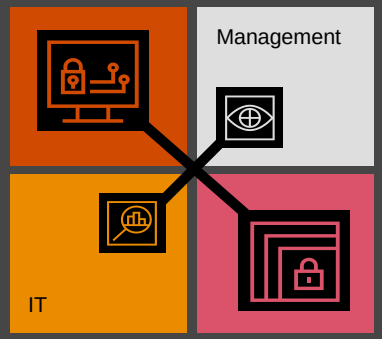
Virtual Case Experience Cybersecurity

Model Work Task 2

1

Part 1

Risk assessment I



What main stakeholders at Boldi AG should we talk to and what should the agenda of these interviews be?

There must be two different approaches in place, one for the management and one for the IT business.

Management and business leaders (top-down approach)

Talk to Boldi AG's management and business leaders (top-down approach). The purpose is to analyse the activity sectors of the company and which disruptive events are feared. Based on those fears, the idea is to analyse which applications are concerned. Here is how the agenda could look like:

1. Understand the main areas of activity of the company and the processes in those activity sectors (for example: logistics, production, procurement, etc.)
2. Have each leader of a main area of activity spontaneously speak up about their 1 to 3 principal security fears
3. Identify the main applications concerned by those fears
4. Proceed with step 2 of the risk assessment

IT department (bottom-up approach)

Talk to Boldi AG's IT department (bottom-up approach). The idea is to analyse the applications and the risks that they are exposed to and to then analyse how those risks would impact the processes of the company's main areas of activity. Here is how the agenda could look like:

1. Identify critical applications for each main area of activity of the company
2. Review documentation of applications
3. Analyse gap between current state of applications and industry standards
4. Filter out the least likely scenarios (focus necessary also for financial reasons as it is not possible to cover all risk)
5. Review applications and most likely scenarios with the IT department

2

Part 2

Risk assessment II

What kind of information Boldi AG typically stands to lose with which impact?

Information risk for Boldi AG?

Yes, because the data could represent significant vulnerabilities of company systems, and its inadvertent or deliberate disclosure could be very damaging to the company; because the lack of controls on access and use suggests that data integrity is lacking or cannot be assessed and because conflicting formats and content might make much of the data unusable for analysis and decision making without a lot of effort, impacting whether that data can support decision making in a timely manner. These are the expression of confidentiality, integrity, and availability for these data sets.

C – no controls on access

I – no controls on access

A – inconsistent in format

Part 3

Risk assessment III

Quantitative Assessments

Quantitative assessments attempt to arithmetically compute values for the probability of occurrence and the single loss expectancy. These assessments typically need significant insight into costs, revenues, usage rates, and many other factors that can help estimate lost opportunities, for example. Quantitative assessments rely on a sufficiently large pool of reliable data.

Qualitative Assessments

Qualitative assessments, by contrast, depend on experienced people to judge the level or extensiveness of a potential impact, as well as its frequency of occurrence. Not all clients have a sufficient amount of reliable data for a quantitative assessment, which is the reason why qualitative assessment might be the better approach for information security risk assessments. It all depends on the client in the end.

Both are valuable and provide important insight; quite often, management and leadership will not have sufficient data to support a quantitative assessment, or enough knowledge and wisdom in an area of operations to make a qualitative judgment.