Summary of the Cyber Metrics Workshop at EUROCONTROL

One of the main conclusions of the conference on "Cybersecurity frameworks, mappings and metrics," held at EUROCONTROL on 23 JAN 2020, was that strategic cyber metrics requires further improvement. Most of the participants were uncomfortable with reporting cyber risk to senior managers and board members.

The current Cyber Metrics Workshop was birthed in 2021, when a group of seasoned CISOs (Chief Information Security Officer) took the challenge of improving the current situation with metrics and reporting for cybersecurity. They agreed to meet periodically to share their experience, lessons learned, successes, and failures in the hopes of creating a better situation. As the first outcome of the group, a white paper was published that presents orientations for reporting cyber risk and its underlying details to CISOs, their senior stakeholders, and their Boards.

The paper describes methods that help CISOs engage in cyber risk management, measure the effectiveness of their programs, provide proper oversight, and communicate this effectively to their stakeholders and teams. While not a focus of the above-mentioned paper, the content also helps with reporting cyber risk to other stakeholders, such as regulators, insurers, and clients.

As a capstone to this paper, the invitation-only workshop on Cyber Metrics was hosted by EUROCONTROL, on 16 SEPT 2022, to broaden the community and report on progress. The workshop offered CISOs and board members the opportunity to exchange their experiences in measuring cyber risk and reporting to boards. Over 80 participants and 18 speakers from the most mature organizations attended the workshop in five sectors (finance, telecom, transport, energy and international organizations).

We summarize they key outcomes of the discussions:

- There is an increasing awareness among C-suites and Boards that cyber risk to their organizations is "material"" and increasing. However, there is also a lack of Board and senior stakeholder understanding of the risk and a communication gap within the departments in charge of mitigating cyber risk. This currently leads to a conservative attitude regarding cyber risk at the strategic level and a low cyber risk appetite.
- In the EU and the US, new cybersecurity regulations (NIS II, DORA, NYDFS …) are being issued, with obligations towards cyber training of Board members, Board oversight of cyber risk management, and individual accountability/liability of Board members. Disclosure obligations to shareholders are also changing to include cyber risk management and Board oversight (SEC, Dutch code).
- Some organizations have already taken steps to report cyber metrics in their annual report to shareholders and include the result of such metrics in the calculation of the bonus scheme for corporate stakeholders (not just the IT departments).
- Benchmarking the cyber-security performance with other companies/competitors seems to be an increasing request of senior management. The request for a "single score" arises. Some vendors offer such a single scoring as a service, however not yet in a way that can be considered as fully representative/satisfactory.
- Many organizations are moving ahead of compliance/standards (using ISO or NIST) over maturity-based models towards quantifiable performance/effectiveness-based (KCI and KPI) approaches. However, the selection of relevant metrics and dashboards a very much organization-specific. Peer comparison and external use of the results is

still beyond the current state of the art, for example insurance purposes are still not pragmatic.

- Prioritization of cyber risk mitigation measures, specific to the organizations and adapting to their changing threat environment, is on top of the agenda of most CISOs. Using inappropriate metrics leads organizations to spend resources, effort, and time addressing the wrong problems at the outset and potentially future business cycles, as senior look for consistency in the metrics used and improvement over time.
- CISOs use a large number (several hundreds) of metrics to keep an up-to-date overview of the current state of implementing their cyber security strategy, policies, and controls, to identify deviations and respond accordingly. Boards cannot cope with the reporting of these. But instead of summarizing them in average overall indicators for the Boards, CISOs would be well advised to select a subset of individual metrics (less than ten), related to the most important controls/policies/solutions which they believe are the most relevant at a particular point in time. Internal alignment on these key controls, the ideal state and the trajectory to reach these is an essential step in the reporting. Board oversight is perceived to facilitate execution.
- The most advanced organizations are using data lakes to ingest all information from their infrastructure and produce dashboards and reporting in the required granularity across stakeholder levels. The same data is therefore becoming an objective for proper reporting at the strategic level, at CISO-level, and at the level of the technical staff responsible for implementing mitigations/controls/policies/solutions. Metrics become in this way an integral element in the implementation and feedback loop ("democratization" of metrics).
- A combination of metrics/dashboards highlighting goals/gaps/trends/trajectories with illustrative stories related to the current threat landscape is perceived as benefiting Board responsiveness and engagement.

Proposed next steps

   a. Raise awareness on existing good practices in Cyber Metrics to increase the knowledge of the challenges and community best practices by increasing the white paper reads via social media promotion, podcasts, and blogs.
   b. Hosting the white paper on additional national cybersecurity centers' webpages
   c. Presenting the knowledge from the white paper at industry events
2. Expand the exchanging of Cyber Metrics and Reporting best practices by:
   a. Continue facilitating trusted exchanges in a small group of peers to drive action
   b. Organize an annual conference for exchanging knowledge across peers
3. Promote the guidelines of the white paper to support standardization activities
   a. Liaise with NIST, ISO
   b. …
4. Launch a project on Cyber Metrics at country level, in collaboration with ITU