Reporting and Feedback

Table of Contents

Reporting and Feedback

Reporting and Feedback

35

**035 Reporting and feedback.

Reporting and Feedback

- Communication between analysts and decision makers, peers, and other intelligence consumers regarding their products and work performance
- Reporting and feedback help identify intelligence requirements and intelligence gaps
- Reporting only as effective as its feedback counterpart

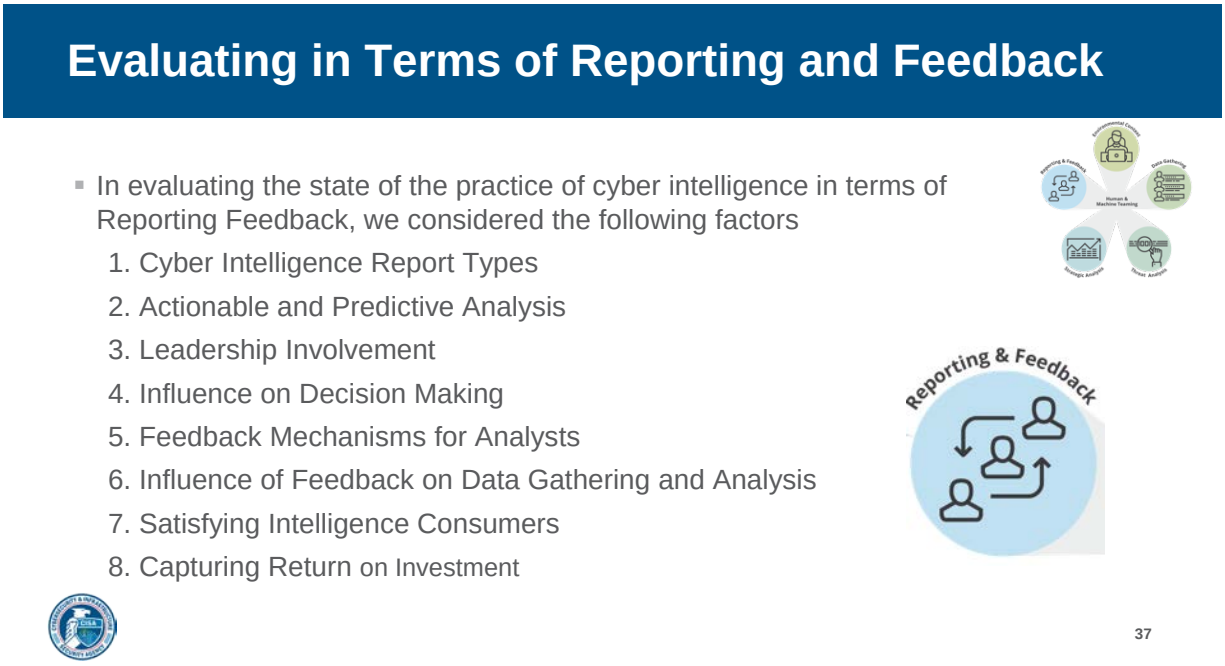
36

**036 This is the last component of the cyber intelligence conceptual framework, and it represents the communication of and subsequent feedback to cyber intelligence analysts regarding their products. A cyber intelligence analyst should take into account their audience's background and technical knowledge when producing verbal or written analysis. I'm talking about being able to communicate technical to non-technical audiences.

Reporting and feedback identifies intelligence gaps for the analyst to fill, concepts needing further explanation, and opportunities for collaboration.
One of the important
things to remember here is that the reporting mechanism, it's only effective as the feedback

counterpart. Where I work, feedback is considered a gift. It helps you build as a person and it helps the mission. So if you're not getting the feedback on the work that you are doing, you need to go and get it, because then you're not sure what the requirements are and when you don't know the requirements, your collection could be stale, your analysis could be stale and static, and the process could suffer and could be missing the threats that are happening today.

Evaluating in Terms of Reporting and Feedback



**037 Evaluating the state of practice of cyber intelligence in terms of reporting and feedback, we considered the following factors. Is your organization producing a variety of cyber intelligence reports? Are the reports actionable? Do they have predictive analysis? Is leadership

really involved in that process? Does leadership's involvement actually give the analysts the information they need to do their job, and in turn does the analysis that the cyber intelligence team, is it producing assessments that lead to decisionmakers actually making decisions? Is it influencing their decision-making process?

Other factors we looked at is feedback mechanisms for analysts? Do the analysts actually have mechanisms to receive feedback, and is it influencing their data gathering and analysis capabilities? Is the reports that the analysis--excuse me--the reports that the cyber intelligence team is reporting out there, how do you know that it is satisfying intelligence consumers? And lastly, is the cyber intelligence team capturing return on investment for its work? Those are the factors that we looked at in terms of assessing organizations for reporting and feedback.

**038 I wanted to list here some more types of specific cyber reports that we heard in our interviews that cyber intelligence teams are producing and disseminating. Aspects in the complete framework that we just talked about, environmental context, data gathering, threat and strategic analysis, reporting feedback, all contribute to these type of reports.

I think you can see from this slide that there's a good mixture of both technical reports that might be done more daily or weekly, and more strategic reports that are less frequent and target a different audience.

Notices

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM20-0262