Cybersecurity Insights for Boldi AG

Strengthening Your Information Risk Management

Date: 21/01/2025

Prepared By: PCW (Gabriel Reis Santos)

Agenda

1. **Introduction and Background**
2. **Part 1: Due Care vs. Due Diligence**
   - Definitions and Differences
   - Boldi AG’s Shortcomings
3. **Part 2: Key Defense Options**
   - Deter, Detect, Prevent, Avoid
4. **Recommendations**
5. **Q&A**

Introduction and Background

- **Introduction & Background**
- **Who We Are (PCW):**
  - A trusted cybersecurity advisory partner with expertise in defending organizations against ransomware and other cyber threats.
- **Why We're Here:**
  - Boldi AG (family-owned, ~90 employees) is concerned after a competitor suffered a severe ransomware attack.
  - Boldi AG's last risk analysis was in 2014; a recent voicemail uncovered an offsite backup vulnerability (lack of 24/7 monitoring).
- **Goal:** Provide a clear, actionable roadmap for Boldi AG to strengthen its security posture and mitigate information risk.

Due Care vs. Due Diligence

- **Due Care**
- **Definition:**
  - A baseline level of security measures or controls a reasonable organization should have in place.
  - *"Doing the right things"* at a fundamental level (e.g., physical security, basic policies, backups).
- **Examples:**
  - Locking server rooms
  - Ensuring antivirus is deployed
  - Running routine data backups
- **Due Diligence**
- **Definition:**
  - The continuous, proactive process of validating that your security measures remain effective and updated.
  - *"Making sure you're doing things right"* via audits, reviews, and improvements.
- **Examples:**
  - Regular patching and penetration testing
  - Annual or quarterly security assessments
  - Auditing user accounts and third-party access

Where Boldi AG Fell Short

- **Voicemail Discovery:** Offsite backups stored in a facility with no 24/7 monitoring.**Due Care Failure:**Missing fundamental controls (e.g., physical security, restricted access).
- **Due Diligence Failure:**Last formal risk analysis was in 2014, indicating no routine checks or ongoing improvements.
- **Conclusion:** Boldi AG needs improvements in **both** due care (set a baseline) and due diligence (continually validate it).

Key Defense Options

PCW recommends a layered, integrated defense built on four core strategies:

Deter	• **Definition:** Discourage potential attackers from targeting your organization. • **Examples:** Visible security measures, strong legal posture, or proven incident response capabilities.
Detect	• **Definition:** Rapidly identify intrusions or suspicious activities. • **Examples:** Intrusion detection systems, real-time monitoring, threat intelligence.
Prevent	• **Definition:** Block or stop threats before they cause damage. • **Examples:** Firewalls, network segmentation, patch management, strict access controls.
Avoid	• **Definition:** Eliminate or reduce the risk at its source. • **Examples:** Not storing unneeded sensitive data, relocating critical infrastructure to a more secure environment, or using a vetted cloud backup provider.

Recommendations for Boldi AG

Update and Formalize Risk Analysis

Conduct a new assessment to reflect current threats.

Align with recognized frameworks (e.g., ISO 27001, NIST CSF).

Shore Up Due Care

Lock down physical security around backups (24/7 surveillance, ID checks).

Ensure all employees are trained and aware of basic security policies.

Reinforce Due Diligence

Establish periodic security audits and continuous monitoring.

Set scheduled reviews for backup protocols, third-party access, and patch cycles.

Adopt the D-D-P-A (Deter, Detect, Prevent, Avoid) Approach

Deter: Post visible security notices, maintain a strong public stance against cybercrime.

Detect: Deploy intrusion detection systems, real-time logging, event correlation.

Prevent: Maintain strong technical controls, privileged access management.

Avoid: Remove unneeded data, shift to secure sites/providers if cost-effective.