A CULTURAL TRANSFORMATION FOR SAFER COMPANY

D.R.E.A.M.

The path of cultural transformation created by IMQ Intuity that aims to increase a company's IT security

D.R.E.A.M. cultural transformation originates from IMQ Intuity's People-Centric approach to cybersecurity.
This approach is based on the assumption that the human factor must be placed at the heart of the information security response: every person, at every level of the company, plays an essential role in improving internal security. Processes and technologies thus become universal reinforcing tools, increasing the effectiveness of the entire organization rather than just the key players, which is all too often the case.

WHY ARE WE DOING THIS?

IMQ Intuity strongly believes that culture is the main tool to counter cyber risks.
Therefore, D.R.E.A.M. aims to increase long-lasting internal responsibility and resilience to cyber threats, transforming the company's cyber security culture both internally and externally to encompass the entire ecosystem of customers and suppliers.

HOW DO WE DO THIS?

D.R.E.A.M, is not a service, but rather a **vision** rooted in IMQ Intuity's core beliefs and visible in its services and solutions.Specifically, the **phases** of the transformation are:

DIAGNOSIS - ASSESSMENT OF THE PRESENT CULTURE

During this phase, an assessment of corporate IT security is carried out through three activities: the administration to all staff of a Security Culture Survey that maps the awareness level and internal knowledge of cyber risks to produce a clear overview of how security is perceived and experienced by employees; a Security Assessment that uses interviews and technical checks to assess the level of corporate security governance; and finally, the simulation of a cyber attack using the IMQ Intuity Red Team that evaluates the actual ability to recognize and react to a real cyber threat.

REVELATION - SHARING OF RESULTS

This is comprised of one or a series of presentations of the results from the previous phase. The aim is to make all company employees aware of the cyber problems and risks, using concrete examples and gamification to convey the message in an incisive and pleasant way.

EDUCATION - INCREASING KNOWLEDGE

The aim of this phase is to provide necessary and useful skills forbetter confronting cyber risk. Specific training activities are proposed based on the type of user and their role in the company. In addition to classroom and e-learning training, there are also simulated phishing campaigns. The purpose of these campaigns is to keep the level of attention to phishing high so that threats have a better chance of being recognized.

ACTION - INTRODUCTION OF SUPPORTING ACTIVITIES AND TOOLS

Given the actual risks demonstrated by the assessment activities, thisphase sees the introduction of tools and processes that will enhance corporate protection, such as the introduction of new security technologies and recurring **Vulnerability Management and Threat Intelligence services** to periodically search for new vulnerabilities.

MONITOR - VERIFICATION OF RESULTS

This last phase monitors the effectiveness of the actions undertaken through a second attack simulation activity by the IMQ Intuity Red Team. At the same time, other risk situations not yet corrected or not previously detected are analyzed.

THE TIMELINE OF D.R.E.A.M.

The cultural transformation path of D.R.E.A.M. is represented below in an example of a one-year project. The **timeline** represents one possible flow of activities, but it is always possible to customize the timeline according to specific business needs.