CONFERENCE DAY SEPTEMBER 30, 2022
INDEPENDENT WORKSHOPS SEPTEMBER 29, 2022

DataMass Gdańsk Summit

Engineering Risk Assessment – how to measure the risk in IT infrastructure

Alicja Grochocka

What is an IT Risk Assessment ?

Risk Assessment

Comprehensively reviewing all major aspects of a company's IT infrastructure

IT Risk Assessment – 3 step process

Risk Evaluation

The first step of the evaluation phase is to understand the critical resources that could be affected by potential threats and vulnerabilities. This allows to realize what processes, and assets are most important to day-to-day business operations.
Then it is easier to identify the components of your IT infrastructure that need the most protection.
The next step is to identify threats, weaknesses, and vulnerabilities that create the most potential risk.

Risk Assessment

Determining the chances of threats penetrating evaluated vulnerabilities.
Understanding the severity of each threat.
Determining possible impact on business.
Prioritize Risks and recommended controls.

Risk Mitigation

Introduce solutions and implementation plan.
Solution implementation.
Introduce performance and effectiveness metrics.
Introduce risk monitoring mesurements.
Introducing closure memos.

How to measure indicated IT risk?

Key Characteristics of a KRI	**Example:** The number of incidents where customer personal data is put at risk
Quantifiable: The indicator needs to be measurable (numbers, percentages, etc.), relatively precise, and meaningful without the need for interpretation.	Provides a precise measurement of incidents.
Predictable: The indicator must provide early warning signs that management can act on.	When examined over time, can demonstrate the likelihood of another incident.
Informative (Auditable): The indicator must measure the status of risk and control.	Illustrates how effective or ineffective the current controls are to stop these incidents.
Comparable: The indicator must be able to track trends over a period of time in order to put a stop to those that are negative.	Can be compared against past months' statistics to show trends in incidents.

How to measure indicated IT risk?

Network

- **Network Availability** – The amount of time (measured in minutes) that the company's network is available for use by all authorized users divided by the total amount of time the network is scheduled to be available for use over the same period of time, as a percentage.
- **Number of Instances Where Network Bandwidth Utilization Exceeded Threshold** – The total number of instances during the measurement period where network bandwidth capacity exceed a defined threshold (identified through network testing and monitoring) at which the network begins to exhibit request delays, low transmission speeds, etc.

Cloud Security

- **High-Risk Cloud Apps Discovered**
  Number of High-Risk Cloud Apps Detected based on Risk classification parameters for apps (e.g.: Apps without a well-defined privacy policy, hosting data outside EU etc.)
- **Cloud Services Having Access to Sensitive Data**
  Number of cloud services which store or process any data which is classified as sensitive by the organization

Cybersecurity

- **Mean Time To Identify (MTTI)** and **Mean Time To Contain (MTTC)** indicates that the Detect and Respond Phases are suffering. Poor performance in **MTTI** and **MTTC** is a huge contributor to breach costs. These should be two most important KPIs when measuring information security
- **Volume of data transferred using the corporate network** If employees have unrestricted access to the internet through the corporate network, monitoring the volume of traffic allows to identify misuse of company resources.