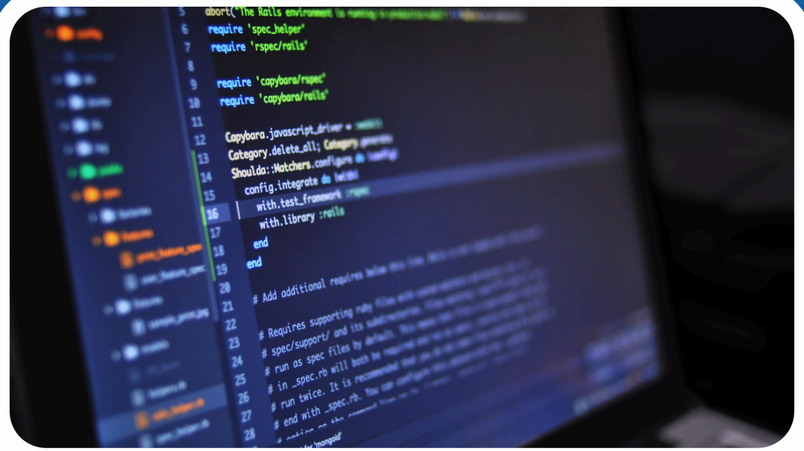
Enhancing Cybersecurity at Boldi AG

By:Aparna Mishra and Stefan

Understanding Due Care and Due Diligence in Information Risk Management

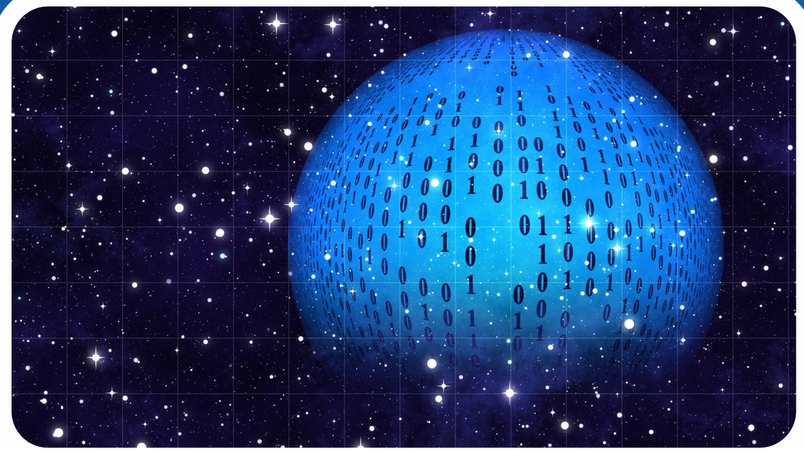
Due Care

- The level of care that a reasonable person would exercise in a particular situation. It involves taking the necessary steps to ensure the protection of assets.
- Examples: Regularly updating security policies, conducting employee training, implementing basic security measures.



Due Diligence

- The ongoing process of managing risks through regular assessment, monitoring, and improvement of security measures.
- Examples: Regular vulnerability assessments, continuous monitoring of systems, audits, and compliance checks.



Boldi AG's Mistake Analysis

- Issue Identified: Storing backups in an offsite facility that is not monitored 24/7.
- Due Care vs. Due Diligence:
- Due Care Failure: Boldi AG did not ensure the physical security of their backup storage, exposing it to unauthorized access.
- Due Diligence Failure: They failed to continuously monitor and reassess the security of the offsite facility.

Basic Options for Limiting or Containing Damage from Risk

Deter:

- Explanation: Implement measures that discourage attackers from attempting to breach the system.
- Examples: Strong passwords, security awareness training, visible security cameras.

Detect:

- Explanation: Implement systems that can identify and alert about potential security incidents.
- Examples: Intrusion detection systems (IDS), log monitoring, anomaly detection.

Prevent:

- Explanation: Implement measures that stop attacks before they cause damage.
- Examples: Firewalls, antivirus software, access controls.

Avoid:

- Explanation: Implement strategies that completely eliminate the risk.
- Examples: Avoiding storing sensitive data in high-risk areas, using cloud services with robust security.

Subject: Key Insights for Boldi AG Cybersecurity Pitch Presentation

Hi Stefan,
I hope this email finds you well.
Based on our recent call with Boldi AG management, I've prepared a detailed analysis for our pitch presentation. Below are the key points:

Differentiating Due Care and Due Diligence

Due Care: Refers to the necessary steps taken to ensure the protection of assets, such as updating security policies and employee training.

Due Diligence: Involves the ongoing process of managing risks through regular assessments, monitoring, and improvements.

Boldi AG's Mistake Analysis:

- The issue of storing backups in an offsite facility without 24/7 monitoring highlights both a due care and due diligence failure. They did not ensure the physical security of their backups (due care) and failed to continuously reassess the security measures in place (due diligence).Subject: Key Insights for Boldi AG Cybersecurity Pitch Presentation

Detect:
Implement systems to identify and alert about security incidents (e.g., intrusion detection systems, log monitoring).
Prevent:
Implement measures to stop attacks before they cause damage (e.g., firewalls, antivirus software).
Avoid:
Implement strategies to eliminate risks completely (e.g., using secure cloud services).
Response to an Attack
Boldi AG can enhance their incident response plan to react effectively to attacks like the one experienced by their competitor. This includes immediate isolation of affected systems, communication with stakeholders, and a thorough investigation to prevent future incidents.
I have also created a PowerPoint slide summarizing these points for our pitch presentation.

Looking forward to your feedback.

Best regards,
Aparna Mishra and Stefan

THANK YOU!