the risk of unauthorized access. This oversight potentially exposed their backups to compromise.

It wasn't due care because the issue lies with the chosen facility, not ongoing security practices within Boldi AG. However, depending on their internal security policies, failing to monitor backups at all could be a separate due care issue.

Part 2: Basic Defense Options for Boldi AG (DDPA)

DDPA represents the four key principles of information security defense:

1. **Deter**: Implement measures to discourage attackers, such as security cameras, alarms, and strong access controls.
2. **Detect**: Establish mechanisms to identify security incidents as soon as possible, like intrusion detection systems and log monitoring.
3. **Prevent**: Take steps to stop attacks from succeeding, such as firewalls, data encryption, and user training.
4. **Avoid**: Mitigate risk by avoiding certain activities altogether, like storing sensitive data offsite in a facility with inadequate security.

Boldi AG's Reaction to a Potential Attack

Here's how Boldi AG can react to an attack like their competitor's:

- **Activate Incident Response Plan:** Initiate their pre-defined plan for handling security incidents, which should outline steps for containment, eradication, and recovery.

- **Isolate Affected Systems:** Immediately isolate compromised systems to prevent further damage and lateral movement within the network.
- **Investigate the Breach:** Determine the scope of the attack, what data was breached, and how the attacker gained access.
- **Notify Authorities and Stakeholders:** Inform relevant authorities and stakeholders about the incident in a timely manner, following legal and regulatory requirements.
- **Remediation and Recovery:** Implement corrective actions to address vulnerabilities and restore affected systems.

By addressing the voicemail's concerns and implementing these measures, Boldi AG can strengthen their security posture and minimize damage from future attacks.

For Stefan's Slide:

- Title: **Boldi AG Security Blindspot: Offsite Backup Storage**
- Content:
    - Briefly explain the voicemail's findings (unmonitored offsite storage facility) and its security risk.
    - Highlight the importance of due diligence in selecting vendors/facilities.
    - Briefly outline potential DDPA strategies to mitigate the risk.