Virtual Case Experience Cybersecurity

Model Work Task 1

1

Part 1

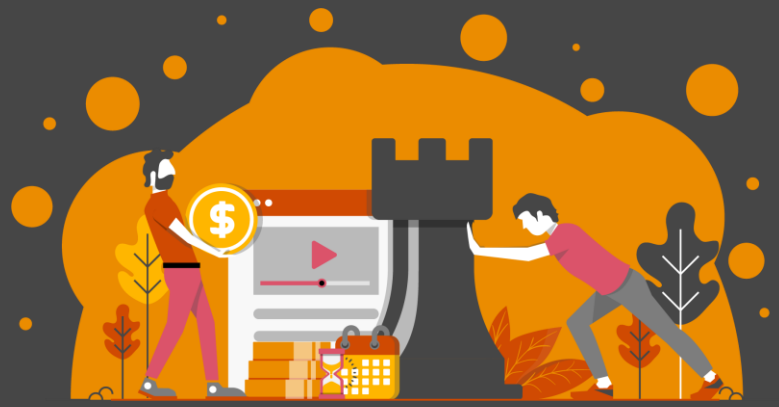
Integrated Information Defense I

Due care

You take *due care* of those responsibilities, and your investors' expectations and investments, when you set up the business, its business logic and processes, and all of its facilities, equipment, people, and supplies so that it can operate. The burden of due care requires you not only to use common sense, but also to use best practices that are widely known in the marketplace or the domain of your business. Since these represent the lessons learned through the successes or failures of others, you are being careful when you consider these; you are perhaps acting recklessly when you ignore them.

Due diligence

As a business leader, owner, or stakeholder, you exercise *due diligence* by inspecting, auditing, monitoring, and otherwise ensuring that the business processes, people, and systems are working correctly and effectively. This means you must check that those processes and people are doing what they were set up to do and that they are performing these tasks correctly. More than that, you must also verify that they are achieving their share of the business's goals and objectives in efficient and effective ways - in the best ways possible.



Source: Mike Wills, Systems Security Certified Practitioner Official Study Guide

Integrated Information Defense II

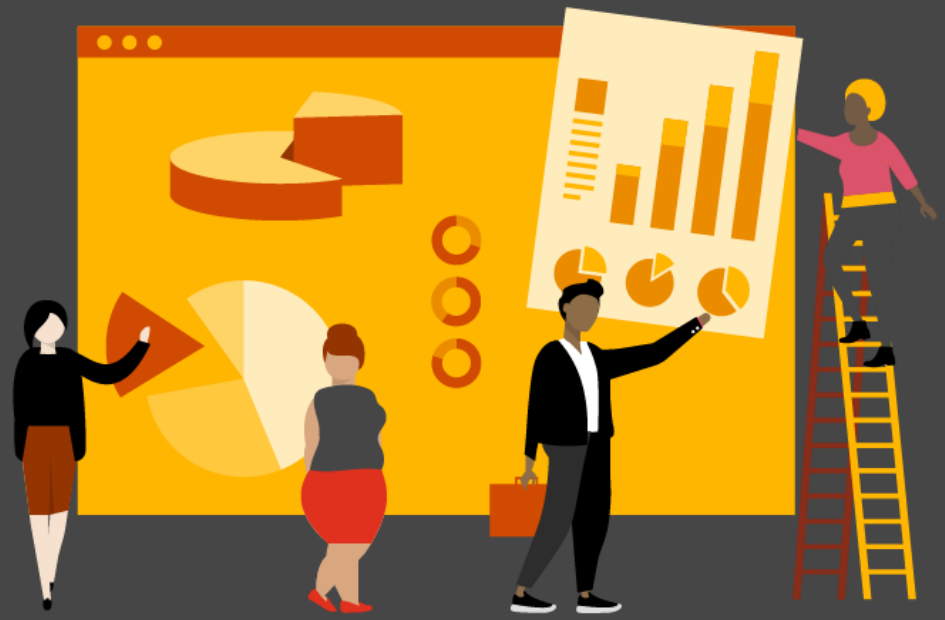
What did Boldi AG wrong? Was it due care, due diligence or both?
This is a case where due care and due diligence were both failed.

Due care requires
- identifying information risks to high-priority goals, objectives, processes, or assets;
- implementing controls, countermeasures, or strategies to limit their possible impacts;
- and operating those controls (and the systems themselves) in prudent and responsible ways.

Here, the information risks were obviously not identified.

Due diligence requires
- ongoing monitoring of these controls as well as periodic verification that they still work correctly and that new vulnerabilities or threats,
- changes in business needs, or changes in the underlying systems have not broken some of these risk control measures.

Here, there were no controls and no periodic verification of them.



2

Part 2

Integrated Information Defense III

Boldi AG - options for limiting or containing damage from risk

You

To Stefan Stamm

Reply | Reply All | Forward | ...

Hi Stefan,

Based on the key principles of defense, the basic options that Boldi AG has for limiting or containing damage from risk are: deter, detect, prevent, and avoid.

Deter means to convince the attacker that costs they'd incur and difficulties they'd encounter by doing an attack are probably far greater than anticipated gains.

Detecting that an attack is imminent or actually occurring is vital to taking any corrective, evasive, or containment actions.

Prevention either keeps an attack from happening or contains it so that it cannot progress further into the target's systems.

Avoiding the possible damage from a risk requires terminating the activity that incurs the risk, or redesigning or relocating the activity to nullify the risk.

Boldi AG should start acting now. I suggest: constant monitoring of their IT system and a statement regarding their measures to make possible attackers clear they have no chance.

Let me know if you need more input for the pitch. Happy to help!

Kind regards,
…